

# දසවැනි පාර්ලිමේන්තුව - පළමුවැනි සභාවාරය

ඔස්ට්‍රේලියාවට ඇමරිකානු ඩොලර් මිලියන 2.5 ක ණය ආපසු ගෙවීමේදී සිදුවූ

සයිබර් අපරාධ හා සම්බන්ධ වංචාව සම්බන්ධයෙන්

## රජයේ මුදල් පිළිබඳ කාරක සභාවේ වාර්තාව

පාර්ලිමේන්තුව වෙත ඉදිරිපත් කරන ලද්දේ

කාරක සභාවේ සභාපති

ගරු (ආචාර්ය) හර්ෂ ද සිල්වා මහතා විසිනි

2026 ජූලි 10 වැනි සිකුරාදා

## කාරක සභාවේ සහිත මන්ත්‍රීවරුන්

- ගරු (ආචාර්ය) හර්ෂ ද සිල්වා මහතා, පා.ම. (සභාපති)
- ගරු චතුරංග අබේසිංහ මහතා, පා.ම.
- ගරු (ආචාර්ය) කෞෂල්‍යා ආරියරත්න (මෙය), පා.ම.
- ගරු අර්කම් ඉල්යාස් මහතා, පා.ම.
- ගරු නිශාන්ත ජයවීර මහතා, පා.ම.
- ගරු නීතිඥ රවුෆ් හකීම් මහතා, පා.ම.
- ගරු රවී කරුණානායක මහතා, පා.ම.
- ගරු හර්ෂණ රාජකරුණා මහතා, පා.ම.
- ගරු භානක්කියන් රාජපුත්තිරන් රාසමාණික්කම් මහතා, පා.ම.
- ගරු අජිත් අගලකඩ මහතා, පා.ම.
- ගරු එම්. කේ. එම්. අස්ලම් මහතා, පා.ම.
- ගරු නිමල් පලිභේන මහතා, පා.ම.
- ගරු නීතිඥ විත්‍රාල් ප්‍රනාන්දු මහතා, පා.ම.
- ගරු විජේසිරි බස්නායක මහතා, පා.ම.
- ගරු සුනිල් රාජපක්ෂ මහතා, පා.ම.
- ගරු තිළිණ සමරකෝන් මහතා, පා.ම.
- ගරු වම්පික හෙට්ටිආරච්චි මහතා, පා.ම.
- ගරු නීතිඥ ලක්මාලි හේමචන්ද්‍ර (මෙය), පා.ම.

# 1. විධායක සාරාංශය

2025 නොවැම්බර් සිට 2026 ජනවාරි දක්වා කාලය තුළ එක්ස්පෝට් ෆයිනෑන්ස් ඕස්ට්‍රේලියා වෙත ගෙවිය යුතුව තිබූ ඇතැම් ණය ආපසු ගෙවීම්වලදී, සයිබර් අපරාධ හා සම්බන්ධ වංචාවක් හේතුවෙන් මහා භාණ්ඩාගාරයට ඇමරිකානු ඩොලර් මිලියන 2.5 ක අලාභයක් සිදු විය. මෙය අදාළ විදේශීය ණය හිමියා වෙත ගෙවිය යුතු හිඟ මුදලක් නිර්මාණය වීමටද හේතු විය. ස්ථාවර නියෝග 121 යටතේ රාජ්‍ය ණය සේවාකරණය පිළිබඳ සිය අධීක්ෂණ කර්තව්‍යයන්ට අනුකූලව, රජයේ මුදල් පිළිබඳ කාරක සභාව විසින් මෙම කරුණ පිළිබඳව විමර්ශනය කරන ලදී. මෙම සිදුවීම් මාලාව සම්බන්ධයෙන් රාජ්‍ය නිලධාරීන් රැසක් සමඟ සාකච්ඡා කිරීම සඳහා කාරක සභාව අවස්ථා හතරකදී රැස් වූ අතර, අදාළ ආයතනවලින් සවිස්තරාත්මක වාර්තා ද ලබා ගන්නා ලදී. එම සාකච්ඡා සහ ලේඛන මගින් කාරක සභාව වෙත ලබා දෙන ලද තොරතුරු පදනම් කරගනිමින්, මෙම සයිබර් අපරාධයට අදාළ වංචාවට බලපෑ සිදුවීම් සහ සාධක රජයේ මුදල් පිළිබඳ කාරක සභාව විසින් හඳුනාගත් ආකාරයට මෙම වාර්තාව මගින් ඉදිරිපත් කරනු ලැබේ.

ණය ආපසු ගෙවීමේ ක්‍රියාවලියේ අභ්‍යන්තර පාලනයන්හි පැවැති පද්ධතිමය දුර්වලතා සහ යල්පැන ගිය විද්‍යුත් තැපැල් (ඊමේල්) යටිතල පහසුකම් හේතුවෙන් සයිබර් අපරාධ හා සම්බන්ධ වංචාවක අවදානම ඉහළ ගිය බව කාරක සභාව නිගමනය කරයි. මෙය හුදකලා බිඳවැටීමක් නොවන අතර, ආයතන කිහිපයක් පුරා පැවැති පාලනමය, ක්‍රියාපටිපාටික සහ මෙහෙයුම්මය අසාර්ථකත්වයන්ගේ ප්‍රතිඵලයකි.

අලුතින් පිහිටුවන ලද රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත ණය ආපසු ගෙවීමේ කාර්යයන් සංක්‍රමණය කිරීමේ ක්‍රියාවලිය සඳහා මගපෙන්වීමට පූර්ව යොමු කිරීම් අනුදේශ ලේඛනයක් නොමැති වීම, කාර්ය පටිපාටිමය සහ මෙහෙයුම්මය පරතරයන් තවදුරටත් උග්‍ර කළ ප්‍රධාන පාලනමය දුර්වලතාවක් විය. සක්‍රීය අභ්‍යන්තර පාලනයන් සහ ශක්තිමත් තොරතුරු තාක්ෂණ පද්ධති නොමැති වීම මෙන්ම ජ්‍යෙෂ්ඨ නිලධාරීන් වෙත ගැටලු වාර්තා කිරීමේ පටිපාටි ප්‍රමාණවත් නොවීම තුළ රාජකාරි පැහැරහැරීමක්, කාර්ය පටිපාටිමය මට්ටමින්, නිරීක්ෂණය විය. මෙහෙයුම් මට්ටමින්, මධ්‍යම මට්ටමේ නිලධාරීන් නොසැලකිලිමත් ලෙස කටයුතු කර ඇති අතර නිවැරදි තීරණ ගැනීමට අසමත් වී ඇත. විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය තුළ මෙකී කාර්ය පටිපාටිමය අඩුපාඩු ඓතිහාසිකව පැවතී ඇති බව කාරක සභාව විසින් වැඩිදුරටත් නිරීක්ෂණය කරන ලදී.

මෙම නිගමන පදනම් කරගනිමින්, රාජ්‍ය මුදල් කළමනාකරණය තුළ මෙවැනි බරපතල අසාර්ථකත්වයන් නැවත සිදු වීම වැළැක්වීමේ තීරණාත්මක පියවර ලෙස කාරක සභාව විසින් ප්‍රධාන නිර්දේශ කිහිපයක් ඉදිරිපත් කරනු ලැබේ. සමස්ත විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය සම්බන්ධයෙන් ජාතික විගණන කාර්යාලය මගින් වහාම විශේෂ විගණනයක් පැවැත්වීමේ අවශ්‍යතාව, රාජ්‍ය අංශයේ තොරතුරු තාක්ෂණ පද්ධති පිළිබඳ ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර ඒකකයේ නිර්දේශ ක්‍රියාත්මක කිරීම සහතික කිරීම සඳහා ඩිජිටල් ආර්ථික අමාත්‍යාංශය විසින් නොපමාව පියවර ගැනීම සහ රාජ්‍ය මුදල් ක්‍රියාවලීන් මෙහෙයවනු ලබන මුදල් රෙගුලාසි මුදල් අමාත්‍යාංශය මගින් වහාම පූර්ණ ප්‍රතිසංස්කරණයකට ලක් කිරීම මීට ඇතුළත් වේ.

මෙම වාර්තාවේ අන්තර්ගතය, රාජ්‍ය මුදල් අධීක්ෂණය සම්බන්ධයෙන් රජයේ මුදල් පිළිබඳ කාරක සභාවේ බලතල තුළට පමණක් සීමා වේ. අපරාධ විමර්ශන පැවැත්වීම හෝ නීතිමය වගකීම් පිළිබඳ තීන්දු ප්‍රකාශ කිරීම රජයේ මුදල් පිළිබඳ කාරක සභාවේ බලතලවලට අයත් නොවේ.

## 2. හැඳින්වීම

ශ්‍රී ලංකා පාර්ලිමේන්තුවේ ස්ථාවර නියෝග 121 ට අනුකූලව, ස්ථාපිත නෛතික රාමුවලට සහ වාර්ෂික විසර්ජන පනතට අනුකූලව මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධන අමාත්‍යාංශය (මුදල් අමාත්‍යාංශය) සහ අනෙකුත් අදාළ රාජ්‍ය ආයතන විසින් අදාළ නීතිමය ප්‍රතිපාදන, මුදල් රෙගුලාසි සහ ක්‍රියාවලීන් අනුගමනය කරන්නේදැයි තහවුරු කරමින්, රාජ්‍ය මුදල් පිළිබඳ ඕනෑම අංශයක් පරීක්ෂා කිරීම රජයේ මුදල් පිළිබඳ කාරක සභාවේ බලතලවලට අයත් වේ. රජයේ මුදල් පිළිබඳ කාරක සභාවේ කාර්යභාරය වන්නේ රාජ්‍ය මුදල් අධීක්ෂණය කිරීමයි; ණය කළමනාකරණය සහ ණය සේවාකරණය මීට ඇතුළත් වේ. එබැවින්, විදේශ ණය ආපසු ගෙවීමේදී ඇමරිකානු ඩොලර් මිලියන 2.5 ක් අතුරුදහන් වීම පිළිබඳ සිදුවීම කාරක සභාවේ විෂය පථයට අයත් වේ. අපරාධ විමර්ශන පැවැත්වීම හෝ නීතිමය වගකීම් පිළිබඳ තීන්දු ප්‍රකාශ කිරීම රජයේ මුදල් පිළිබඳ කාරක සභාවේ බලතලවලට අයත් නොවේ.

2026 අප්‍රේල් 30 වන දින පැවැති කාරක සභා සාකච්ඡාවෙන් සහ 2026 මැයි 08 වන දින කාරක සභාවේ මූලික වාර්තාව පාර්ලිමේන්තුවට ඉදිරිපත් කිරීමෙන් පසුව,<sup>1</sup> රජයේ මුදල් පිළිබඳ කාරක සභාව මගින් ලබා දුන් උපදෙස්වලට ප්‍රතිචාර වශයෙන්, සයිබර් අපරාධ හා සම්බන්ධ මෙම වංචාව පිළිබඳ සවිස්තරාත්මක වාර්තාවක්, 2026 ජුනි මස මුල් භාගයේදී මුදල් අමාත්‍යාංශය විසින් ලබා දෙන ලදී.<sup>2</sup> එම වාර්තාව මගින් වංචාව අනාවරණය කර ගැනීමට තුඩු දුන් සිදුවීම් මෙන්ම ඒ වන තෙක් ගන්නා ලද පියවරයන් ද ආවරණය කරන ලදී. අදාළ ලේඛන සහ විද්‍යුත් තැපැල් සංවාද සටහන් ඇතුළත් ඇමුණුම් ද ඊට ඇතුළත් කර තිබුණි

මුදල් අමාත්‍යාංශ වාර්තාව පිළිබඳව 2026 ජුනි 08 වන දින පවත්වන ලද සාකච්ඡාවේදී, ශ්‍රී ලංකා මහ බැංකුවේ අධිපතිවරයා විසින් එම වාර්තාවේ ඉදිරිපත් කර තිබූ ඇතැම් කරුණු අභියෝගයට ලක් කරන ලද අතර, ශ්‍රී ලංකා මහ බැංකුව මගින් වාර්තාවක් ඉදිරිපත් කිරීම සඳහා කාලය ලබා දෙන ලෙස ඉල්ලා සිටින ලදී. මෙහිදී මතභේදයට තුඩු දුන් ප්‍රධාන කරුණ වූයේ, ණය ආපසු ගෙවීමේ ක්‍රියාවලියට අදාළ සුදුසු කාර්ය පටිපාටි සහ වගකීම් පිළිබඳව — විශේෂයෙන්ම මුදල් ගනුදෙනු වාර්තා කිරීමේ පනත යටතේ මුදල් විශුද්ධීකරණය වැළැක්වීමේ කරුණු සම්බන්ධයෙන් — මුදල් අමාත්‍යාංශයට උපදෙස් ලබා නොදීම පිළිබඳව ශ්‍රී ලංකා මහ බැංකුවට චෝදනා එල්ල වී තිබීමයි. එම සාකච්ඡාවේ ප්‍රතිඵලයක් ලෙස පහත සඳහන් වාර්තා රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලදී:

- ශ්‍රී ලංකා මහ බැංකුව විසින් ඉදිරිපත් කරන ලද වාර්තා දෙකක්: එකක් මගින් සිදුවීම් පිළිබඳ ශ්‍රී ලංකා මහ බැංකුවේ අදහස ඉදිරිපත් කර ඇති අතර,<sup>3</sup> අනෙක මගින් මුදල් අමාත්‍යාංශයේ වාර්තාව සම්බන්ධයෙන් නිශ්චිත ප්‍රතිවිරුද්ධ ප්‍රතිචාර ඉදිරිපත් කර ඇත.<sup>4</sup> අදාළ ලේඛන සහ විද්‍යුත් තැපැල් සංවාද සටහන් ඇතුළත් සවිස්තරාත්මක ඇමුණුම් ද ඊට ඇතුළත් වේ.

<sup>1</sup> ඇමුණුම 1 - ඇමරිකානු ඩොලර් මිලියන 2.5 ක විදේශ ණය ආපසු ගෙවීමේ වංචනික ගනුදෙනුව පිළිබඳ රජයේ මුදල් පිළිබඳ කාරක සභාවේ වාර්තාව -2026 මැයි 08 දිනැති

<sup>2</sup> ඇමුණුම 2 - සිදුව ඇතැයි කියනු ලබන, ආසන්න වශයෙන් ඇමරිකානු ඩොලර් මිලියන 2.5 ක විදේශ ණය ආපසු ගෙවීමේ වංචනික ගනුදෙනුව සම්බන්ධයෙන් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත මුදල් අමාත්‍යාංශය විසින් ඉදිරිපත් කරන ලද වාර්තාව -2026 ජුනි 01 දිනැති (ඇමුණුම් හැර)

<sup>3</sup> ඇමුණුම 3 - රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ශ්‍රී ලංකා මහ බැංකුව විසින් ඉදිරිපත් කරන ලද විස්තීර්ණ වාර්තාව - 2026 ජුනි 15 දිනැති (ඇමුණුම් හැර)

<sup>4</sup> ඇමුණුම 4 - සිදුව ඇතැයි කියනු ලබන, ආසන්න වශයෙන් ඇමරිකානු ඩොලර් මිලියන 2.5 ක විදේශ ණය ආපසු ගෙවීමේ වංචනික ගනුදෙනුව සම්බන්ධයෙන්, රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත මුදල් අමාත්‍යාංශය ඉදිරිපත් කළ වාර්තාවට පිළිතුරු වශයෙන් ශ්‍රී ලංකා මහ බැංකුව විසින් ඉදිරිපත් කරන ලද වාර්තාව -2026 ජුනි 15 දිනැති (ඇමුණුම් හැර)



- වර්තමාන ජාතික සයිබර් ආරක්ෂණ පදනම ස්ථාපිත කරන ලද 2023 වසරේ සිට රාජ්‍ය ආයතන සඳහා වන සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය මෙන්ම මුදල් අමාත්‍යාංශයේ තොරතුරු තාක්ෂණ පද්ධති සම්බන්ධයෙන් සිදු කරන ලද ඇගයීම් හා විගණනයන් සවිස්තරාත්මකව දක්වනු ලබන ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර ඒකකයේ ප්‍රතිචාර වාර්තාව<sup>5</sup>
- මුදල් ගනුදෙනු වාර්තා කිරීමේ පනත ශ්‍රී ලංකා මහ බැංකුව සඳහා අදාළ වන ආකාරය සහ ණය කළමනාකරණය පිළිබඳ එහි අන්තර්කාලීන වගකීම සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකු පනතේ 132 වන වගන්තිය බලපැවැත්වෙන ආකාරය පිළිබඳව නීතිපති දෙපාර්තමේන්තුව විසින් ලබා දුන් අර්ථ නිරූපණය.<sup>6</sup>

මෙම කරුණු දැක්වීම් 2026 ජුනි 23 වන දින සාකච්ඡාවට ලක් කරන ලද අතර, එමගින් අදාළ ආයතන විසින් ලබා දෙන ලද තොරතුරු සංසන්දනය කිරීමට සහ ඇගයීමට කාරක සභාවට අවස්ථාව හිමි විය. 2025 දෙසැම්බර් 31 වන දින ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව වසා දැමීමට පෙර සහ 2026 මැයි 22 වන දින නිකුත් කරන ලද ගැසට් නිවේදනය මගින් රාජ්‍ය ණය කළමනාකරණය සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකුවේ කාර්යභාරය නිල වශයෙන් අවසන් කරන තෙක්, ශ්‍රී ලංකා මහ බැංකු පනතේ 132 වන වගන්තිය බලපැවැත්වූ ආකාරය පිළිබඳව මෙම රැස්වීමේදී නීතිපතිවරයාගෙන් තවදුරටත් පැහැදිලි කිරීමක් ඉල්ලා සිටින ලදී.<sup>7</sup>

මෙම වාර්තාව මගින් ඉහත සඳහන් සියලුම වාර්තා, ආයතන හතරෙන් ලැබුණු ප්‍රතිචාර සහ 2026 අප්‍රේල් 30, ජුනි 08 සහ ජුනි 23 යන දිනයන්හි රජයේ මුදල් පිළිබඳ කාරක සභාවේදී පැවැති සාකච්ඡා සලකා බලනු ලැබේ. මෙම වාර්තාව තවත් කොටස් පහකින් සමන්විත වේ: සයිබර් අපරාධ හා සම්බන්ධ වංචාව සිදු වූ ආයතනික පසුබිම පිළිබඳ දළ සටහනක්; ඊට අදාළ සිදුවීම් සහ සයිබර් අපරාධ හා සම්බන්ධ වංචාව අනාවරණය කර ගැනීම පිළිබඳ සවිස්තරාත්මක සාරාංශයක්; ඇතැම් කරුණු සහ සිදුවීම් සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකුව සහ මුදල් අමාත්‍යාංශය අතර පැවැති මතභේදාත්මක කරුණු; ඉන්පසුව කාරක සභාවේ නිගමන සහ ඉන් අනතුරුව කාරක සභාවේ නිර්දේශයන් වේ. මෙහි අන්තර්ගතය සහ නිගමන කාරක සභාව වෙත ලබා දෙන ලද තොරතුරුවලට පමණක් සීමා වන බව නිරීක්ෂනය කිරීම වැදගත් වේ.

### 3. පසුබිම

සයිබර් අපරාධ හා සම්බන්ධ වංචාව සිදු වූ කාලපරිච්ඡේදය (2025 නොවැම්බර් සිට 2026 මාර්තු මාසයේදී එය අනාවරණය කර ගන්නා තෙක්), 2022 අප්‍රේල් මාසයේදී ද්විපාර්ශ්වික සහ වාණිජ ණය හිමියන් වෙත ණය ආපසු ගෙවීම ඒකපාර්ශ්විකව අත්හිටුවීමෙන් පසු ඔවුන්ගේ එකඟතාව මත සිදුවූ බාහිර ණය ප්‍රතිව්‍යුහගත කිරීමේ ක්‍රියාවලියේ අවසාන අදියර සහ ණය කළමනාකරණ වගකීම් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත පැවරීමේ ආයතනික සංක්‍රමණික ක්‍රියාවලියේ අවසාන අදියර

<sup>5</sup> ඇමුණුම 5 - 2026 ජුනි 09 දාතමින් ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර ඒකකය විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත යොමු කරන ලද ලිපිය - සයිබර් ආරක්ෂණ වාර්තා ඉදිරිපත් කිරීම සහ විදේශ සම්පත් දෙපාර්තමේන්තුවේ විද්‍යුත් තැපැල් සර්වරයේ තත්ත්වය පිළිබඳ පැහැදිලි කිරීම (ඇමුණුම් හැර)

<sup>6</sup> ඇමුණුම 7 - 2026 ජුනි 15 දාතමින් නීතිපති දෙපාර්තමේන්තුව විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත යොමු කරන ලද ලිපිය

<sup>7</sup> ඇමුණුම 8 - 2026 ජුනි 25 දාතමින් නීතිපති දෙපාර්තමේන්තුව විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත යොමු කරන ලද ලිපිය

සමග සමපාත විය. ප්‍රතිව්‍යුහගත කිරීමේ කොන්දේසි සම්බන්ධයෙන් 2024 මැද භාගයේදී ද්විපාර්ශ්වික ණය හිමියන් සමඟ අත්සන් කරන ලද අවබෝධතා ගිවිසුම් පදනම් කරගනිමින්, 2025 අගභාගය වැනි මෑත කාලයක් දක්වාම සංශෝධිත ණය ගිවිසුම් අවසන් කිරීමේ ක්‍රියාවලියෙහි මුදල් අමාත්‍යාංශය නිරතව සිටියේය.

2024 ජුනි මාසයේදී 2024 අංක 33 දරන රාජ්‍ය ණය කළමනාකරණ පනත සම්මත කිරීමෙන් අනතුරුව, රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත රාජ්‍ය ණය කළමනාකරණය කිරීමේ කාර්යය පැවරීමේ ආයතනික සංක්‍රමණික ක්‍රියාවලිය 2024 නොවැම්බර් මාසයේදී ආරම්භ කරන ලද අතර, ඒ සඳහා 2026 මැයි දක්වා මාස 18 ක සංක්‍රමණික කාලපරිච්ඡේදයක් පැවැතිණි. ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව, මුදල් අමාත්‍යාංශයේ විදේශ සම්පත් දෙපාර්තමේන්තුව සහ මුදල් අමාත්‍යාංශයේ රාජ්‍ය ව්‍යවසාය දෙපාර්තමේන්තුව පුරා විසිරී තිබූ වගකීම් මධ්‍යගත කිරීම මීට ඇතුළත් විය.

සමස්ත සංක්‍රමණික ක්‍රියාවලියට ණය කළමනාකරණයේ විවිධ අංශ ඇතුළත් වූවද, මෙම වාර්තාවේ අවධානය යොමු කර ඇත්තේ විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය සංක්‍රමණය වීම පිළිබඳව පමණි. සලකා බලනු ලබන සයිබර් අපරාධ හා සම්බන්ධ වංචාව සිදු වූයේ මෙම ක්‍රියාවලිය තුළදීය.

### 3.1 . රාජ්‍ය ණය කළමනාකරණ කාර්යාලය ස්ථාපිත කිරීමට පෙර පැවැති විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය

වගකීම් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත පැවරීමට පෙර, ද්විපාර්ශ්වික සහ බහුපාර්ශ්වික ණය ආපසු ගෙවීම් හසුරුවන ලද ක්‍රියාවලිය පහත පරිදි විය:

- I. විදේශ සම්පත් දෙපාර්තමේන්තුව මගින් ණය හිමියන්ගෙන් ඉන්වොයිසි ලබා ගත් අතර, එහි ණය කළමනාකරණ අංශය විසින් ඒවා සකස් කිරීම, සත්‍යාපනය කිරීම සහ අනුමත කිරීම සිදු කරන ලදී.
- II. අනුමත කරන ලද ඉන්වොයිසි ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව වෙත යොමු කරන ලද අතර, එමගින් ඉන්වොයිසියේ සඳහන් සත්‍යාපනය කළ ගෙවීම් තොරතුරු, ප්‍රමිතගත ගෙවීම් උපදෙස් ලෙස සංචිත නොවන කළමනාකරණ පද්ධතියට ඇතුළත් කරන ලදී.
- III. සෑම ප්‍රමිතගත ගෙවීම් උපදෙසකම අවශ්‍ය ගෙවීම් තොරතුරු අඩංගු බව ශ්‍රී ලංකා මහ බැංකුවේ මුදල් දෙපාර්තමේන්තුව විසින් සත්‍යාපනය කරන ලදී.
- IV. මහා භාණ්ඩාගාරයේ ඒකාබද්ධ අරමුදලේ කොටසක් ලෙස, ශ්‍රී ලංකා මහ බැංකුවේ පවත්වාගෙන යනු ලබන නියෝජ්‍ය භාණ්ඩාගාර ලේකම් ගිණුමේ තැන්පත් කර තිබූ විදේශ විනිමය භාවිත කරමින්, සත්‍යාපිත තොරතුරු පදනම් කරගෙන, ශ්‍රී ලංකා මහ බැංකුවේ ගෙවීම් සහ පියවීම් දෙපාර්තමේන්තුව විසින් ප්‍රතිලාභියාගේ ගිණුම වෙත ජාත්‍යන්තර SWIFT පද්ධතිය ඔස්සේ ගනුදෙනුව සිදු කරන ලදී.

රාජ්‍ය ණය කළමනාකරණ කාර්යාලය ස්ථාපිත කිරීමට පෙර පැවති විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය

මූලාශ්‍රය: ද්විපාර්ශ්වික බහුපාර්ශ්වික / ණයහිමියන්  
ණය ආපසු ගෙවීම සඳහා ඉන්වොයිසිය නිකුත් කිරීම



ඉන්වොයිසිය



පියවර I - විදේශ සම්පත් දෙපාර්තමේන්තුව - ණය කළමනාකරණ අංශය  
ඉන්වොයිසිය ලබාගැනීම • සැකසීම • සත්‍යාපනය කිරීම • අනුමැතිය ලබා දීම



අනුමත කළ ඉන්වොයිසිය



පියවර II - ශ්‍රී ලංකා මහ බැංකුව (CBSL) - රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD)  
අනුමත කළ ඉන්වොයිසියේ තොරතුරු භාවිත කරමින්, ප්‍රමිතිගත පියවිම් උපදෙස් (SSI) හරහා  
සංචිත නොවන කළමනාකරන පද්ධතියට ගෙවීම් තොරතුරු ඇතුළත් කිරීම; සංචිත නොවන  
කළමනාකරන පද්ධති මගින් SWIFT-අනුකූල උපදෙස් ජනනය කිරීම



ප්‍රමිතිගත පියවිම් උපදෙස්  
සත්‍යාපනය SSI for  
verification



III වන පියවර: ශ්‍රී ලංකා මහ බැංකුව (CBSL) - මූල්‍ය දෙපාර්තමේන්තුව  
අවශ්‍ය සියලුම ගෙවීම් තොරතුරු ප්‍රමිතිගත පියවිම් උපදෙස් (SSI) තුළ අන්තර්ගත වී ඇති බව තහවුරු  
කිරීම



ගෙවීම් විස්තර සත්‍යාපනය  
කිරීම



IV වන පියවර: ශ්‍රී ලංකා මහ බැංකුව (CBSL) - ගෙවීම් දෙපාර්තමේන්තුව  
ශ්‍රී ලංකා මහ බැංකුවේ ඇති භාණ්ඩාගාර නියෝජ්‍ය ලේකම් (DST) ගිණුමේ රඳවා ඇති විදේශ  
විනිමය භාවිතයෙන් SWIFT ගනුදෙනුව ක්‍රියාත්මක කිරීම භාණ්ඩාගාරයේ ඒකාබද්ධ —  
අරමුදලෙන් ලබාගත් අරමුදල්



ණයහිමියාගේ ගිණුම  
වෙත SWIFT ගෙවීම

### 3.2. රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) සඳහා මාස 18ක සංක්‍රාන්ති කාලසීමාව

2024 නොවැම්බර් සිට 2026 මැයි දක්වා පැවති මාස 18ක සංක්‍රාන්ති කාලසීමාව තුළ, විවිධ දෙපාර්තමේන්තු අතර බෙදී පැවති ණය නිකුත් කිරීමේ සහ කළමනාකරණ කාර්යයන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් භාරගෙන මධ්‍යගත කිරීමට සිදු විය.

කෙසේ වෙතත්, ආයතන කිහිපයක් සම්බන්ධ වන මෙම සංකීර්ණ, බහු ආකෘතික සංක්‍රාන්ති ක්‍රියාවලිය- සඳහා සවිස්තරාත්මක මාර්ගෝපදේශයක් හෝ කාර්යය නියමයන්(Terms of Reference) සපයන කිසිදු ලේඛනයක් කාරක සභාවට ලබාදීමට නොහැකි විය. සංක්‍රාන්තිය නිසි පරිදි අවසන් කරන ලද්දේ දැයි විනිශ්චය කිරීමට කිසිදු ප්‍රධාන කාර්ය සාධන දර්ශකයක් (KPIs) නොමැත. රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ (PDMO) මෙහෙයුම් පාලනය කරන මාර්ගෝපදේශ ප්‍රකාශයට පත් කර ඇත්තේ, කාර්යාලය ස්ථාපිත කර මාස 10කට පසුව, එනම් 2025 සැප්තැම්බර් 19 වන දිනය. ශ්‍රී ලංකා මහ බැංකුව (CBSL) සහ රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) අතර ඔවුන්ගේ සහයෝගීතා ක්ෂේත්‍ර පිළිබඳ අවබෝධතා ගිවිසුම (MoU) අත්සන් කර ඇත්තේ නිල සංක්‍රාන්ති කාලසීමාව අවසන් වීමට ආසන්නව, එනම් 2026 මාර්තු 09 වන දිනය.

මාස 18ක සංක්‍රාන්ති ක්‍රියාවලියේ කාලරාමුව

|                       |   |                                                                                                                                                                                         |
|-----------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2024 නොවැම්බර් 24     | ● | රාජ්‍ය ණය කළමනාකරණ කාර්යාලය ස්ථාපිත කිරීම<br>මාස 18ක සංක්‍රාන්ති කාලසීමාව ආරම්භ වීම                                                                                                     |
| 2025 ජනවාරි 01        | ● | විදේශ සම්පත් දෙපාර්තමේන්තුවේ ණය අංශය රාජ්‍ය ණය කළමනාකරණ කාර්යාලය සමඟ සම්බන්ධ වීම<br>විදේශ ණය කළමනාකරණය මධ්‍යගත කිරීම                                                                    |
| 2025 මාර්තු දෙසැම්බර් | ● | ශ්‍රී ලංකා මහ බැංකුව විසින් රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ නිලධාරීන් පුහුණු කිරීම.<br>සියලුම ණය කළමනාකරණ කාර්යයන් සඳහා ධාරිතාව වර්ධනය කිරීම                                               |
| 2025 ඔක්තෝබර් 13-15   | ● | දේශීය මෙහෙයුම් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත භාර දීම<br>භාණ්ඩාගාර වෙන්දේසි ( ඔක්තෝබර්13) · ණය සේවාකරණය ( ඔක්තෝබර්15)                                                                  |
| 2025 ඔක්තෝබර් 13-24   | ● | විදේශ ණය : පද්ධති ප්‍රවේශය ලබාදෙන ලදී.<br>සංචිත නොවන කළමනාකරන පද්ධති ගෙවීම් උපදෙස් ( ඔක්තෝබර් 13) · ප්‍රමිතිගත පියවීම් උපදෙස් නිර්මාණය කිරීම ( ඔක්තෝබර්24))                             |
| 2025 ඔක්තෝබර් 30      | ● | දේශීය ණය නිකුත්ව භාරගැනීම දෙසැම්බර් දක්වා ප්‍රමාද වීම<br>ප්‍රාථමික ගනුදෙනුකරුවන් සඳහා වන නියාමන අවශ්‍යතා ප්‍රමාද වී තිබීම.                                                              |
| 2025 දෙසැම්බර්        | ● | දේශීය ණය නිකුත්ව රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත සංක්‍රමණය වීම<br>මුදල් අමාත්‍යාංශය යටතේ රාජ්‍ය ණය දෙපාර්තමේන්තු පරිශ්‍රය (1 වන සතිය( → රාජ්‍ය ණය කළමනාකරණ කාර්යාල පරිශ්‍රය (2 වන සතිය) |
| 2025 දෙසැම්බර් 31     | ● | රාජ්‍ය ණය දෙපාර්තමේන්තුව නිල වශයෙන් වසා දැමීම<br>2026 ජනවාරි 01 දින නිල වසා දැමීමේ උත්සවය                                                                                               |
| 2026 මාර්තු 09        | ● | අවබෝධතා ගිවිසුම අත්සන් කිරීම : රාජ්‍ය ණය කළමනාකරණ කාර්යාලය සහ ශ්‍රී ලංකා මහ බැංකුව<br>අඛණ්ඩ සහයෝගීතාව සඳහා වන රාමුව                                                                     |
| 2026 මැයි 22          | ● | ශ්‍රී ලංකා මහ බැංකුවෙහි සංක්‍රාන්ති කාර්යභාරය නිල වශයෙන් අවසන් වීම<br>මාස 18ක සංක්‍රාන්තිය සම්පූර්ණ වීම · ගැසට් පත්‍රය ප්‍රකාශයට පත් කිරීම                                              |

සංක්‍රාන්ති කාලසීමාව ආරම්භයේදී, පොදුරාජ්‍ය මණ්ඩලීය ලේකම් කාර්යාලයේ ණය වාර්තා කිරීමේ සහ කළමනාකරණය කිරීමේ පද්ධතිය (CS-DRMS) හැසිරවූ විදේශ සම්පත් දෙපාර්තමේන්තුවේ (ERD) ණය කළමනාකරණ අංශය, ඊට අනුයුක්ත කාර්ය මණ්ඩලය ද සමඟින් 2024 දෙසැම්බර් මාසයේදී රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) වෙත මාරු කරනු ලැබීය. ඔවුන් 2025 ජනවාරි 01 වන දින රාජකාරි භාර ගන්නා ලදී.

සංක්‍රාන්තීය අතරතුර, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි හි පසු කාර්යාලය (Back Office) විසින් ණය ගිවිසුම් සහ ගෙවීම් සැසඳීමේ සහ වාර්තා කිරීමේ කාර්යය භාර ගන්නා ලදී. මින් අදහස් වූයේ, කලින් විදේශ සම්පත් දෙපාර්තමේන්තුවේ වගකීමක්ව පැවති ඉන්වොයිස් තහවුරු කිරීම සහ ගෙවීම් අනුමත කිරීම සඳහා දැන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වගකිව යුතු බවයි.

කෙසේ වෙතත්, විදේශීය ණයහිමියන් සමඟ සම්බන්ධීකරණය කිරීමේ පෙර සිට පැවති කාර්යභාරය (Legacy role) හේතුවෙන්, ණයහිමියන්ගෙන් ලැබෙන ඉන්වොයිසයන්ගෙන් වැඩි කොටසක් ඉලෙක්ට්‍රොනික සන්නිවේදනය හරහා අඛණ්ඩව විදේශ සම්පත් දෙපාර්තමේන්තුව වෙත ලැබුණු අතර, ඒවා සැකසීම සඳහා රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි පසු කාර්යාලය වෙත යොමු කරන ලදී.

ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව විසින් හසුරුවන ලද ණය කළමනාකරණ කාර්යයන් භාර ගැනීම සම්බන්ධයෙන්, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි කාර්ය මණ්ඩලය 2025 මාර්තු සහ දෙසැම්බර් අතර කාලයේදී කණ්ඩායම් තුනක් ලෙස රාජ්‍ය ණය දෙපාර්තමේන්තු කාර්ය මණ්ඩලය විසින් පුහුණු කරන ලදී. විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලියේදී ප්‍රමිතිගත පියවීම් උපදෙස් (SSIs) නිර්මාණය කිරීම ඇතුළුව සංචිත නොවන කළමනාකරණ පද්ධතියේ කාර්යයන් ද මීට ඇතුළත් විය.

රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් රාජ්‍ය ණය දෙපාර්තමේන්තුවෙහි කාර්යයන් භාර ගැනීමේ කාලරාමුව, 2025 සැප්තැම්බර් 23 වන දින මුදල් අමාත්‍යාංශය සහ ශ්‍රී ලංකා මහ බැංකුව අතර පැවති සම්බන්ධීකරණ සභා රැස්වීමේදී සහ 2025 සැප්තැම්බර් 25 වන දින භාණ්ඩාගාර ලේකම්වරයා විසින් ශ්‍රී ලංකා මහ බැංකුව වෙත යවන ලද ලිපියක් මගින් තහවුරු කරන ලදී. මෙම වාර්තාවේ සලකා බලන ගැටලුවට අදාළ කරුණු පහත පරිදි වේ:

- I. දේශීය භාණ්ඩාගාර සුරැකුම්පත් නිකුත් කිරීමේ වෙන්දේසි අඛණ්ඩව රාජ්‍ය ණය දෙපාර්තමේන්තුව විසින් සිදු කරනු ලැබූ නමුත්, 2025 ඔක්තෝබර් 13 වන දින සිට ශ්‍රී ලංකා මහ බැංකුව අනුමත කිරීමේ ක්‍රියාවලිය යටතේ රාජ්‍ය ණය කළමනාකරණ කාර්යාල නිලධාරීන් විසින් ඒවා හසුරුවනු ලැබීය.
- II. දේශීය ණය සේවාකරණය 2025 ඔක්තෝබර් 15 වන දින සිට රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත මාරු කිරීමට නියමිත විය.
- III. විදේශ ණය සේවාකරණය සම්බන්ධයෙන්, ඔක්තෝබර් 13 වන දින සිට ගෙවීම් උපදෙස් ලබා ගැනීමට සහ ඔක්තෝබර් 24 වන දින සිට ප්‍රමිතිගත පියවීම් උපදෙස් (SSI) නිර්මාණය කිරීමට ඉඩ සලසමින් සංචිත නොවන කළමනාකරණ පද්ධතියට ප්‍රවේශය ලබා දීම සඳහා රාජ්‍ය ණය කළමනාකරණ කාර්යාල නිලධාරීන් වෙනුවෙන් පිවිසුම් තොරතුරු (Login credentials) නිර්මාණය කරන ලදී.

මෙම සංක්‍රාන්තීය සමඟින්, පෙර විදේශ සම්පත් දෙපාර්තමේන්තුව විසින් සිදු කරන ලද ණයහිමියන්ගේ ඉන්වොයිස සහ ගෙවීම් තොරතුරු තහවුරු කිරීම සහ අනුමත කිරීම සඳහා රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වගකිව යුතු ආයතනය බවට පත් විය. මීට පෙර ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD-CBSL) විසින් සිදු කරන ලද, සංචිත නොවන කළමනාකරණ පද්ධතියට ප්‍රමිතිගත පියවීම් උපදෙස් (SSI) ලෙස ගෙවීම් උපදෙස් ඇතුළත් කිරීමේ ආයතනය බවට ද එය පත් විය. ශ්‍රී ලංකා මහ බැංකුවෙහි මූල්‍ය දෙපාර්තමේන්තුව අඛණ්ඩව ප්‍රමිතිගත පියවීම් උපදෙස් හි අවශ්‍ය ගෙවීම්

තොරතුරු තහවුරු කළේය. ශ්‍රී ලංකා මහ බැංකුවෙහි ගෙවීම් සහ පියවීම් දෙපාර්තමේන්තුව අඛණ්ඩව ගෙවීම් ක්‍රියාත්මක කළේය.

2025 දෙසැම්බර් මාසයේදී මෙම කාර්යයන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත සංක්‍රමණය වීමත් සමඟ ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව සතුව තවදුරටත් ඉටු කිරීමට කිසිදු කාර්යයක් නොතිබුණි. එහි ප්‍රතිඵලයක් ලෙස, 2025 දෙසැම්බර් 31 වන දින සිට ක්‍රියාත්මක වන පරිදි රාජ්‍ය ණය දෙපාර්තමේන්තුව වසා දමන ලද අතර, 2026 ජනවාරි 01 වන දින මුදල් අමාත්‍යාංශයේ ජ්‍යෙෂ්ඨ නිලධාරීන්ගේ සහභාගීත්වයෙන් නිල වසා දැමීමේ උත්සවයක් පවත්වන ලදී.

දෘඩාංග සහ මෘදුකාංග සම්බන්ධයෙන් ගත් කල, කලින් රාජ්‍ය ණය දෙපාර්තමේන්තුව විසින් භාවිතා කරන ලද පද්ධති අඛණ්ඩව රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් ද භාවිතා කරනු ලබයි . විශේෂයෙන්ම, සංචිත නොවන කළමනාකරණ පද්ධතිය සහ රාජ්‍ය සුරැකුම්පත් වෙන්දේසි පද්ධතිය (GSAS) පිළිවෙලින් විදේශ ණය ආපසු ගෙවීමේ සහ දේශීය ණය නිකුත් කිරීමේ කළමනාකරණ ක්‍රියාවලීන්හි අඛණ්ඩව කොටසක් වේ .2026 මාර්තු 09 දිනැති අවබෝධතා ගිවිසුම මගින්, 2025 දෙසැම්බර් සිට වසර 2ක කාලයක් සඳහා රාජ්‍ය සුරැකුම්පත් වෙන්දේසි පද්ධතිය(GSAS )සඳහා ප්‍රවේශය ලබා දෙන බවත්, ඒ සමඟම සංචිත නොවන කළමනාකරණ පද්ධතියට සහ රාජ්‍ය ණය කළමනාකරණය සඳහා අත්‍යවශ්‍ය දත්ත සමුදායන් සහ මෙවලම් වැනි අනෙකුත් පද්ධති සඳහා අඛණ්ඩ ප්‍රවේශය ලබා දෙන බවත් නිශ්චිතව දක්වා ඇත .රාජ්‍ය සුරැකුම්පත් වෙන්දේසි පද්ධතිය (GSAS) භාවිතයේ පවතින තෙක්, ශ්‍රී ලංකා මහ බැංකුවෙහි ආපදා ප්‍රතිසාධන මධ්‍යස්ථානය සහ බැංකු අධ්‍යයන කේන්ද්‍රය ද රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි නිලධාරීන් වෙත ලබා දෙන ලදී.

රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත සංක්‍රමණය වීමෙන් පසු විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය

මූල්‍යාශ්‍රය -ද්විපාර්ශ්වික / බහුපාර්ශ්වික ණයහිමියන්

ණය ආපසු ගෙවීම සඳහා ඉන්වොයිසිය නිකුත් කිරීම

ඉන්වොයිසිය



පියවර I - විදේශ සම්පත් දෙපාර්තමේන්තුව

ණයහිමියාගෙන් ඉන්වොයිසිය භාරගෙන රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ පසු කාර්යාලය වෙත යොමු කිරීම



ඉන්වොයිසිය යොමු කිරීම



පියවර II රාජ්‍ය ණය කළමනාකරණ කාර්යාල - රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ පසුපෙළ කාර්යාලය

ඉන්වොයිසිය සැකසීම, තහවුරු කිරීම සහ අනුමත කිරීම; ප්‍රමිතිගත පියවිම් උපදෙස් හරහා සංචිත නොවන කළමනාකරණ පද්ධතියට ගෙවීම් තොරතුරු ඇතුළත් කරමින් SWIFT-අනුකූල උපදෙස් ජනනය කිරීම



ප්‍රමිතිගත පියවිම් උපදෙස් සත්‍යාපනය  
SSI for verification



III වන පියවර ශ්‍රී ලංකා මහ බැංකුව :- මූල්‍ය දෙපාර්තමේන්තුව

අවශ්‍ය සියලුම ගෙවීම් තොරතුරු ප්‍රමිතිගත පියවිම් උපදෙස් තුළ අන්තර්ගත වී ඇති බව තහවුරු කිරීම



ගෙවීම් විස්තර සත්‍යාපනය  
කිරීම



IV වන පියවර ශ්‍රී ලංකා මහ බැංකුව :- ගෙවීම් සහ පියවිම් දෙපාර්තමේන්තුව

ශ්‍රී ලංකා මහ බැංකුවේ ඇති භාණ්ඩාගාර නියෝජ්‍ය ලේකම් ගිණුමේ රඳවා ඇති විදේශ විනිමය භාවිතයෙන් SWIFT ගනුදෙනුව ක්‍රියාත්මක කිරීම - භාණ්ඩාගාරයේ ඒකාබද්ධ අරමුදලෙන් ලබාගත් අරමුදල්



ණයහිමියාගේ ගිණුමට  
SWIFT ගෙවීම



### 3.3 මුදල් අමාත්‍යාංශයේ පවතින තොරතුරු තාක්ෂණ පද්ධති සහ සයිබර් ආරක්ෂණ යටිතල පහසුකම්

මුදල් අමාත්‍යාංශය සතුව අමාත්‍යාංශයේ තොරතුරු තාක්ෂණ පද්ධති කළමනාකරණය කිරීම සඳහා නිශ්චිත තොරතුරු තාක්ෂණ කළමනාකරණ දෙපාර්තමේන්තුවක් (DITM) පවතියි. කෙසේ නමුත්, මෙම දෙපාර්තමේන්තුවට, treasury.gov.lk යන ඩොමේන් නාමය භාවිත කරන දෙපාර්තමේන්තු 17ක තොරතුරු තාක්ෂණ පද්ධතිවල වගකීම පමණක් භාර වී ඇත. නමුත්, විදේශ සම්පත් දෙපාර්තමේන්තුව (ERD) සතුව, 2000 වර්ෂයේ පමණ සිට erd.gov.lk යන ඩොමේන් නාමය ද සමඟ ක්‍රියාත්මක වන වෙනම තොරතුරු තාක්ෂණ පද්ධතියක් පවතින අතර, එහි සේවය කරන තොරතුරු තාක්ෂණ නිලධාරීන් සෘජුවම විදේශ සම්පත් දෙපාර්තමේන්තුවේ අධ්‍යක්ෂ ජනරාල් වෙත වාර්තා කරනු ඇත. මෙම තොරතුරු තාක්ෂණ කණ්ඩායම් දෙක අතර කිසිදු සම්බන්ධීකරණයක් ඇති නොවූ බව පෙනෙන අතර, එය පාලනය සහ ක්‍රියාපටිපාටියේ ඉතා කනගාටුදායක බිඳ වැටීමක් සේ පෙනෙන්නට ඇත. වෙනම පද්ධතියක් ලෙස පවත්වාගෙන යනු ලැබූව ද, විදේශ සම්පත් දෙපාර්තමේන්තුවේ පද්ධති පිළිබඳව, අධීක්ෂණ කටයුතු තොරතුරු තාක්ෂණ කළමනාකරණ දෙපාර්තමේන්තුවේ අධ්‍යක්ෂ ජනරාල් විසින් ක්‍රියාත්මක කළ යුතුව තිබුණි.

රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ අධ්‍යක්ෂ ජනරාල්ට අනුව, එම කාර්යාලය ස්ථාපිත කිරීමේ දී දෙපාර්තමේන්තුවේ විද්‍යුත් තැපැල් සහ අනෙකුත් කාර්යයන් සඳහා අවශ්‍ය සර්වර් ධාරිතාව (server space) විදේශ සම්පත් දෙපාර්තමේන්තුවෙහි පද්ධතිවලින් ලබා ගෙන ඇත. රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි තොරතුරු තාක්ෂණ නිලධාරියාව, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ පද්ධති නඩත්තු කිරීම සඳහා විදේශ සම්පත් දෙපාර්තමේන්තුව වෙතින් අනුයුක්ත කර ඇත. 2026 ජුනි මස 23 වැනි දින වන විටත්, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයට තමන්ගේම සර්වරයන් ලබා ගැනීම සඳහා ප්‍රසම්පාදන ක්‍රියාවලිය අඛණ්ඩව සිදුවෙමින් පැවත ඇත.

මෙහිදී වඩාත් ඉස්මතු වූ ගැටලුව වූයේ, විදේශ සම්පත් දෙපාර්තමේන්තුව විසින් යල් පැන ගිය Microsoft Exchange Server 2016 භාවිත කරමින් සිටීමයි. ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදයට අනුව, සර්වරයේ ප්‍රධාන ධාරාවේ 2020 ඔක්තෝබර් මාසයේ දී අවසන් විය. නමුත්, මයික්‍රොසොෆ්ට් ආයතනය සහය යටතේ 2025 ඔක්තෝබර් මස 14 වන දින දක්වා දීර්ඝ කරන ලද සුළු ආරක්ෂක යාවත්කාලීනයන් ලැබී ඇත. සැපයුම්කරු විසින් ලබාදෙන තාක්ෂණික සහාය දීර්ඝ කිරීමට පියවර ගෙන තිබුණ ද, යාවත්කාලීන පද්ධතියක් ප්‍රසම්පාදනය කරනු නොලැබ ඇති බැවින්, විදේශ සම්පත් දෙපාර්තමේන්තුවේ සහ රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ හි තොරතුරු තාක්ෂණ පද්ධති, සයිබර් ප්‍රහාරවලට ලක්වීමේ සම්පූර්ණ අවදානමකට ලක් කර ඇත. එබැවින්, ප්‍රශ්න සහගත සයිබර් අපරාධය හා සම්බන්ධ වංචාව 2025 නොවැම්බර් මස මැද භාගයේදී ආරම්භ වූයේ, සර්වර් පද්ධතියට මයික්‍රොසොෆ්ට් ආරක්ෂක යාවත්කාලීනයන් ලැබීම නතර වී මාසයකට පමණ පසුව වීම, හුදු අහම්බයක් පමණක් නොවන බව පැහැදිලිය.

2024 දෙසැම්බර් මාසයේ දී KPMG ආයතනය සහ ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය විසින් ඒකාබද්ධව සිදු කරන ලද සවිස්තරාත්මක විගණනයකදී, විදේශ සම්පත් දෙපාර්තමේන්තුව ඇතුළු මුදල් අමාත්‍යාංශයේ තොරතුරු තාක්ෂණ යටිතල පහසුකම් සහ සයිබර් ආරක්ෂණ පියවරයන්හි පවතින පද්ධතිමය අඩුපාඩු ඉස්මතු කර ඇත. එම පද්ධතිවල බහු-සාධක සත්‍යාපනය (multifactor authentication) වැනි සරල ආරක්ෂණ ක්‍රමවේදයන් පවා නොමැති බවත්, සහ එම පද්ධති සඳහා දුර්වල මුරපද භාවිත කරමින් සිටි බවත් එම විගණනය මගින් ඉස්මතු කර ඇත. ආයතනයේ සේවකයින් අතර නිශ්චිත කාර්ය සහ වගකීම් නිර්වචනය නොකිරීම නිසා ඔවුන්ගේ වගවීමේ අසමත්වීම් සහ මෙහෙයුම් අකාර්යක්ෂමතාවයන් පවතින බව හඳුනාගන්නා ලදී. 2026 ජනවාරි සහ අප්‍රේල් මාසවලදී ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය සහ ජාතික සයිබර් ආරක්ෂණ මෙහෙයුම් මධ්‍යස්ථානය (NCSOC) විසින් සිදු කරන ලද සමාලෝචනයන්හිදී ද, මෙම තොරතුරු තාක්ෂණ පද්ධති සයිබර් ප්‍රහාරවලට ලක්වීමේ අවදානම් ඉස්මතු කරනු ලැබ තිබුණි.

අවාසනාවකට, ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදයට, තම අනතුරු ඇඟවීම් සහ නිර්දේශ සම්බන්ධව අදාළ ආයතන විසින් ක්‍රියාවට නංවාලීම සහතික කිරීමේ බලයක් ඇති බවක් දැක ගැනීමට නොමැත. අවශ්‍ය ක්‍රියාමාර්ග ගැනීමේ වගකීම එම ආයතන වෙත ම පැවරී ඇත.

#### 4. සිදුවීම්වල කාල රාමුව

රාජ්‍ය මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද ලේඛන මත පදනම්ව, අදාළ සයිබර් අපරාධය හා සම්බන්ධ වංචාව සිදු වූ ආකාරය සහ එහි ප්‍රධාන සිදුවීම් හා ලේඛනවල සාරාංශයක් මෙම කොටසින් ඉදිරිපත් කරනු ඇත. මෙම සිදුවීම් මාලාව ඇති වූ ආකාරය වඩාත් හොඳින් අවබෝධ කර ගැනීම සඳහා අභ්‍යන්තර පාලන පරිසරය සමාලෝචනය කිරීම මෙම කොටසෙහි අරමුණ වේ.

##### 4.1. ඉන්දියාවට සිදු කරන ලද ආපසු ගෙවීම් සම්බන්ධ ගැටලුවක් සොයාගැනීම

විමර්ශනයට ලක්ව ඇති සයිබර් අපරාධය හා සම්බන්ධ වංචාව, එක්ස්පෝර්ට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනය (Export Finance Australia) වෙත සිදු කරන ලද ගෙවීමක් සම්බන්ධයෙන් වුවද, මුදල් අමාත්‍යාංශය විසින් සයිබර් ආරක්ෂණ තර්ජනයක් ප්‍රථම වරට සොයාගනු ලැබුවේ 2026 ජනවාරි මාසයේ දී ඉන්දියානු අපනයන-ආනයන බැංකුවට (EXIM Bank) ගෙවීමට නියමිතව තිබූ ණය ආපසු ගෙවීමක් ක්‍රියාත්මක කිරීමේ දීය.

2026 ජනවාරි මස 6 වැනි දින ඉන්දියානු අපනයන-ආනයන බැංකුවට (EXIM Bank) කරන ලද ගෙවීමක් ක්‍රියාත්මක කිරීම අසාර්ථක වී ඇත<sup>8</sup>. ශ්‍රී ලංකා මහ බැංකුව විසින් JPMorgan සමාගම අතරමැදි ආයතනය ලෙස යොදා ගනිමින්, රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් ලබා දුන් ගිණුම් විස්තර වෙත ගෙවීමක් කිරීමට උත්සාහ කළ විට, JPMorgan සමාගමේ ගෝලීය වංචා වැළැක්වීමේ මෙහෙයුම් කණ්ඩායම විසින් එම ගෙවීම ප්‍රතික්ෂේප කර ඇත. රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ නිලධාරීන් විසින් ඉන්දියානු අපනයන-ආනයන බැංකුවේ (EXIM Bank) කණ්ඩායමක් සමග සම්බන්ධ වී ඇති අතර, එම සම්බන්ධතාව හරහා, වංචනික ගෙවීම් උපදෙස් ලබා දී ඇති බවට තහවුරු කර ගැනීමට මුදල් අමාත්‍යාංශයට හැකියාව ලැබී ඇත.

ඉන්දියානු අපනයන-ආනයන බැංකුව (EXIM Bank) සමඟ සන්නිවේදනය කිරීමෙන් හා ඔවුන් විසින් සත්‍යාපනය කරනු ලැබීමෙන් අනතුරුව, නිවැරදි ගිණුමට ගෙවීම සිදු කර ලැබ ඇත. මෙම සැක සහිත ක්‍රියාකාරකම, 2026 ජනවාරි මස 09 වන දින අපරාධ පරීක්ෂණ දෙපාර්තමේන්තුව (CID) සහ ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසඳය වෙත වාර්තා කර ඇත. සැක සහිත වංචනික විද්‍යුත් තැපැල් ලිපිනය, [eximbankindia.in](http://eximbankindia.in) යන ඩොමේන් නාමය භාවිත කර ඇති බව, විදේශ සම්පත් දෙපාර්තමේන්තුවේ තොරතුරු තාක්ෂණ නිලධාරියා විසින් ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසඳය වෙත කළ පැමිණිල්ලේ සඳහන්ව ඇත. (නිවැරදි ඩොමේන් නාමය [eximbankindia.in](http://eximbankindia.in) ලෙස දැක් වේ).

##### 4.2. ඕස්ට්‍රේලියාවට කරන ලද ආපසු ගෙවීම් ක්‍රියාත්මක නොවීම සොයාගැනීම

ඉන්දියානු අපනයන-ආනයන බැංකුව (EXIM Bank) සම්බන්ධ සිද්ධියෙන් අනතුරුව, සයිබර් ආරක්ෂණ තර්ජනයක අවදානම භාණ්ඩාගාර ලේකම්වරයා වෙත දැනුම් දී ඇති අතර, තත්ත්වය විමර්ශනය කිරීමේ කාර්ය භාරය, විදේශ සම්පත් දෙපාර්තමේන්තුවේ අධ්‍යක්ෂ ජනරාල් වෙත පවරා ඇත. සංවිධානාත්මක ප්‍රතිව්‍යුහගත කිරීමේ ක්‍රියාවලීන් සම්පූර්ණ කිරීමෙන් පසුව ඉදිරිපත් කරන ලද ඉන්වොයිසි මත පදනම්ව කරන ලද පෙර ගෙවීම් සියුම් ලෙස පරීක්ෂා කිරීමට විදේශ සම්පත් දෙපාර්තමේන්තුව ක්‍රියාමාර්ග ගෙන ඇත. එක්සත් රාජධානිය වෙත (එ.ජ.ඩො. 1,294,605.99 ක් ද), ජර්මනිය වෙත (යුරෝ 4,059,987.81 ක් ද) සහ බෙල්ජියම් වෙත (යුරෝ 60,974.88 ක් ද) ගෙවීම් ඇතුළු තවත් නියමිත වූ ගෙවීම් කිහිපයක් සඳහා විද්‍යුත් තැපෑලෙන් ලැබුණු ගෙවීම් උපදෙස් ද වංචනික බව තවදුරටත් හඳුනාගනු ලැබ ඇත.

සලකුණු කරන ලද ඉන්වොයිසිවල වලංගුභාවය තහවුරු කර ගැනීම සඳහා මෙම ණයහිමියන් තිදෙනා සමඟ පසු විපරම් කටයුතු 2026 ජනවාරි මස සිට මාර්තු මාසය දක්වා සිදු කරනු ලැබ ඇත. එහි ප්‍රතිඵලයක් ලෙස, එක්සත් රාජධානිය හා සම්බන්ධ ගෙවීම් වහාම අත්හිටුවන ලැබ ඇත. සැක සහිත පාර්ශ්වය විසින් ආරම්භ කරන ලද සන්නිවේදනයන් හඳුනාගෙන විමර්ශන බලධාරීන් දැනුවත් කරනු ලැබ ඇත. බෙල්ජියම් හා සම්බන්ධ ගෙවීම් නිවැරදි ගිණුමට සිදු කර ලැබ ඇත.

මෙම සත්‍යාපන ක්‍රියාවලිය අතරතුර, 2026 මාර්තු 23 වන දින එක්ස්පෝර්ට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනය (Export Finance Australia) විසින් පෙර මාසවල ඔවුන්ට ලැබිය යුතු ණය ආපසු ගෙවීම් නොලැබීම පිළිබඳව මුදල් අමාත්‍යාංශයේ නිලධාරීන් දැනුවත් කරනු ලැබ ඇත.

<sup>8</sup> මෙම ගෙවීම 2025 දී ප්‍රතිව්‍යුහගත කළ ණයවල පොලිය සඳහා වේ.

#### 4.3. සයිබර් අපරාධය හා සම්බන්ධ වංචාව ඇතුළත් විද්‍යුත් තැපෑල් දාමවල සාරාංශය

සයිබර් අපරාධය හා සම්බන්ධ වංචාවේ ක්‍රියාවලිය සහ එහි කාල රාමුව අවබෝධ කර ගැනීමේ පැහැදිලිම මාර්ගය නම්, විදේශ සම්පත් දෙපාර්තමේන්තුවේ නිලධාරීන් (සැබෑ නිලධාරීන් සහ ඵලෙස පෙනී සිටින ලද ව්‍යාජ නිලධාරීන්), එක්ස්පෝර්ට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනයේ (Export Finance Australia) නිලධාරීන් (සැබෑ නිලධාරීන් සහ ඵලෙස පෙනී සිටින ලද ව්‍යාජ නිලධාරීන්), සහ ක්‍රියාවලියේ දී සම්බන්ධ වූ අනෙකුත් ශ්‍රී ලාංකික ආයතනවල නිලධාරීන් අතර හුවමාරු වූ විද්‍යුත් තැපෑල් දාමයයි. මුදල් අමාත්‍යාංශය සහ ශ්‍රී ලංකා මහ බැංකුව විසින් රාජ්‍ය මුදල් පිළිබඳ කාරක සභාව වෙත ලබා දුන් විද්‍යුත් තැපෑල් දාම ඇසුරෙන් නිරූපිත සාරාංශයක් මෙම කොටසෙහි ඉදිරිපත් කර ඇත. ඩොමේන් නාමයන් පවත්වාගෙන යමින් විද්‍යුත් ලිපිනවල පුද්ගල නාම බැහැර කිරීම සඳහා නිර්නාමිකකරණය කළ, වෙනම විද්‍යුත් තැපෑල් දාම තුනක් කෙරෙහි මෙහි දී අවධානය යොමු කෙරෙනු ඇත.

2025 ඔක්තෝබර් මස 28 සිට 2026 ජනවාරි මස 15 දක්වා කාලය තුළ විදේශ සම්පත් දෙපාර්තමේන්තුවේ සහ ණයහිමියාගේ යැයි කියනු ලබන විද්‍යුත් තැපෑල් ලිපිනයන් අතර හුවමාරු වූ පණිවුඩ විද්‍යුත් තැපෑල් දාම 01 ඇතුළත් වේ.

##### 1. A@erd.gov.lk → Z@exportfinance.gov.au

2025 ඔක්තෝබර් මස 28

අත්සන් කරන ලද ප්‍රතිව්‍යුහගත ණය ගිවිසුම්වල ස්කෑන් කරන ලද පිටපත් යවා ඇත.

ඕස්ට්‍රේලියාව සමඟ ණය ප්‍රතිව්‍යුහගත කිරීම 2025 ඔක්තෝබර් මස 27 වන දින සම්පූර්ණ කරන ලද අතර, එය 2025 ඔක්තෝබර් මස 28 වන දින ප්‍රසිද්ධියේ ප්‍රකාශයට පත් කරනු ලැබ ඇත. මුල් අත්සන් කරන ලද පිටපත්වල පිටපත් විදේශ සම්පත් දෙපාර්තමේන්තුව විසින් රාජ්‍ය ණය දෙපාර්තමේන්තුව සහ රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත යවා ඇත. එක්ස්පෝර්ට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනය (Export Finance Australia) වෙත ආපසු ගෙවීම් සඳහා පවතින ගිණුම් විස්තර සංශෝධිත ගිවිසුමේ වෙනස් කර නොමැති බව මුදල් අමාත්‍යාංශයේ නිලධාරීන් කාරක සභාවේ දී පැවසූහ.

##### 2. Z@exportfinance-au.com → A@erd.gov.lk

2025 නොවැම්බර් මස 13

ඕස්ට්‍රේලියා ණය ප්‍රතිව්‍යුහගත කිරීමේ ගිවිසුම යටතේ ගෙවීම් සකස් කිරීම සඳහා ඉන්වොයිසි හයක් යවා ඇත.

මෙම විද්‍යුත් තැපෑල, Z@exportfinance.gov.au යන ලිපිනයෙන් කළ පෙර විද්‍යුත් තැපෑලට ප්‍රතිචාරයක් ලෙස ලැබී ඇත.

සටහන: මෙම ඉන්වොයිසි සඳහා 2025 නොවැම්බර් මස 14 දින ගෙවීම් සිදු කර ඇත.

ඉන්වොයිසි හය (මුළු එකතුව ඇමරිකානු ඩොලර් 2,180,184ක් පමණ):

I. ඕස්ට්‍රේලියානු ඩො. 141,739.95: නීති ගාස්තු

II. එ.ජ.ඩො. 996,221.85: Outotec ගනුදෙනුව සඳහා පොලී හිඟ මුදල්

III. එ.ජ.ඩො. 69,199.59: Wellard 1 ගනුදෙනුව සඳහා පොලී හිඟ මුදල්

IV. එ.ජ.ඩො. 340,126.84: Wellard 2 ගනුදෙනුව සඳහා පොලී හිඟ මුදල්

V. එ.ජ.ඩො. 304,432.45: Wellard 3 ගනුදෙනුව සඳහා පොලී හිඟ මුදල්

VI. එ.ජ.ඩො. 377,660.26: R.R. ටේලර් ගනුදෙනුව සඳහා පොලී හිඟ මුදල්

##### 3. A@erd.gov.lk → Z@exportfinanceau.com

2025 නොවැම්බර් මස 25

2025 නොවැම්බර් මස 24 වන දින සිදු කරන ලද ඇ.ඩො. 1,375,882.11 ක ගෙවීම, ප්‍රතිලාභී බැංකුව විසින් සපයන ලද පැහැදිලි හේතුවක් නොමැතිව, ශ්‍රී ලංකා මහ බැංකුව වෙත ආපසු ලබා දී ඇති බව දන්වා ඇත. (සත්‍ය වශයෙන් ආපසු ලබා දී ඇත්තේ ඇ.ඩො. 1,375,459.74 ක් පමණි).

##### 4. Z@exportfinanceau.com → A@erd.gov.lk

2025 නොවැම්බර් මස 26

ගෙවීම ආපසු ලැබෙන්නට ඇති හේතු පිළිබඳ සවිස්තරාත්මක පැහැදිලි කිරීමක් ලබා දී, සංශෝධිත, නිවැරදි ඉන්වොයිසි එවන බවට පොරොන්දු වී ඇත.

මෙම ගෙවීම, එක්සත් ජනපද බැංකු ගිණුමකට ඇමරිකානු ඩොලර් 377,660.26 ක් වන ලෙස සහ එක්සත් අරාබි එමීර් රාජ්‍යයේ බැංකු ගිණුමකට ඇමරිකානු ඩොලර් 997,799.48 ක් වන ලෙස, ගෙවීම් දෙකකට වෙන් කර ඇති බව ශ්‍රී ලංකා මහ බැංකු වාර්තාවේ දක්වා ඇත. එක්සත් අරාබි එමීර් රාජ්‍යයේ ගිණුමට කරන ලද ගෙවීම පිළිබඳව ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තු නිලධාරීන් විසින් විද්‍යුත් තැපෑල 02 හි දී ප්‍රශ්න කර ඇත.

2025 නොවැම්බර් මස 28 දින ඇමරිකා එක්සත් ජනපදයේ බැංකු ගිණුමට සංශෝධිත ගෙවීම සම්පූර්ණ කරන ලද නමුත්, 2025 දෙසැම්බර් මස 17 දින එක්සත් අරාබි එමීර් රාජ්‍යයේ ගිණුමට කරන ලද ගෙවීම අතරමැදි බැංකුව විසින් ප්‍රතික්ෂේප කර ඇත. 2026 ජනවාරි මස 13 දින ශ්‍රී ලංකා මහ බැංකුව වෙත අරමුදල් ආපසු ලබා දී ඇත.

#### 5. A@erd.gov.lk → Z@exportfinanceau.com

2026 ජනවාරි මස 07

රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් යොමු කරන ලද විද්‍යුත් තැපෑලකට අනුව අරමුදල් ශ්‍රී ලංකා මහ බැංකුවට ආපසු ලැබී නොමැති බව සඳහන් කර ඇත.

#### 6. Z@exportfinanceau.com → A@erd.gov.lk

2026 ජනවාරි මස 14

අතරමැදි බැංකුවෙන් ආපසු ලබා දෙන ලෙස ඉල්ලා සිටි ඉන්වොයිසියක් සඳහා කරන ලද ගෙවීමක් සම්බන්ධයෙන් පසු විපරමක් ඉල්ලා සිටින ලදී. ගෙවීම තවදුරටත් ප්‍රමාද වුවහොත් අමතර පොලියක් සක්‍රීය කිරීමේ හැකියාව සඳහන් කර ඇත.

#### 7. A@erd.gov.lk → Z@exportfinanceau.com

2026 ජනවාරි මස 14

අරමුදල් ආපසු ලැබී ඇති බව ශ්‍රී ලංකා මහ බැංකුව විසින් තහවුරු කර ඇති බව සඳහන් කර ඇත. ඒ අනුව ඉන්වොයිසිය නැවත නිකුත් කරන ලෙස උපදෙස් දී ඇත.

#### 8. Z@exportfinanceau.com → A@erd.gov.lk

2026 ජනවාරි මස 15

සංශෝධිත ඉන්වොයිසිය යවා ඇත.

පෙර ගෙවීම් උත්සාහයන් දෙකකදී අසාර්ථක වූ ඇමරිකානු ඩොලර් 997,799.48 ක මුදල, 2026 ජනවාරි මස 20 වන දින එක්සත් ජනපදයේ බැංකු ගිණුමකට සාර්ථකව ගෙවා ඇත.

මේ අතරතුර, එක්ස්පෝර්ට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනය (Export Finance Australia) වෙත 2026 ජනවාරි මාසය වන විට ගෙවීමට නියමිතව තිබූ ආපසු ගෙවීම්වල දෙවන කොටසක් ද සකස් කර 2026 ජනවාරි මස 05 වන දින සාර්ථකව ගෙවා ඇත.

#### 9. F@erd.gov.lk → Z@exportfinanceau.com

2025 දෙසැම්බර් මස 22

2026 ජනවාරි මස 05 දිනට ගෙවිය යුතු ඉන්වොයිසිය පහක් ඉල්ලා ඇත.

#### 10. Z@exportfinanceau.com → F@erd.gov.lk

2025 දෙසැම්බර් මස 23

ද්විපාර්ශ්වික ගිවිසුම් පහක් සඳහා 2026 ජනවාරි මස 05 දිනට නියමිත පොලී ගෙවීම සඳහා ඉන්වොයිසිය පහ එවා ඇත.

දෙවන (2) ඊමේල් පණිවුඩ දාමය 2025 නොවැම්බර් 26 දින, එක්ස්පෝර්ට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනය වෙත යොමු කිරීමට නියමිත ගෙවීමක් ප්‍රතික්ෂේප වීමෙන් අනතුරුව, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ සහ ශ්‍රී ලංකා මහ බැංකු නිලධාරීන් අතර හුවමාරු වූ ඊමේල් සංවාදයයි.

#### 1. D@cbsl.lk → ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුවේ සේවකයෙකුගේ ඊමේල් ලිපිනය

2025 නොවැම්බර් 26

රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙන් ලැබුණු ඊමේල් පණිවුඩය ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුව වෙත යොමු කරන ලදී. එහි සඳහන් වූයේ ණය දෙන ආයතනයෙන්, සංශෝධිත ණය ආපසු ගෙවීමේ උපදෙස් ලැබී ඇති බවත් එම උපදෙස්වලට , එක්සත් අරාබි එමීර් රාජ්‍යයේ නව ප්‍රතිලාභියෙකු වෙත සිදු කළ යුතු ගෙවීමක් ද ඇතුළත් බවත්ය. එම ගෙවීම සිදු කළ හැකිද යන්න සහ අතරමැදි බැංකුවක් අවශ්‍ය ද යන්න පිළිබඳ අනුමැතිය හා මාර්ගෝපදේශ ඉල්ලා සිටින ලදී.

**2. ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුවේ සේවකයෙකුගේ ඊමේල් ලිපිනය. →D@cbsl.lk**

2025 නොවැම්බර් 26

ඉහත ඊමේල් පණිවුඩයට පිළිතුරු ලබාදුන් ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුව , ප්‍රතිලාභියාගේ ලිපිනය එක්ස්පෝර්ට් ඕනෑන්ස් ඕස්ට්‍රේලියා ආයතනයේ ලිපිනය නොවන බවත්, මෙම තත්ත්වය හේතුවෙන් ප්‍රතිලාභියාගේ බැංකුව විසින් මුදල් විශුද්ධීකරණය වැළැක්වීමේ අවශ්‍යතා ඇතුළු කරුණු සැලකිල්ලට ගනිමින්, ගෙවීම නැවතත් ප්‍රතික්ෂේප කිරීමට ඉඩ ඇති බව ද පෙන්වා දෙන ලදී. තවද, ආපසු ගෙවීම සඳහා ගිණුම් විස්තර යළි තහවුරු කර ගැනීම පිණිස ණය දෙන ආයතනය සමඟ සන්නිවේදනය කරන ලෙස උපදෙස් ලබා දෙන ලදී.

**3. D@cbsl.lk → G@pdmo.gov.lk**

2025 නොවැම්බර් 26

එක්සත් අරාබි එමීර් රාජ්‍යයේ ගිණුමකට ගෙවීමට නියමිත ඉන්වොයිසිය සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුව සිය සැකය යොමු කර ඇති බවත්, ඒ සම්බන්ධයෙන් අවශ්‍ය පියවර ගන්නා ලෙසත් ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුවේ අදාළ නිලධාරියා විසින් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත දැනුම් දෙන ලදී.

තෙවන ( 3 ) ඊමේල් පණිවුඩ දාමය 2025 නොවැම්බර් 25 සිට 2026 මාර්තු 23 දක්වා කාලය තුළ, විදේශ සම්පත් දෙපාර්තමේන්තුව සහ ණය දෙන ආයතනයේ බවට පෙනී සිටි විද්‍යුත් තැපැල් ලිපින අතර හුවමාරු වූ ඊමේල් සංවාදයයි.

**1. A@erd.gov.lk → Z@exportfinance.gov.au**

2025 නොවැම්බර් 25

ප්‍රතිලාභියාගේ තොරතුරු වැරදි වීම හේතුවෙන්, ගෙවීම ප්‍රතික්ෂේප වී ඇති බව පැහැදිලි කරමින්, යාවත්කාලීන කළ ඉන්වොයිසි විදේශ සම්පත් දෙපාර්තමේන්තුවේ අදාළ නිලධාරියා වෙත එවන ලෙස ඉල්ලා සිටින ලදී.

**2. Z@exportfinance.gov.au → A@erd.gov.lk & B@erd.gov.lk**

2025 නොවැම්බර් 26

නිවැරදි කරන ලද බැංකු තොරතුරු ඇතුළත් සංශෝධිත ඉන්වොයිසි එවා ඇත.

**3. B@erd.gov.lk → Z@exportfinance.gov.au**

2025 නොවැම්බර් 27

බැංකු තොරතුරු නිවැරදි ලෙස ලැබී ඇති බව තහවුරු කරන ලදී.

**4. Z@exportfinance.gov.au → B@erd.gov.lk**

2025 දෙසැම්බර් 3 – 16

ගෙවීම සිදු කිරීමට අපේක්ෂිත දිනය කවදාදැයි ණය හිමියා විසින් විමසන ලදී.

**5. B@erd.gov.lk → Z@exportfinance.gov.au**

2025 දෙසැම්බර් 19

ඊට පිළිතුරු වශයෙන්, ගෙවීම ජනවාරි මස පළමු සතිය තුළ ප්‍රේෂණය කිරීමට අපේක්ෂා කරන බව විදේශ සම්පත් දෙපාර්තමේන්තුවේ නිලධාරියා විසින් සඳහන් කරන ලදී. ප්‍රමාදය දිව්වා සුළු කුණාටුව හේතුවෙන් ඇති වූ සම්පත් සීමාකිරීම් නිසා සිදු වූ බව සඳහන් කරන ලදී. එමෙන්ම ද්විපාර්ශ්වික ගිවිසුම් යටතේ, 2026 ජනවාරි 5 වන දිනට ගෙවීමට නියමිත සියලුම ඉන්වොයිසි, මේ අතරතුර යොමු කරන ලෙස ඉල්ලා සිටින ලදී.

**6. Z@exportfinance.gov.au → B@erd.gov.lk**

2025 දෙසැම්බර් 23

2026 ජනවාරි 5 දිනට ගෙවීමට නියමිත ඉන්වොයිසි පහ (5) යොමු කරන ලදී.

**7. Z@exportfinance.gov.au → B@erd.gov.lk**

2026 ජනවාරි 12 – 20

මෙම කාලසීමාව තුළ හුවමාරු වූ විද්‍යුත් තැපැල් පණිවිඩ මගින්, ගෙවීමට නියමිතව ඇති සියලුම හිඟ ඉන්වොයිසිවල ගෙවීම් තත්ත්වය පිළිබඳ යාවත්කාලීන තොරතුරු ඉල්ලා සිටින ලද අතර, ප්‍රමාද වූ ගෙවීම් සම්බන්ධ කරුණ, අධ්‍යක්ෂ මණ්ඩලය වෙත ඉදිරිපත් කිරීමට සිදුවිය හැකි බවට අනතුරු ඇඟවීමක් ද ජනවාරි 20 දින සිදු කරන ලදී.

**8. B@erd.gov.lk → Z@exportfinance.gov.au**

2026 ජනවාරි 20

ඊට පිළිතුරු වශයෙන්, එක්ස්පෝට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනයට ගෙවීමට ඇති , ප්‍රමාද වූ ගෙවීම් සම්බන්ධයෙන් ඉදිරියට ගත යුතු ක්‍රියාමාර්ග පිළිබඳව, 2026 පෙබරවාරි 2 දින වන විට රාජ්‍ය ණය කළමනාකරණ කාර්යාලය සහ කැබිනට් මණ්ඩලය විසින් තීරණයකට එළඹෙනු ඇති බවට විදේශ සම්පත් දෙපාර්තමේන්තුවේ නිලධාරියා විසින් සහතික කරන ලදී.

**9. A@erd.gov.lk → Z@exportfinance.gov.au**

2026 පෙබරවාරි 2

හිඟව පවතින ගෙවීම් පියවීම සඳහා කැබිනට් මණ්ඩලය විසින් අනුමත කරන ලද බවට සඳහන් කාලසටහනක් ඇතුළත් විස්තරාත්මක ඊ මේල් පණිවිඩය.

- 2025 නොවැම්බර් 15 දිනට ගෙවිය යුතුව තිබූ ඉන්වොයිසි 5ක්, 2026 මාර්තු 16 දින ගෙවීමට නියමිතය.
- 2026 ජනවාරි 5 දිනට ගෙවිය යුතුව තිබූ ඉන්වොයිසි 5ක්, 2026 අප්‍රේල් 6 දින ගෙවීමට නියමිතය.

**10. Z@exportfinance.gov.au → A@erd.gov.lk**  
**2026 පෙබරවාරි 16**

ඉහත සඳහන් ගෙවීම් කාලසටහන පිළිගන්නා ලදී.

**11. Z@exportfinance.gov.au → A@erd.gov.lk**  
**2026 පෙබරවාරි 19**

ගෙවීම සිදුකිරීම සඳහා නැවත කාලසටහන්ගත කරන ලද මුළු මුදල් ප්‍රමාණයන් තහවුරු කරන ලදී.

- ඇමෙරිකානු ඩොලර් 2,089,640.99 — 2026 මාර්තු 16 දින ගෙවීමට නියමිතය.
- ඇමෙරිකානු ඩොලර් 420,211.96 — 2026 අප්‍රේල් 6 දින ගෙවීමට නියමිතය.

**12. B@erd.gov.lk → Z@exportfinance.gov.au**  
**2026 මාර්තු 14 – 16**

ගෙවීමේ ක්‍රියාවලිය සිදුවෙමින් පවතින බව සඳහන් කළ අතර, සම්පූර්ණ ගෙවීම්/මුදාහැරීම් තත්ත්වය සම්බන්ධයෙන් යාවත්කාලීන තොරතුරු ලබා දීම ලබා දීම සඳහා 2026 මාර්තු 20 වන සිකුරාදා දක්වා කාලය ලබා දෙන ලෙස ඉල්ලා සිටින ලදී.

**13. B@erd.gov.lk → Z@exportfinance.gov.au**  
**2026 මාර්තු 15 – 16**

ගෙවීම් පිළිබඳ යාවත්කාලීන තොරතුරු ණය හිමියා විසින් අඛණ්ඩව ඉල්ලා සිටින ලදී.

**14. Z@exportfinance.gov.au → B@erd.gov.lk + A@erd.gov.lk**  
**2026 මාර්තු 21**

නව ගෙවීම් කාලසටහනට අනුව ආපසු ගෙවීම ලැබී නොමැති බවට පැමිණිලි කරන ලදී.

**15. A@erd.gov.lk → විදේශ සම්පත් දෙපාර්තමේන්තුවේ විවිධ නිලධාරීන්**  
**2026 මාර්තු 23**

එකම සම්බන්ධතා ස්ථානය (Contact Point) වෙත ණය හිමියාගේ වෙනස් විද්‍යුත් තැපැල් ලිපින තුනකින් ඊමේල් පණිවුඩ ලැබී ඇති බව දැනුම් දෙන ලදී.

මෙම අවසන් විද්‍යුත් තැපැල් පණිවිඩය, එක්ස්පෝට් ෆිනෑන්ස් ඕස්ට්‍රේලියා ආයතනය වෙත සිදු කළ යුතු ණය ආපසු ගෙවීම් සම්බන්ධයෙන් ගැටලුවක් පවතින බව, විදේශ සම්පත් දෙපාර්තමේන්තුවේ නිලධාරීන් අවබෝධ කරගත් අවස්ථාව ලෙස පෙනී යයි. එම දැනගැනීමෙන් පසුව, අදාළ පියවර ගැනීම් සහ විමර්ශන ක්‍රියාමාර්ග ආරම්භ විය.

**2026 මාර්තු 24 වන දින,** විදේශ සම්පත් දෙපාර්තමේන්තුවේ අධ්‍යක්ෂ ජනරාල් විසින්, අතුරුදන් වූ ගෙවීම් සම්බන්ධයෙන් ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර කණ්ඩායම වෙත ලිපියක් යොමු කරන ලදී. එහිදී, සැක කටයුතු සහිතව අපරාධයක් සම්බන්ධයෙන් **2026 ජනවාරි 9 සහ 2026 මාර්තු 7 යන දිනවල** යොමු කළ පෙර ලිපි පිළිබඳවද සඳහන් කරන ලදී. තවද, මූල්‍ය ගනුදෙනු වාර්තා කිරීමේ පනත යටතේ මෙම කරුණ සම්බන්ධයෙන් තොරතුරු ඉල්ලා මූල්‍ය බුද්ධි ඒකකය විසින් කරන ලද ඉල්ලීමට ප්‍රතිචාර වශයෙන්, විදේශ සම්පත් දෙපාර්තමේන්තුවේ අධ්‍යක්ෂ ජනරාල් විසින් **2026 අප්‍රේල් 3 වන දින** අදාළ විස්තර ඇතුළත් ලිපියක් මූල්‍ය බුද්ධි ඒකකය වෙත යොමු කරන ලදී.

**2026 මාර්තු 24 වන දින,** “රීමේල් මගින් ලැබුණු වංචනික ගෙවීම් උපදෙස්වල අවදානම සහ ඕස්ට්‍රේලියාව වෙත සිදු කළ අතුරුදන් වූ ගෙවීම්” සම්බන්ධයෙන් විමර්ශනය කිරීම සඳහා තාක්ෂණික විමර්ශන කමිටුවක් පත් කරන ලදී. එම කමිටුව, භාණ්ඩාගාර නියෝජ්‍ය ලේකම්. ඒ. එන් හසුගල, භාණ්ඩාගාර නියෝජ්‍ය ලේකම්. එස්.එස්. මුදලිගේ, ජාතික සැලසුම් දෙපාර්තමේන්තුවේ අධ්‍යක්ෂ ජනරාල්. කේ.ටී. අයි ප්‍රේමරත්න, අතිරේක අධ්‍යක්ෂ ජනරාල් (නීති කටයුතු). ඒ.කේ.ඩී.ඩී.ඩී අරන්දර, තොරතුරු තාක්ෂණ කළමනාකරණ දෙපාර්තමේන්තුවේ සහකාර අධ්‍යක්ෂ. ඊ.ඩී ශිරන්ත යන නිලධාරීන්ගෙන් සමන්විත විය. කමිටුව විසින් **2026 අප්‍රේල් 10 වන දින** සිය විමර්ශන වාර්තාව ඉදිරිපත් කරන ලදී. එම වාර්තාවේ අනාවරනයන් මත පදනම්ව, **2026 අප්‍රේල් 17 වන දින** සේවකයින් සිව් දෙනෙකුගේ සේවය අත්හිටුවන ලදී.

පවතින මුදල් රෙගුලාසි 135 අනුව ණය ආපසු ගෙවීම් සම්බන්ධ වගකීම් පිළිබඳව මුදල් අමාත්‍යාංශය තුළ විධිමත් බලතල පැවරීමේ ක්‍රියාවලියක් නොතිබූ බව රාජ්‍ය මුදල් පිළිබඳ කාරක සභාව විසින් අනාවරණය කොට ගෙන තිබීම සැලකිල්ලට ගත යුතු වැදගත් කරුණකි. “**2026 අප්‍රේල් 30 වන දින පැවති සාකච්ඡාවෙන් පසුව** රාජ්‍ය මුදල් පිළිබඳ කාරක සභාව විසින් කළ විමසීමට ප්‍රතිචාර දක්වමින්, ණය ආපසු ගෙවීමේ ක්‍රියාවලිය, අභිමතය මත සිදුකරන වියදම් අයිතමයක්<sup>9</sup> නොවන හෙයින් එය පෙර සිටම පවතින මුදල් රෙගුලාසි වලට යටත් වී නොමැති බව භාණ්ඩාගාර ලේකම්වරයා **2026 ජූනි 23 දිනැති ලිපියකින්** සඳහන් කළේ ය”. මුදල් අමාත්‍යාංශය තුළ අවසන් ගෙවීම් අනුමැතිය ලබාදීමේ කාර්යය පෙර සිටම සිදු කර ඇත්තේ, ණය සේවාකරණ කාර්යයට බලය පැවරී ඇති අධ්‍යක්ෂවරයා විසිනි. එය මීට කලින් විදේශ සම්පත් දෙපාර්තමේන්තුව යටතේ, වර්තමානයේ රාජ්‍ය ණය කළමනාකරණ කාර්යාලය යටතේ ක්‍රියාත්මක වී ඇත. කෙසේ වෙතත් එම අවසන් අනුමැතිය ලබාදීමේ ක්‍රියාවලියට පෙර, වඩා ජ්‍යෙෂ්ඨ නිලධාරීන් විසින් කිසිදු සහායක ක්‍රියාවලියක් සිදු කර නොතිබීම, දුර්වල අභ්‍යන්තර පාලන ක්‍රමවේදයන් පවතින බව පෙන්නුම් කරයි.

## 5. එම සිද්ධි මාලාවෙන් පසුව, ක්‍රියාවලීන් වැඩිදියුණු කිරීම සඳහා මුදල් අමාත්‍යාංශය විසින් ගනු ලැබූ පියවර

මුදල් අමාත්‍යාංශ වාර්තාවට අනුව, එම සිද්ධීම් මාලාවෙන් පසුව නැවත එවැනි සිද්ධීම් ඇතිවීමේ අවදානම අවම කිරීම සහ විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය වැඩිදියුණු කිරීම සඳහා අමාත්‍යාංශය විසින් පියවර කිහිපයක් ගෙන ඇත<sup>10</sup>.

එම ප්‍රධාන පියවරවල සාරාංශය පහත දැක්වේ:

- ණය සේවාකරණය සම්බන්ධ ණය හිමියන් සමඟ සම්බන්ධීකරණ කාර්යය විදේශ සම්පත් දෙපාර්තමේන්තුවෙන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ වෙත සම්පූර්ණයෙන්ම පැවරීම.

<sup>9</sup> ඇමුණුම 9- 2026 ජූනි 23 දිනැති, ණය ආපසු ගෙවීම් කාර්යයන් සඳහා බලය පැවරීම සම්බන්ධයෙන් භාණ්ඩාගාර ලේකම්වරයා විසින් රාජ්‍ය මුදල් පිළිබඳ කාරක සභාව වෙත යොමු කරන ලද ලිපිය.

<sup>10</sup> අමාත්‍යාංශය විසින් ගනු ලැබූ ක්‍රියාමාර්ග පිළිබඳ සවිස්තරාත්මක විස්තර ඇමුණුම 2 හි ඉදිරිපත් කර ඇත.



- රාජ්‍ය තාන්ත්‍රික මාර්ගද ඇතුළත්ව අදාළ ණය දෙන්නන් සමඟ විධිමත් සන්නිවේදන මාර්ග ස්ථාපිත කිරීම තුළින් ණය දෙන්නන් විසින් ඉදිරිපත් කරන තොරතුරු අවම වශයෙන් මාර්ග දෙකක් හරහා සත්‍යාපනය කිරීම සහතික කිරීම.
- පළමු ගෙවීමට අවම වශයෙන් දින 10කට පෙර, මාසික ණය සේවාකරණ පුරෝකථනය, ගෙවීම් අනුමැතිය සඳහා භාණ්ඩාගාර ලේකම්වරයා වෙත ඉදිරිපත් කිරීම.
- භාණ්ඩාගාර මෙහෙයුම් දෙපාර්තමේන්තුව විධිමත් ලෙස සත්‍යාපන ක්‍රියාවලියට ඇතුළත් කර ඇති අතර, එය කළමනාකරණය කරන ඒකාබද්ධ අරමුදල් ගිණුම්වලින් මාසික ණය ආපසු ගෙවීම් සඳහා මුදල් වෙන් කිරීමේ අවසරය ලබා දෙන්නේ, සත්‍යාපන ක්‍රියාවලිය තුළ නිවැරදි තොරතුරු තහවුරු වී ඇත්නම් පමණි.
- සංචිත නොවන කළමනාකරණ පද්ධතියේ පවතින බැංකු තොරතුරු නිසි අවසරය සහ සත්‍යාපනයකින් තොරව වෙනස් කිරීම සීමා කිරීම.
- මුදල් අමාත්‍යාංශයේ සමස්ත සයිබර් ආරක්ෂාව ශක්තිමත් කිරීම සඳහා සහ විදේශ සම්පත් දෙපාර්තමේන්තුවේ තොරතුරු තාක්ෂණ පද්ධතිවල හඳුනාගත් අඩුපාඩු විසඳීම සඳහා, ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර අංශය සහ ජාතික සයිබර් ආරක්ෂක මෙහෙයුම් මධ්‍යස්ථානය ඇතුළුව ඩිජිටල් ආර්ථික අමාත්‍යාංශයේ සහාය ලබා ගනිමින් පවතී.

මුදල් අමාත්‍යාංශය තුළ අභ්‍යන්තර පාලන ක්‍රමවේද ස්ථාපිත කිරීම සහ ශක්තිමත් කිරීම මෙන්ම මූලික සයිබර් ආරක්ෂක ක්‍රියාමාර්ග සහතික කිරීම හා මෙම පියවරයන් සම්බන්ධ වේ.

මෙවැනි පියවරයන් මූලික ආරක්ෂක ක්‍රමවේද ලෙස ක්‍රියාත්මක විය යුතුව තිබුණි. මෑතකාලීන සිදුවීම් මගින්, මෙම අත්‍යවශ්‍ය මූලික පාලන ක්‍රියාමාර්ග ක්‍රියාත්මක කිරීමේ තීරණාත්මක වැදගත්කම අවධාරණය කර ඇත.

## 6. විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය තුළ ශ්‍රී ලංකා මහ බැංකුවේ වගකීම් පිළිබඳව ශ්‍රී ලංකා මහ බැංකුවේ සහ මුදල් අමාත්‍යාංශයේ පරස්පර මත

විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය සහ රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත වගකීම් පැවරීමේ සංක්‍රාන්ති ක්‍රියාවලිය තුළ ශ්‍රී ලංකා මහ බැංකුවේ වගකීම සම්බන්ධයෙන් 2026 ජුනි 8 වැනි දින පැවැති සාකච්ඡාවලදී මතු වූ විවිධ අදහස් සැලකිල්ලට ගනිමින්, මුදල් අමාත්‍යාංශයේ මූලික වාර්තාවට ප්‍රතිචාර වශයෙන් ශ්‍රී ලංකා මහ බැංකුව විසින් වාර්තා දෙකක් ඉදිරිපත් කරන ලදී. මහ බැංකුවේ වගකීම්වලට අදාළ නිශ්චිත කරුණු පිළිබඳව වැඩිදුර පැහැදිලි කිරීමක් ලබාදෙන ලෙස කාරක සභාව විසින් නීතිපතිවරයාගෙන් ඉල්ලා සිටින ලදී.

මුදල් ගනුදෙනු වාර්තා කිරීමේ පනත (Financial Transactions Reporting Act – FTRA) යටතේ මුදල් විශුද්ධීකරණය වැළැක්වීම (Anti-Money Laundering – AML) සම්බන්ධ කටයුතු පිළිබඳව ශ්‍රී ලංකා මහ බැංකුව වඩාත් සුපරීක්ෂාකාරීව කටයුතු කරමින්, අවශ්‍ය ක්‍රියාකාරී පියවර ගත යුතු බව මුදල් අමාත්‍යාංශයේ මතය විය. රජයේ බැංකුකරු ලෙස තම කාර්යභාරය ඉටු කිරීමේදී මුදල් ගනුදෙනු වාර්තා කිරීමේ පනත (Financial Transactions Reporting Act – FTRA) යටතේ ශ්‍රී ලංකා මහ බැංකුවට කිසිදු නීතිමය වගකීමක් නොමැති බව ශ්‍රී ලංකා මහ බැංකුවේ (CBSL) මතය විය. මේ සම්බන්ධව කාරක සභාව විසින් ද ගැඹුරින් විමර්ශනය කර ඒ සම්බන්ධයෙන් නීතිපති දෙපාර්තමේන්තුවේ ද උපදෙස් ද ලබා ගන්නා ලදී. වත්මන් නෛතික තත්ත්වය පිළිබඳ නීතිපතිවරයාගේ අර්ථ නිරූපණය බොහෝ දුරට ශ්‍රී ලංකා මහ බැංකුවේ (CBSL) මතය සමඟ අනුකූල වන අතර, අනාගතයේදී එවැනි වගකීමක් ස්ථාපිත කිරීම සඳහා ප්‍රතිපත්තිමය තීරණ ගැනීමේ අවකාශය පවතින බව ද එම අර්ථ නිරූපණයෙන් පැහැදිලි වේ.

2025 නොවැම්බර් මාසයේදී වංචනික ඉන්වොයිසි සම්බන්ධ ගෙවීම් සඳහා රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ නිලධාරීන් විසින් ප්‍රමිතිගත පියවීම් උපදෙස් (Standard Settlement Instructions (SSI)) සකස් කරන ලද කාලසීමාව තුළ, ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුවේ (PDD) නිලධාරීන් විසින් එම ක්‍රියාවලිය අඛණ්ඩව අධීක්ෂණය කරන ලද බව මුදල් අමාත්‍යාංශය විසින් පෙන්වා දෙන ලදී. 2025 ඔක්තෝබර් 24 වන දින වන විට, සංචිත නොවන කළමනාකරණ (Non-Reserve Management – NRM) පද්ධතියේ පාලනය රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) වෙත පැවරීමේ කටයුතු සහ රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ (PDMO) නිලධාරීන් සඳහා ප්‍රමිතිගත පියවීම් උපදෙස් (Standard Settlement Instructions (SSIs)) සකස් කිරීම රාජ්‍ය ණය දෙපාර්තමේන්තුව විසින් සම්පූර්ණ කර තිබූ බැවින්, 2025 නොවැම්බර් මාසයේදී වංචනික ගනුදෙනු සිදු වූ අවස්ථාවේදී ඒ සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකුවට කිසිදු වගකීමක් නොපැවති බව ශ්‍රී ලංකා මහ බැංකුවේ මතය විය.

ජාත්‍යන්තර අරමුදල් හුවමාරු ක්‍රියාවලීන් සහ මුදල් විශුද්ධීකරණය වැළැක්වීම සම්බන්ධ කරුණු පිළිබඳව රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ කාර්ය මණ්ඩලයට ප්‍රමාණවත් අවබෝධයක් නොතිබූ අතර, එහි ප්‍රතිඵලයක් ලෙස එවැනි කරුණු සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකුවේ කාර්ය මණ්ඩලය විසින් සපයන ලද සීමිත තොරතුරු මත පමණක් ක්‍රියා කිරීමට ඔවුන්ට සිදු වූ බව මුදල් අමාත්‍යාංශය විසින් පැහැදිලි කරන ලදී. ගෙවීම් සත්‍යාපනය සඳහා මුදල් අමාත්‍යාංශය තුළ පවතින අභ්‍යන්තර පාලන පද්ධතීන් අක්‍රිය වූ අවස්ථාවක, ශ්‍රී ලංකා මහ බැංකුවට තම ගෙවීම් ක්‍රියාවලිය තුළින් එම සත්‍යාපනය තහවුරු කළ නොහැකි බව ශ්‍රී ලංකා මහ බැංකුව විසින් පැහැදිලි කරන ලදී. තවද, එවැනි තත්ත්වයක් යටතේ සයිබර් අපරාධවලට සම්බන්ධ වංචනික ක්‍රියා වැළැක්වීමට ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව පවා අසමත් විය හැකි බව ද එහිදී සඳහන් කර ඇත.

2026 ජුනි 25 දිනැති ලිපිය මගින් දැනුම් දී ඇති නීතිපතිවරයාගේ මතයට අනුව, ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව විසින් යම් කාර්යයක් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත නිසි පරිදි භාර දීමෙන් අනතුරුව, එම කාර්යය සම්බන්ධ වගකීම ඉන් ඉදිරියට රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත පැවරෙන බව අවධාරණය කර ඇත.

## 7. නිගමන

- I. සයිබර් අපරාධයකට සම්බන්ධ වංචනික ක්‍රියාවක් පැහැදිලිවම සිදුවී ඇති අතර, ඒ හේතුවෙන් ඇමරිකානු ඩොලර් මිලියන 2.5ක මහජන අරමුදල් වංචා සහගත ලෙස නැති වී ඇත. සයිබර් අපරාධයකට සම්බන්ධ මෙම වංචාව සිදු කිරීමේදී අදාළ ආයතන තුළ කිසියම් අභ්‍යන්තර කුමන්ත්‍රණයක් සිදුවී ඇත්ද යන්න අපරාධ විමර්ශන ඇතුළු නීතිය ක්‍රියාත්මක කිරීමේ ක්‍රියාවලිය මගින් තීරණය කළ යුතුය. මෙය අදාළ නිලධාරීන්ගේ ක්‍රියාකලාපය නොදැනුවත්කම, අකාර්යක්ෂමතාව හෝ නොසැලකිලිමත්භාවය මත පමණක් පදනම් වූවක්ද යන්න ද මෙහිදී තහවුරු කරගත හැකි වනු ඇත.
- II. රජයේ මුදල් පිළිබඳ කාරක සභාවට (COPF) අදාළ කාර්යය වනුයේ සයිබර් අපරාධයකට සම්බන්ධ වංචනික සිද්ධිය එහි අධීක්ෂණ කාර්යභාරයට අදාළව සලකා බැලීම සහ පාලනමය ක්‍රියා පටිපාටිමය හා මෙහෙයුම් අංශ හරහා පවතින අවදානම් වර්ධනය වීමට බලපෑ රාජ්‍ය මූල්‍ය කළමනාකරණයේ අඩුපාඩු මොනවාදැයි හඳුනා ගැනීම වේ.

අ. සමස්තයක් ලෙස පරිපාලනමය වශයෙන් භාණ්ඩාගාර ලේකම්වරයා සහ ශ්‍රී ලංකා මහ බැංකු අධිපතිවරයාගේ මට්ටමින් ජේෂ්ඨ නිලධාරීන් ඇතුළු අඩුපාඩු සම්බන්ධයෙන් වගකිව යුතු වේ.

- i. අලුතින් පිහිටුවන ලද රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත කාර්යයන් පැවරීමේ මාස 18ක සංක්‍රාන්ති ක්‍රියාවලිය සඳහා පැහැදිලි මාර්ගෝපදේශ සහ කාර්යය නියමයන් සහිත පූර්ව අවබෝධතා ගිවිසුමක් පැවතියේ නම්, එම සංක්‍රාන්ති ක්‍රියාවලිය සාර්ථකව ක්‍රියාත්මක කිරීමේ වගකීම සම්බන්ධයෙන් භාණ්ඩාගාර ලේකම්වරයා සහ ශ්‍රී ලංකා මහ බැංකු අධිපතිවරයා අතර ඇති වූ මතභේද මඟහරවාගත හැකිව තිබුණි. එවැනි ගිවිසුමක ප්‍රමාණවත් පුහුණුවක් ලබා දීම, අනුගමනය කළ යුතු කාලරාමුව සහ ඒවායේ ප්‍රගතිය මැනීම සඳහා ප්‍රධාන කාර්ය සාධන දර්ශක ඇතුළත් කළ හැකිව තිබුණි. අවබෝධතා ගිවිසුමක් නොතිබීම සහ මෙම සිදුවීම් අතර සෘජු සම්බන්ධතාවක් කාරක සභාවට තහවුරු කළ නොහැකි වුවද, එවැනි ගිවිසුමක් විධිමත් ලෙස ස්ථාපිත කර තිබුණේ නම්, එම සංක්‍රාන්ති කාලසීමාව තුළ සම්බන්ධ වූ සියලුම නිලධාරීන්ගේ වගකීම් පැහැදිලිව නිර්වචනය කිරීමටත්, මෙවැනි සිදුවීම් වළක්වා ගැනීමටත් හැකිව තිබූ බව එහි අදහසයි.
  
- ii. 2026 මුල් භාගයේදී, සයිබර් අපරාධයකට සම්බන්ධ මෙම වංචනික ක්‍රියාව පිළිබඳ කිසිදු තොරතුරක් අනාවරණය වීමට පෙර, විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලියේදී මුදල් අමාත්‍යාංශය සහ ශ්‍රී ලංකා මහ බැංකුව අතර පවතින සම්බන්ධීකරණ යාන්ත්‍රණ පිළිබඳව සාකච්ඡාවක් පැවැත්වීමට රජයේ මුදල් පිළිබඳ කාරක සභාව විසින් ඉල්ලීමක් සිදුකර ඇත. මෙම ඉල්ලීමට ප්‍රතිචාර දක්වමින්, 2026 අප්‍රේල් 4 දිනැතිව රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද සම අත්සන්-සහිත ලිපියක් මගින් භාණ්ඩාගාර ලේකම්වරයා සහ මහ බැංකු අධිපතිවරයා විසින් සම්බන්ධීකරණය සඳහා දැනට පවතින යාන්ත්‍රණ ප්‍රමාණවත් බව තහවුරු කර ඇත<sup>11</sup>. කෙසේ වෙතත්, පසුව සිදු කරන ලද සමාලෝචනයේදී, ණය ආපසු ගෙවීම සම්බන්ධ සංක්‍රාන්ති ක්‍රියාවලිය ඇතුළුව ආයතන අතර සම්බන්ධීකරණය වැඩිදියුණු කිරීම සඳහා සැලකිය යුතු අවස්ථා පැවති බව අනාවරණය විය.
  
- iii. ණය ආපසු ගෙවීමේ ක්‍රියාවලියට අදාළ කාර්යයන් නීතිපතා පැවරීමේ ක්‍රමවේදයක් මුදල් අමාත්‍යාංශය තුළ නොපවතින බවත්, එය අභිමතානුසාරී වියදම් අයිතමයක් නොවන බැවින් දැනට පවතින මූල්‍ය රෙගුලාසිවල විෂය පථයට එය ඇතුළත් නොවන බවත් 2026 ජුනි 23 දිනැති ලිපිය මගින් භාණ්ඩාගාර ලේකම්වරයා විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත දැනුම් දී ඇත. රාජ්‍ය මූල්‍ය පාලනය සඳහා අදාළ වන මූල්‍ය රෙගුලාසි කාලීන අවශ්‍යතාවලට අනුව සමාලෝචනය කර යාවත්කාලීන කිරීමේ වැදගත්කම මෙයින් අවධාරණය කෙරේ. එමෙන්ම, රාජ්‍ය මූල්‍ය ක්‍රියාවලීන් පාලනය කරන මූල්‍ය රෙගුලාසි කඩිනමින් සංශෝධනය කිරීමේ සහ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය පිළිබඳ පුළුල් සමාලෝචනයක් සිදු කිරීමේ අවශ්‍යතාවය ද මෙයින් පැහැදිලි වේ.

<sup>11</sup> ඇමුණුම 10 – 2026 අප්‍රේල් 04 දිනැතිව භාණ්ඩාගාර ලේකම්වරයා සහ ශ්‍රී ලංකා මහ බැංකු අධිපතිවරයා විසින් සම- අත්සන් කරන ලද-, භාණ්ඩාගාරය සහ ශ්‍රී ලංකා මහ බැංකුව අතර සම්බන්ධීකරණ යාන්ත්‍රණවල ප්‍රමාණවත් බව දන්වමින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත යොමු කරන ලද ලිපිය

ආ. ක්‍රියා පටිපාටික මට්ටමින්, විදේශ සම්පත් දෙපාර්තමේන්තුවේ සහ රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ අධ්‍යක්ෂ ජනරාල්වරුන් විසින් කරුණු කිහිපයක් සම්බන්ධයෙන් රාජකාරි පැහැර හැරීම් සිදුවී ඇති බව නිරීක්ෂණය කර ඇත.

i. ණය ගිවිසුම්වලට අදාළව ණයහිමියන් විසින් ඉදිරිපත් කරන ලද ඉන්වොයිසි සත්‍යාපනය කිරීම සඳහා ප්‍රමාණවත් අභ්‍යන්තර පාලන ක්‍රමවේදයක් ස්ථාපිත කිරීමට සහ සත්‍යාපිත සන්නිවේදන මාර්ග සහතික කිරීමට ඔවුන් අපොහොසත් වී ඇත. මෙම මූලික පරීක්ෂණ ක්‍රියාමාර්ග නිසි පරිදි ක්‍රියාත්මක කර තිබුණේ නම්, සයිබර් අපරාධයකට සම්බන්ධ මෙම වංචනික ක්‍රියාව වළක්වා ගත හැකිව තිබූ බව පැහැදිලිය.

ii. තීරණාත්මක තොරතුරු තාක්ෂණ පද්ධති ප්‍රමාණවත් පරිදි යාවත්කාලීන කර පවත්වාගෙන යාම සහ ඒවා නිසි පරිදි ක්‍රියාත්මක වන බව සහතික කිරීම සඳහා ඔවුන් අපොහොසත් වී ඇත.

ඇ. මෙහෙයුම් මට්ටමින්, විදේශ සම්පත් දෙපාර්තමේන්තුවේ, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ සහ රාජ්‍ය ණය දෙපාර්තමේන්තුවේ මධ්‍යම මට්ටමේ නිලධාරීන් විසින් ප්‍රමාණවත් සැලකිල්ලක් දැක්වීමට අපොහොසත් වී ඇති අතර, ඔවුන්ගේ රාජකාරි ඉටු කිරීමේදී මනා වෘත්තීය විනිශ්චයකින් යුතු වූ බව සහතික කිරීමටද අපොහොසත් වී ඇත.. :මෙය පහත සඳහන් කරුණු මගින් පැහැදිලි වේ

i. විදේශ සම්පත් දෙපාර්තමේන්තුවේ නිලධාරීන් විසින් ඔවුන් සමඟ සන්නිවේදනය සඳහා භාවිත කළ විද්‍යුත් තැපෑල ලිපිනය වසම් නාම (domain names) සත්‍ය හා අනුකූල බව තහවුරු කිරීමට අපොහොසත් වී තිබුණි.

ii. ආයතන අතර සංක්‍රාන්ති ක්‍රියාවලිය සිදුවෙමින් පැවති අවස්ථාවේදී, ණයහිමියන් සමඟ සිදු කරන ලද විද්‍යුත් තැපෑල සන්නිවේදනයන් සම්බන්ධයෙන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි සිටින තම සමාන්තර නිලධාරීන් විද්‍යුත් තැපෑල (email) වෙත සම්බන්ධ කර ගැනීමට (CC) විදේශ සම්පත් දෙපාර්තමේන්තුවේ නිලධාරීන් අපොහොසත් වී ඇත.

iii. විදේශ සම්පත් දෙපාර්තමේන්තුවේ තොරතුරු තාක්ෂණ නිලධාරීන් විසින් එහි තොරතුරු තාක්ෂණ පද්ධතිවල ශක්තිමත්භාවය සහතික කිරීමට අපොහොසත් වී ඇත.

iv. 2025 නොවැම්බර් මාසයේදී විදේශීය නියෝජිත බැංකුව විසින් ශ්‍රී ලංකා මහ බැංකුවේ මුදල් දෙපාර්තමේන්තුවේ අවධානයට යොමු කර තිබූ සිදු විය හැකි මුදල් විශුද්ධිකරණය වැළැක්වීම සම්බන්ධ ගැටලු / අවදානම් සම්බන්ධයෙන්, ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුවේ ජ්‍යෙෂ්ඨ නිලධාරීන් වෙත නැවත නැවතත් අවධාරණය කර තිබුණ ද, ආයතන අතර පැවැති සංක්‍රාන්ති කාලය තුළ රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි

කණ්ඩායමේ අත්දැකීම් සීමිත බව දැන සිටියදීත්, ශ්‍රී ලංකා මහ බැංකුවෙහි රාජ්‍ය ණය දෙපාර්තමේන්තුවේ නිලධාරීන් විසින් මුදල් විශුද්ධීකරණය වැළැක්වීම සම්බන්ධ ගැටලු පිළිබඳව දැනුවත් කිරීමක් සිදු කර නොතිබුණි.

III. සංක්‍රාන්ති සමයේදී දීර්ඝ කාලයක් පුරා නැවත නැවතත් වංචනික ගනුදෙනු සිදු වීමට හේතු වූ ණය ආපසු ගෙවීමේ ක්‍රියාවලියේ පද්ධතිමය අසාර්ථකත්වයන් මෙම වාර්තාවෙන් හඳුනාගෙන ඇත. කෙසේ වෙතත්, සයිබර් අපරාධවලට සම්බන්ධ මෙම වංචාවට සම්බන්ධ මෙහෙයුම් අඩුපාඩු හේතුවෙන් මුදල් අමාත්‍යාංශයේ මධ්‍යම මට්ටමේ සේවකයින් හතර දෙනෙකු පමණක් වැඩ තහනමට ලක් කර ඇති බව කාරක සභාව වෙත දන්වා ඇත. මෙම සේවකයින් හතර දෙනාගෙන් එක් අයෙකුගේ හදිසි මරණය සැබවින්ම ඉතාමත් අවාසනාවන්ත සිදුවීමකි. පුද්ගලික වගකීම සම්බන්ධයෙන් තීරණයකට එළඹිය යුතු නම්, එය මෙම වාර්තාවේ අවසන් නිගමන සහ දැනට සිදුවෙමින් පවතින අපරාධ සම්බන්ධ විමර්ශනවල ප්‍රතිඵල මත පදනම්ව සිදු කළ යුතුයි.

IV. සයිබර් අපරාධයකට සම්බන්ධ මෙම වංචනික ක්‍රියාවෙන් අනතුරුව, නැවත එවැනි සිදුවීම් ඇතිවීම වැළැක්වීම සහ අනාගත අවදානම් අවම කිරීම සඳහා මුදල් අමාත්‍යාංශය විසින් ක්‍රියාත්මක කර ඇති ආයතනික ක්‍රියාමාර්ග, විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලියේ අභ්‍යන්තර පාලන සහ සයිබර් ආරක්ෂණ රාමුව ශක්තිමත් කිරීම සඳහා මීට පෙර සිටම ගත යුතුව තිබූ මූලික පියවර ලෙස සැලකේ. මෙමගින් පාලනමය, ක්‍රියා පටිපාටික සහ මෙහෙයුම් මට්ටම්වල පැවති අඩුපාඩු නැවත වරක් ඉස්මතු වේ.

V. මෙම සිදුවීම් මාලාව හේතුවෙන් එක්ස්පෝට් ෆයිනෑන්ස් ඔස්ට්‍රේලියා සමාගමට ගෙවීමට තිබූ හිඟ මුදල් ද කඩිනමින් ගෙවීමට රජයට සිදු විය.

## 8. නිර්දේශ

මෙම වාර්තාවේ අන්තර්ගත සොයාගැනීම් පදනම් කරගනිමින්, පාර්ලිමේන්තුව වෙත ඉදිරිපත් කිරීම සඳහා රජයේ මුදල් පිළිබඳ කාරක සභාව විසින් පහත සඳහන් නිර්දේශ යෝජනා කරනු ලබයි..

1. මෙම වාර්තාවේ අවසන් නිගමන මත පදනම්ව, ගරු කථානායකතුමා සහ මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශය විසින් සුදුසු විමර්ශන ක්‍රියාමාර්ග ගැනීම සඳහා අවශ්‍ය සහ ප්‍රමාණවත් පියවර ගැනීම.
2. සමස්ත විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය සම්බන්ධයෙන් විශේෂ විගණනයක් සිදු කරන ලෙස ජාතික විගණන කාර්යාලයට ගරු කථානායකතුමා විසින් උපදෙස් ලබා දීම.
3. අදාළ විමර්ශන අවසන් වීමෙන් අනතුරුව, කිසියම් නිලධාරියෙකුගේ වගකීම තහවුරු වන්නේ නම්, මූල්‍ය රෙගුලාසි 105 හි විධිවිධාන අනුව සිදුවූ පාඩුවෙන් අවම වශයෙන් කොටසක් හෝ අයකර ගැනීම සඳහා අවශ්‍ය ක්‍රියාමාර්ග ගැනීමේ හැකියාව මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශය විසින් සලකා බැලීම.
4. ණය කළමනාකරණ ක්‍රියාවලීන්ට අදාළ විධිවිධාන ද ඇතුළත්ව, රාජ්‍ය මූල්‍ය කළමනාකරණ පනත යටතේ සංශෝධිත මූල්‍ය රෙගුලාසි හඳුන්වාදීම කඩිනම් කිරීමට මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශය විසින් කටයුතු කිරීම. මෙම සංශෝධිත රෙගුලාසි මාස තුනක් ඇතුළත ක්‍රියාත්මක කිරීම. විශේෂයෙන්, ණයහිමියන්ගේ ඉන්වොයිසි ණය ගිවිසුම් සහ අනුමත සන්නිවේදන මාර්ග සමඟ සසඳා සත්‍යාපනය කිරීම සම්බන්ධ අභ්‍යන්තර පාලන ක්‍රමවේද ස්ථිරවම ශක්තිමත් කිරීමේ අවශ්‍යතාවක් පවතී. අනාගතයේදී මෙවැනි සිදුවීම් වැළැක්වීම සඳහා මෙම සම්මත සත්‍යාපන ක්‍රමවේද ක්‍රියාත්මක කිරීම අත්‍යවශ්‍ය වේ.

5. පවතින රාජ්‍ය ණය කළමනාකරණය සහ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය පිළිබඳ පුළුල් තක්සේරුවක් සිදු කිරීම සඳහා මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශය විසින් ස්වාධීන, සුදුසුකම්ලත් සහ දක්ෂ බාහිර පාර්ශ්වයක සේවාව ලබා ගැනීම.
6. . මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශය විසින් ඩිජිටල් ආර්ථික අමාත්‍යාංශය සමඟ සම්බන්ධීකරණයෙන්, ණයහිමියන්ගේ තොරතුරු සඳහා ආරක්ෂිත දත්ත පද්ධතියක් ස්ථාපිත කිරීම.
7. මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශය, එක්සපෝට් ෆයින්ෆැන්ස් ඔස්ට්‍රේලියා වෙත ගෙවිය යුතු හිඟ මුදල් පියවීම සම්බන්ධයෙන් සාකච්ඡා ආරම්භ කිරීම.
8. මුදල්, සැලසුම් හා ආර්ථික සංවර්ධන අමාත්‍යාංශයේ සියලුම දෙපාර්තමේන්තුවල තොරතුරු තාක්ෂණ පද්ධති අමාත්‍යාංශයේ තොරතුරු තාක්ෂණ කළමනාකරණ දෙපාර්තමේන්තුව මගින් අධීක්ෂණය කිරීමේ හැකියාව සලකා බැලීම.
9. රාජ්‍ය ආයතනවල තොරතුරු තාක්ෂණ සහ සයිබර් ආරක්ෂණ පද්ධති සම්බන්ධයෙන් ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසඳය (SL-CERT) විසින් ලබා දී ඇති නිර්දේශ ක්‍රියාත්මක කිරීම සහතික කිරීමේ වගකීම ඩිජිටල් ආර්ථික අමාත්‍යාංශය විසින් භාර ගැනීම, තීරණාත්මක තොරතුරු තාක්ෂණ පද්ධති නිසි පරිදි යාවත්කාලීන කර ක්‍රියාකාරී තත්ත්වයේ පවත්වාගෙන යාම කෙරෙහි වැඩි අවධානයක් යොමු කිරීම.
10. රජයේ බැංකුකරු ලෙස එහි කාර්යයභාරය ඉටු කිරීමේදී ශ්‍රී ලංකා මහ බැංකුවේ වගකීම්වලට අදාළ විධිවිධාන සම්බන්ධයෙන් මූල්‍ය ගනුදෙනු වාර්තා කිරීමේ පනතට අවශ්‍ය සංශෝධන රජය විසින් සලකා බැලීම.
11. සයිබර් අපරාධයකට සම්බන්ධ මෙම වංචාව සම්බන්ධයෙන් ඉහත සඳහන් නිශ්චිත නිර්දේශවලට අමතරව, රාජ්‍ය අංශය සඳහා තොරතුරු හෙළි කරන්නන් ආරක්ෂා කිරීම සම්බන්ධ පුළුල් ප්‍රතිපත්තියක් රජය විසින් හඳුන්වා දීම.

**ඇමුණුම්**

ඇමුණුම 1 - 2026 මැයි 08 දිනැති ඇමරිකානු ඩොලර් මිලියන 2.5 ක වංචනික විදේශ ණය ආපසු ගෙවීමේ ගනුදෙනුව සම්බන්ධයෙන් රජයේ මුදල් පිළිබඳ කාරක සභාවේ වාර්තාව

ඇමුණුම 2 - ආසන්න වශයෙන් ඇමරිකානු ඩොලර් මිලියන 2.5ක වංචනික විදේශ ණය ආපසු ගෙවීමේ ගනුදෙනුව සම්බන්ධයෙන් මුදල් අමාත්‍යාංශය විසින් 2026 ජුනි 01 වැනි දින රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද වාර්තාව (ඇමුණුම රහිත)

ඇමුණුම 3 - ශ්‍රී ලංකා මහ බැංකුව විසින් 2026 ජුනි 15 වැනි දින රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද සවිස්තරාත්මක වාර්තාව

ඇමුණුම 4 - ආසන්න වශයෙන් ඇමරිකානු ඩොලර් මිලියන 2.5ක වංචනික විදේශ ණය ආපසු ගෙවීමේ ගනුදෙනුව සම්බන්ධයෙන් මුදල් අමාත්‍යාංශය විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද වාර්තාවට ප්‍රතිචාර වශයෙන් ශ්‍රී ලංකා මහ බැංකුව විසින් ඉදිරිපත් කරන ලද 2026 ජුනි 15 දිනැති වාර්තාව (ඇමුණුම රහිත)

ඇමුණුම 5 - සයිබර් ආරක්ෂණ වාර්තා ඉදිරිපත් කිරීම සහ විදේශ සම්පත් දෙපාර්තමේන්තුවේ විද්‍යුත් තැපැල් සර්වරයේ තත්ත්වය පිළිබඳ පැහැදිලි කිරීම සම්බන්ධයෙන් ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසඳය (SL-CERT) විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද 2026 ජුනි 09 වැනි දිනැති ලිපිය (ඇමුණුම රහිත)

ඇමුණුම 6 - ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසඳය (SL-CERT) විසින් ඉදිරිපත් කරන ලද රජයේ ආයතන සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

ඇමුණුම 7 - 2026 ජුනි 15 දිනැති නීතිපති දෙපාර්තමේන්තුව විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද ලිපිය

ඇමුණුම 8 - 2026 ජුනි 25 දිනැති නීතිපති දෙපාර්තමේන්තුව විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද ලිපිය

ඇමුණුම 9 - 2026 ජුනි 23 දිනැති ණය ආපසු ගෙවීමේ කාර්යයන් සඳහා බලය පැවරීම පිළිබඳව භාණ්ඩාගාර ලේකම්වරයා විසින් රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද ලිපිය

ඇමුණුම 10 - භාණ්ඩාගාරය සහ ශ්‍රී ලංකා මහ බැංකුව අතර පවතින සම්බන්ධීකරණ යාන්ත්‍රණවල ප්‍රමාණවත් බව පිළිබඳව භාණ්ඩාගාර ලේකම් සහ මහ බැංකු අධිපති විසින් සම-අත්සන් කළ, 2026 අප්‍රේල් 04 දින රජයේ මුදල් පිළිබඳ කාරක සභාව වෙත ඉදිරිපත් කරන ලද ලිපිය

වාර්තාව සහ ඇමුණුම් සඳහා කරුණාකර පහත QR කේතය බලන්න



## **දසවැනි පාර්ලිමේන්තුව - පළමුවැනි සභාවාරය**

**එ.ජ. ඩොලර් මිලියන 2.5 ක විදේශ ණය පියවීමේ වංචනික ගනුදෙනුව  
සම්බන්ධයෙන්**

**රජයේ මුදල් පිළිබඳ කාරක සභාවේ වාර්තාව**

**පාර්ලිමේන්තුව වෙත ඉදිරිපත් කරන ලද්දේ**

**කාරක සභාවේ සාමාජික**

**ගරු. රවී කරුණානායක මහතා විසිනි**

**2026 මැයි මස 08 වැනි සිකුරාදා**



## කාරක සභාවේ සාමාජික මන්ත්‍රීවරුන්

ගරු (ආචාර්ය) හර්ෂ ද සිල්වා මහතා, පා.ම. (සභාපති)

ගරු චතුරංග අබේසිංහ මහතා, පා.ම.

ගරු (ආචාර්ය) කෞෂල්‍යා ආරියරත්න මෙනවිය, පා.ම.

ගරු අර්කම් ඉල්යාස් මහතා, පා.ම.

ගරු නිශාන්ත ජයවීර මහතා, පා.ම.

ගරු නීතිඥ රවුෆ් හකීම් මහතා, පා.ම.

ගරු රවි කරුණානායක මහතා, පා.ම.

ගරු හර්ෂණ රාජකරුණා මහතා, පා.ම.

ගරු ෂානක්කියන් රාජපුත්තිරන් රාසමාණික්කම් මහතා, පා.ම.

ගරු අජිත් අගලකඩ මහතා, පා.ම.

ගරු එම්.කේ.එම්. අස්ලම් මහතා, පා.ම.

ගරු නිමල් පලිභේන මහතා, පා.ම.

ගරු නීතිඥ වික්‍රාල් ප්‍රනාන්දු මහතා, පා.ම.

ගරු විජේසිරි බස්නායක මහතා, පා.ම.

ගරු සුනිල් රාජපක්‍ෂ මහතා, පා.ම.

ගරු තිළිණ සමරකෝන් මහතා, පා.ම.

ගරු වම්පික හෙට්ටිආරච්චි මහතා, පා.ම.

ගරු නීතිඥ ලක්මාලි හේමවන්ද මෙනවිය, පා.ම.

එ.ජ. ඩොලර් මිලියන 2.5 ක විදේශ ණය පියවීමේ වංචනික ගනුදෙනුව සම්බන්ධයෙන් රජයේ මුදල් පිළිබඳ කාරක සභාවේ වාර්තාව

ගෙවීම් දහයකට බලපාන ආකාරයෙන් එ.ජ.ඩො. මිලියන 2.5 කට ආසන්න වටිනාකමකින් යුත් වංචනික ගනුදෙනුවක් සිදුවී ඇති බව, 2026 අප්‍රේල් 30 වන දින පැවති රජයේ මුදල් පිළිබඳ කාරක සභාවේ මාධ්‍යයට විවෘත නොවූ සාකච්ඡාවකදී, මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධන අමාත්‍යාංශය විසින් පිළිගන්නා ලදී.

**පැමිණ සිටි සහිත මන්ත්‍රීවරුන්:**

ගරු (ආචාර්ය) හර්ෂ ද සිල්වා මහතා, පා.ම. (සභාපති)  
ගරු චතුරංග අබේසිංහ මහතා, පා.ම.  
ගරු (ආචාර්ය) කේෂලයා ආරියරත්න මෙනවිය, පා.ම.  
ගරු අර්කම් ඉල්යාස් මහතා, පා.ම.  
ගරු නීතිඥ රවුෆ් හකීම් මහතා, පා.ම.  
ගරු රවි කරුණානායක මහතා, පා.ම.  
ගරු හර්ෂණ රාජකරුණා මහතා, පා.ම.  
ගරු ෂානක්කියන් රාජපුත්තිරන් රාසමාණික්කම් මහතා, පා.ම. ( මාර්ගගත ලෙස)  
ගරු එම්.කේ.එම්. අස්ලම් මහතා, පා.ම.  
ගරු නිමල් පලිභේන මහතා, පා.ම.  
ගරු නීතිඥ වික්‍රාල් ප්‍රනාන්දු මහතා, පා.ම.  
ගරු විජේසිරි බස්නායක මහතා, පා.ම.  
ගරු සුනිල් රාජපක්ෂ මහතා, පා.ම.  
ගරු තිළිණ සමරකෝන් මහතා, පා.ම.  
ගරු වම්පික හෙට්ටිආරච්චි මහතා, පා.ම.  
ගරු නීතිඥ ලක්මාලි හේමවන්ද්‍ර මෙනවිය, පා.ම.

**පැමිණ සිටි නිලධාරීන්:**

**මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධන අමාත්‍යාංශය**

ආචාර්ය හර්ෂණ සූරියප්පෙරුම මහතා, භාණ්ඩාගාර ලේකම්  
ඒ.කේ. සෙනෙවිරත්න මහතා, භාණ්ඩාගාර නියෝජ්‍ය ලේකම්  
එස්.එස්. මුදලිගේ මහතා, භාණ්ඩාගාර නියෝජ්‍ය ලේකම්

**විදේශ සම්පත් දෙපාර්තමේන්තුව**

ආර්.එම්.එස්.පී.එස්. බණ්ඩාර මහතා, අධ්‍යක්ෂ ජනරාල්  
වසන්ත ධර්මසේන මහතා, අතිරේක අධ්‍යක්ෂ ජනරාල්

**රාජ්‍ය ණය කළමනාකරණ කාර්යාලය**

උදේනි උඩුගහපත්තුව මහත්මිය, අධ්‍යක්ෂ ජනරාල්

**ශ්‍රී ලංකා මහ බැංකුව**

කේ.එම්.ඒ.එන්. දවුලගල මහත්මිය, ජ්‍යෙෂ්ඨ නියෝජ්‍ය අධිපති/ප්‍රධාන විධායක නිලධාරී  
කේ.ඒ.පී. සිරිකුමාර මහතා, නියෝජ්‍ය අධිපති  
කේ.වී.කේ. අල්විස් මහතා, අධ්‍යක්ෂ, ගෙවීම් සහ පියවීම් දෙපාර්තමේන්තුව  
ඩී.එස්.එල්. සිරිමාන්න මහත්මිය, ප්‍රධාන ගණකාධිකාරී  
එන්.ඩී.වයි.සී. වීරසිංහ මහතා, මුදල් අධිකාරී

## පසුබිම

• 2024 ජුනි මාසයේදී 2024 අංක 33 දරන රාජ්‍ය ණය කළමනාකරණ පනත බලාත්මක කිරීමෙන් අනතුරුව, රාජ්‍ය ණය කළමනාකරණය කිරීම රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) වෙත ආයතනික වශයෙන් පවරා දීමේ කාර්යය 2024 වසරේ අග භාගයේ සිට අඛණ්ඩව සිදුවෙමින් පවතියි. ශ්‍රී ලංකා මහ බැංකුවේ (CBSL) රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD) , මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධන අමාත්‍යාංශයේ (මුදල් අමාත්‍යාංශයේ) විදේශ සම්පත් දෙපාර්තමේන්තුව (ERD) සහ මුදල් අමාත්‍යාංශයේ රාජ්‍ය ව්‍යවසාය දෙපාර්තමේන්තුව (PED) වෙත පැවරී තිබූ වගකීම් මධ්‍යගත කිරීම ද මෙයට ඇතුළත් විය.

• ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD) වෙතින් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) වෙත කාර්යයන් පැවරීම 2025 වසරේ අග භාගය වන විට අවසන් කරන ලද අතර, ඒ අනුව 2026 ජනවාරි මාසයේදී රාජ්‍ය ණය දෙපාර්තමේන්තුව(PDD)වසා දමන ලදී. විදේශ සම්පත් දෙපාර්තමේන්තුවේ (ERD) බොහෝ කාර්යයන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය(PDMO) වෙත පැවරී ඇතත්, රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) සමඟ එක්ව ද්විපාර්ශ්වික සහ බහුපාර්ශ්වික ණය ලබාගැනීම් සම්බන්ධයෙන් සාකච්ඡා කිරීම සහ ඒවා ක්‍රියාත්මක කිරීම සඳහා විදේශ සම්පත් දෙපාර්තමේන්තුව (ERD) තවදුරටත් සම්බන්ධ වෙයි.

• රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) පෙර මෙහෙයුම් කාර්යාලය (Front Office), මැදි මෙහෙයුම් කාර්යාලය (Middle Office) සහ පසු මෙහෙයුම් කාර්යාලය (Back Office) ලෙස ව්‍යුහගත කර ඇත. පසු මෙහෙයුම් කාර්යාලය විසින් ණය සේවාකරණ කාර්යය හසුරුවනු ලැබේ.

### රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ බලතල සහ කාර්යයන් සංක්ෂිප්තව

#### රාජ්‍ය ණය කළමනාකරණ කාර්යාලය

##### පෙර මෙහෙයුම් කාර්යාලය (Front Office)

- දේශීය ණය ගැනීමේ ඒකකය (Domestic Borrowing Unit)
- විදේශීය ණය ගැනීමේ ඒකකය (External Borrowing Unit)
- ආයෝජක සබඳතා සහ අලෙවිකරණ සංවර්ධන ඒකකය (Investor Relations and Market Development Unit)

##### කාර්යය (Functions)

- රජයේ ණය ගැනීම් (Government borrowings)
- ඇපකර සහ ණය දීම (Guarantees and on-lending)
- සැපයුම්කරුගේ ණය සහ මූල්‍ය කල්බදු (Supplier's Credits and Finance leases)
- ආයෝජක සබඳතා (Investor relations)

##### මැදි මෙහෙයුම් කාර්යාලය (Middle Office)

- ප්‍රතිපත්ති සහ විශ්ලේෂණ ඒකකය (Policy and Analysis Unit)

- ණය අවදානම් විශ්ලේෂණ සහ අධීක්ෂණ ඒකකය ( *Credit Risk Analysis and Monitoring Unit*)
- අවදානම් පාලන සහ අනුකූලතා ඒකකය ( *Risk Control and Compliance Unit*)

#### කාර්යය(Functions)

- මධ්‍ය කාලීන ණය කළමනාකරණ උපාය මාර්ගය සහ වාර්ෂික ණය ගැනීමේ සැලැස්ම( *Medium term debt management strategy and annual borrowing plan*)
- ණය අවදානම් තක්සේරුව සහ අධීක්ෂණය( *Credit Risk Assessment & Monitoring*)
- අවදානම් පාලනය සහ අනුකූලතාව ( *Risk Control and Compliance*)
- ණය සේවා පුරෝකථනය ( *Debt service forecasting*)

#### පසු මෙහෙයුම් කාර්යාලය -Back Office

- ණය සටහන් කිරීමේ ඒකකය ( *Debt Recording Unit*)
- ණය සේවාකරණ ඒකකය ( *Debt Servicing Unit*)
- ණය සංඛ්‍යාලේඛන සහ වාර්තාකරණ ඒකකය( *Debt Statistics and Reporting Unit*)

#### කාර්යය(Functions)

- ණය සටහන් කිරීම( *Debt recording*)
- ණය සේවාකරණය( *Debt Servicing*)
- වාර්තාකරණය සහ ප්‍රකාශනය( *Reporting and Publications*)

මුදල්, ආර්ථික ස්ථායීකරණ සහ ජාතික ප්‍රතිපත්ති අමාත්‍යාංශය Ministry of Finance, Economic Stabilization and National Policies

#### නිරීක්ෂණ

#### අනාවරණය සිදුවුණු කාලරේඛාව:

1. 2026 ජනවාරි මැද භාගයේදී, ඉන්දියාව බවට ඇඟවෙන , ද්විපාර්ශ්වික ණය හිමි රටක් සම්බන්ධ සිය විදේශ ණය ආපසු ගෙවීමේ ක්‍රියාවලිය හා සම්බන්ධ සැක සහිත සයිබර් ක්‍රියාකාරකම් පිළිබඳව, මුදල් අමාත්‍යාංශයට අනතුරු ඇඟවීමක් කරනු ලැබුණි. ඒ මත පදනම්ව, ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර ඒකකය (SLCERT) සහ ශ්‍රී ලංකා පොලිසියේ සයිබර් ආරක්ෂක අංශය දැනුවත් කිරීම ඇතුළු පියවර මුදල් අමාත්‍යාංශය විසින් ගන්නා ලදී.

2. 2026 මාර්තු මාසයේදී, මුදල් අමාත්‍යාංශය විසින් ද කරන ලද විමසීමවලින් පසුව, 2025 තුන්වන කාර්තුවේදී එක්ස්පෝට්ට් ගයිනෑන්ස් ඕස්ට්‍රේලියා (Export Finance Australia ) වෙත ආපසු ගෙවිය යුතු ණය වාරික නොලැබීම සම්බන්ධයෙන් ඕස්ට්‍රේලියානු බලධාරීන් විසින් වාර්තා කරන ලදී<sup>1</sup> .මෙම අනාවරණයෙන්

<sup>1</sup> PDMO Q4-2025 ණය ප්‍රකාශනයට අනුව ඇමරිකානු ඩොලර් මිලියන 39 ක පමණ ණය සඳහා; එනම්; Export Finance &

අනතුරුව, 2006 අංක 6 දරන මුදල් ගනුදෙනු වාර්තා කිරීමේ පනතට සහ මුදල් රෙගුලාසි (FR) වලට අනුකූලව, නියමිත කාල සීමාවන් තුළ, ශ්‍රී ලංකා පොලිසියේ අපරාධ පරීක්ෂන දෙපාර්තමේන්තුව (CID) සහ ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය බුද්ධි ඒකකය (FIU) වෙත පැමිණිලි ගොනු කිරීම සිදු විය.

3. දැනට විමර්ශනයට ලක්ව ඇත්තේ 2025 සැප්තැම්බර් සිට 2026 ජනවාරි දක්වා කාලය තුළ ඇමරිකානු ඩොලර් මිලියන 2.5ක් පමණ මුදලකට අදාළව සිදු කර ඇති ගනුදෙනු 10කි. මෙම විමර්ශනයට ශ්‍රී ලංකාව සහ ඕස්ට්‍රේලියාව පමණක් නොව වෙනත් රටවල් කිහිපයක්ද ඇතුළත්ය.

4. මුදල් රෙගුලාසි (FR) 104 යටතේ අභ්‍යන්තර විමර්ශනය සඳහා අවශ්‍ය පියවර ගෙන ඇති බවත්, එමඟින් නිලධාරීන් හතර දෙනෙකු තාවකාලිකව වැඩ තහනමට ලක් කිරීමට හේතු වූ බවත් කාරක සභාවේ ප්‍රශ්න කිරීම්වලදී මහා භාණ්ඩාගාරයේ ලේකම්වරයා විසින් ප්‍රකාශ කරන ලදී. මුදල් රෙගුලාසි (FR) 104 යටතේ, වංචාව හෙළිදරව් වූ දින සිට දින 7ක් ඇතුළත මූලික වාර්තාවක් සම්පාදනය කළ යුතු අතර, අනාවරණයෙන් මාස තුනක් ඇතුළත අවසන් වාර්තාව සම්පාදනය කළ යුතුය. 2006 අංක 6 දරන මුදල් ගනුදෙනු වාර්තා කිරීමේ පනතට අනුකූලව, මූල්‍ය බුද්ධි ඒකකය (FIU) වෙත පැමිණිලි ගොනු කර ඇති බව ද එවැනිම ප්‍රශ්න කිරීම් මගින් තහවුරුකරගන්නා ලදී.

5. ස්ථාවර නියෝග 121(2) යටතේ රාජ්‍ය ණය සහ ණය සේවාකරනය පරීක්ෂා කිරීම සඳහා නිශ්චිත වරමක් ඇති එකම අධීක්ෂණ ආයතනය ලෙස පාර්ලිමේන්තුව, රජයේ මුදල් පිළිබඳ කාරක සභාව(COPF) හරහා සිදුකරන කාර්යභාරය කාරක සභාව විසින් නැවත අවධාරණය කරමින් , මෙම කාරණය කාරක සභාවට විශේෂයෙන් අදාළ වන බව පෙන්වා දෙන ලදී.

#### ආයතනික ක්‍රියාවලීන්

6. 2026 ජනවාරි මාසයේදී රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD) වසා දැමීමට පෙර, ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුවේ (PDD) සිට රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) වෙත ණය කළමනාකරණ ක්‍රියාවලීන් මාරු කිරීමේ අවසාන අදියර 2025 සැප්තැම්බර් සිට 2026 ජනවාරි දක්වා කාල වකවානුවේ සිදු විය. 2024 අංක 33 දරන රාජ්‍ය ණය කළමනාකරණ පනතෙහි සහ 2023 අංක 16 දරන ශ්‍රී ලංකා මහ බැංකු පනතේ විධිවිධාන අනුගත වන පරිදි , රාජ්‍ය මූල්‍ය කටයුතුවලින් ශ්‍රී ලංකා මහ බැංකුව ඉවත් කිරීමේ අපේක්ෂාවන්ට අනුකූලව මෙය සිදු කරන ලදී.

7. එම කාලය තුළ, අසම්පූර්ණ තොරතුරු සහිත ගනුදෙනු දෙකක් ඔවුන්ගේ පද්ධති මගින් ගෙවීම ප්‍රතික්ෂේප කර ඇති බව ශ්‍රී ලංකා මහ බැංකු නිලධාරීහු ප්‍රකාශ කළහ. ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුව

---

*Insurance Corporation of Australia සඳහා ඇමරිකානු ඩොලර් මිලියන 20.4 ක හිඟ මුදල් සහ ANZ Investment Bank Australia සඳහා ගෙවිය යුතු ඇමරිකානු ඩොලර් මිලියන 18.7 ක හිඟ මුදල් සඳහා ඕස්ට්‍රේලියාව සහ ශ්‍රී ලංකාව අතර ද්විපාර්ශ්වික ණය ප්‍රතිව්‍යුහගත කිරීම සඳහා නිල වශයෙන් අත්සන් තැබීම 2025 ඔක්තෝබර් 27 වන දින සිදු විය.*

අවම වශයෙන් එක් ගනුදෙනුවක තොරතුරු, නැවත තහවුරු කරන ලෙස රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) සහ රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD) වෙත යොමු කර තිබුණි.

8. රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) පිහිටුවීමට පෙර, ද්විපාර්ශ්වික සහ බහුපාර්ශ්වික ණය කළමනාකරණයට අදාළ සියලුම කාර්යයන් විදේශ සම්පත් දෙපාර්තමේන්තුව (ERD) විසින් සිදු කරන ලදී. එම දෙපාර්තමේන්තුව ණය ආපසු ගෙවීම් සඳහා ණයනිමියන්ගෙන් ඉන්වොයිසි ලබාගන්නා ලද අතර, එහි මෙහෙයුම් කාර්යාලය හරහා ගෙවීම් උපදෙස් සකස් කර ඒවා ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD) වෙත යොමු කරන ලදී. රාජ්‍ය ණය දෙපාර්තමේන්තුව (PDD) විසින් එම ගෙවීම් උපදෙස් තහවුරු කර ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුව වෙත යොමු කරන ලද අතර, එමඟින් ශ්‍රී ලංකා මහ බැංකුවේ ගෙවීම් දෙපාර්තමේන්තුව විසින් SWIFT හුවමාරු කිරීම් සඳහා අවශ්‍ය තහවුරු කිරීම් නිකුත් කරන ලදී.

9. රාජ්‍ය ණය කළමනාකරණ කාර්යාලය (PDMO) පිහිටුවීමත් සමඟ, විදේශ සම්පත් දෙපාර්තමේන්තුවෙහි (ERD) මෙහෙයුම් කාර්යාලයෙහි (back office) කාර්යයන්, රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි මෙහෙයුම් කාර්යාලය විසින් පවරා ගන්නා ලදී. නමුත් විදේශ සම්පත් දෙපාර්තමේන්තුව විසින් ණය නිමියන්ගෙන් බොහෝ ගෙවීම් ඉන්වොයිසි ලබා ගැනීම අඛණ්ඩව කරගෙන යන ලද අතර, එමඟින් ඒවා ඉදිරි කටයුතු සඳහා රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි මෙහෙයුම් කාර්යාලයට යොමු කරනු ලදී. සිය මෙහෙයුම් කාර්යාලයෙහි ණය සේවාකරණ කාර්යය , එම ක්‍රියාවලියම අනුගමනය කරන ලද බවත්, ගෙවීම් තොරතුරු තහවුරු කිරීමේ ක්‍රියාවලිය සඳහා ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව විසින් භාවිතා කරන මෘදුකාංග පද්ධති යොදාගත් බවත්, තහවුරු කරන ලද උපදෙස් ශ්‍රී ලංකා මහ බැංකුවේ මූල්‍ය දෙපාර්තමේන්තුවට යවා ඇති බවත් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් කාරක සභාව වෙත දන්වන ලදී. 2025 දෙසැම්බර් මස දක්වා, මෙම ක්‍රියාවලියට සහය දක්වනු පිණිස, රාජ්‍ය ණය කළමනාකරණ කාර්යාලය සමඟ ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව එක්ව කටයුතු කර ඇති බව පෙනේ.

10. මුදල් අමාත්‍යාංශය තුළ අදාළ නිලධාරීන්ට අධිකාරී බලය පැවරීම මගින්, ණය සේවාකරණ කාර්යය සම්පූර්ණයෙන්ම ඩිජිටල්කරණය කරන ලද ක්‍රියාවලියක් හරහා භෞතික ලියකියවිලි සහ අත්සන් යොදා ගැනීමකින් තොරව සිදු කෙරේ. මෙම ක්‍රියාවලිය තුළ, ණය සේවාකරණ කාර්යය භාරව සිටින රාජ්‍ය ණය කළමනාකරණ කාර්යාලයෙහි පසු මෙහෙයුම් කාර්යාලයෙහි අධ්‍යක්ෂවරයාට, ඒකාබද්ධ අරමුදලෙන් සිදු කරන සියලුම විදේශ ණය සේවා ගෙවීම් අනුමත කිරීමේ බලය ඇති බව පෙනේ.

11. ඒකාබද්ධ අරමුදලෙන් ලබා ගන්නා මුදල් ප්‍රවාහ සඳහා ක්‍රියාකාරීව වගකිව යුතු භාණ්ඩාගාර මෙහෙයුම් දෙපාර්තමේන්තුව (TOD), ණය සේවා ගෙවීම් තහවුරු කිරීම් සම්බන්ධයෙන් දැනුවත් කරනු ලැබේ. නමුත් ගෙවීම් තහවුරු කර, ගෙවීමේ අවසන් අවසරය එම දෙපාර්තමේන්තුව ලබා දීම අවශ්‍ය නොවේ.

12. මුදල් අමාත්‍යාංශයේ විවිධ දෙපාර්තමේන්තු වලට වෙනස් තොරතුරු තාක්ෂණ පද්ධති තිබෙන අතර ITMIS වැනි පොදු පද්ධතිවලට අමතරව, ඔවුන්ගේ නිශ්චිත කාර්යයන්ට අදාළව සේවා සපයන්නන් සිටී.

13. මුදල් පාලනය සඳහා වන කාර්යයන් පවරා දීම පිළිබඳ මූල්‍ය රෙගුලාසි 135 (FR 135) ට අනුකූලව ඉහත විස්තර කර ඇති ඩිජිටල් ගෙවීම් ක්‍රියාවලීන් සිදු කිරීම සඳහා, භාණ්ඩාගාර ලේකම්වරයාගෙන් අවශ්‍ය නිලධාරීන්ට බලය පැවරීම වාර්ෂිකව සිදු කරන්නේ දැයි කාරක සභාව ප්‍රශ්න කළේය. මේ සම්බන්ධයෙන් අවශ්‍ය තොරතුරු කාරක සභාවට ඉදිරිපත් කිරීමට භාණ්ඩාගාර ලේකම්වරයා පොරොන්දු විය .

14. ආයතනික ක්‍රියාවලීන්හි අංශ කිහිපයක් කාරක සභාවේ විවේචනයට ලක් විය;-

අ. ණය කළමනාකරණ කාර්යයන් ඵලදායී ලෙස මධ්‍යගත කිරීම සඳහා අවශ්‍ය විශේෂඥතාව ඇති නිලධාරීන් බඳවා ගනු ලබන බවට රාජ්‍ය ණය කළමනාකරණ කාර්යාලය විසින් සහතික කළ යුතු බව, 2024 මැයි මාසයේ දී රාජ්‍ය ණය කළමනාකරණ කාර්යාලය පනත සම්මත කරන ලද අවස්ථාවේ සිටම, මුදල් කාරක සභාව විසින් නැවත නැවතත් කරන ලද ඉල්ලීම නැවත අවධාරණය කරන ලදී.

ආ. වඩාත් ජ්‍යෙෂ්ඨ නිලධාරීන් හෝ වෙනත් දෙපාර්තමේන්තුවක නිලධාරීන් විසින් තහවුරු කිරීමකින් තොරව, විශාල ප්‍රමාණයේ ණය මුදල් ආපසු ගෙවීම්වල අවසාන ගෙවීම් සඳහා අනුමැතිය ලබා දීමට වගවීම ණය කළමනාකරණ කාර්යාලයෙහි පසු මෙහෙයුම් කාර්යාලයේ අධ්‍යක්ෂවරයෙකුට පමණක් සීමා කිරීමේ සුදුසු භාවය.

ඇ.විදේශ ණය ගෙවීම් සහ ණය ශේෂ තහවුරු කිරීම සම්බන්ධයෙන් කටයුතු කරනු ලැබූ ආයතන සහ නිලධාරීන් අතර එකඟතාවයක් නොතිබිණි. ණය සේවා සැපයීම හා වාර්තා කිරීම පිළිබඳ සියලුම කාර්යයන් රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත පවරා තිබිය යුතු බවට රාජ්‍ය ණය කළමනාකරණ පනත මගින් නියම කර තිබුණ ද, තව දුරටත් මේ සම්බන්ධයෙන් සැලකිය යුතු කාර්යභාරයක් විදේශ සම්පත් දෙපාර්තමේන්තුව වෙතින් සිදු කෙරෙන බවක් දක්නට ලැබේ .

ඈ .මෙම සිද්ධිය සම්බන්ධයෙන් ශ්‍රී ලංකා මහ බැංකුවේ කිසිදු නිලධාරියකුට තමන් සතු වගකීමකින් නිදහස් වීමේ හැකියාවක් නැත. 2026 වසරේ ජනවාරි මාසය දක්වා ශ්‍රී ලංකා මහ බැංකුවේ රාජ්‍ය ණය දෙපාර්තමේන්තුව මගින් රාජ්‍ය ණය කළමනාකරණ කාර්යාලයේ කටයුතු සඳහා සහාය දක්වා තිබූ අතර, රටේ විදේශ විනිමය සංචිත කළමනාකරණය සිදු කරනු ලබන ආයතනය ලෙස ශ්‍රී ලංකා මහ බැංකුව සතුව පවත්වාගෙන යනු ලබන භාණ්ඩාගාරයේ විදේශ මුදල් ගිණුම් භාවිතා කරන ආකාරය පිළිබඳව ද අවධානය යොමු කළ යුතු විය .

**රාජ්‍ය මූල්‍ය කළමනාකරණය පිළිබඳ ගැටලු:**

15. මෙම වංචනික ගනුදෙනුව හේතුවෙන් ශ්‍රී ලංකාව විසින් ඕස්ට්‍රේලියාවට ගෙවීමට නියමිතව තිබූ ණය වාරික නොගෙවීම හේතුවෙන් මේ වන විට ශ්‍රී ලංකාව තාක්ෂණික වශයෙන් ණය පැහැර හැරීමේ තත්ත්වයකට පත්වී තිබේද යන්න පිළිබඳව කාරක සභාව විසින් ප්‍රශ්න කරන ලදී. අදාළ ණය ගෙවීමට ඇති උවමනාව සහ ඊට ඇති හැකියාව පෙන්වුම් කරනු ලැබ ඇති බැවින් සහ අදාළ ගෙවීම් නියමිත කාලවකවානුවලට අනුව සිදු කරනු ලැබ ඇති හෙයින් ( එය ණයහිමියා වෙත ලැබී නොතිබුණ ද), මෙම සිද්ධිය හේතුවෙන් ශ්‍රී ලංකාව ඕස්ට්‍රේලියාවට ණය පැහැර හැරීමේ තත්ත්වයකට පත්වී ඇතැයි තමන් විශ්වාස නොකරන බව මහා භාණ්ඩාගාර ලේකම්වරයා විසින් කාරක සභාව වෙත දැනුම් දෙන ලදී .ණය ප්‍රතිව්‍යුහගත

කිරීමේ ක්‍රියාවලියට සහාය ලබාදුන් ජාත්‍යන්තර උපදේශකවරුන්ගෙන් ද මේ සම්බන්ධයෙන් අදහස් විමසා තිබේ.

16. මේ හා සමාන ගැටලු සහගත තත්ත්වයක් නැවත ඇති නොවන බව තහවුරු කිරීම සඳහා ගෙන ඇති ක්‍රියාමාර්ග මොනවාද යන්න පිළිබඳව ද කාරක සභාව විසින් විමසීමක් කරන ලදී .

මෙහිදී විශේෂයෙන්ම සත්‍යාපනය කිරීම සහ බලය පැවරීම යන දෙඅංශයන් වැඩි දියුණු කරමින් මහ බැංකුවේ ද සහාය ඇතිව ණය සේවාකරණ ගෙවීම් ක්‍රියාවලිය තව දුරටත් ශක්තිමත් කිරීම සඳහා පියවරයන් අනුගමනය කර ඇති බව මහා භාණ්ඩාගාර ලේකම්වරයා විසින් දැනුම් දෙන ලදී .

17. තව ද, වර්ෂ 1992 න් පසු මුදල් රෙගුලාසි ඒකාබද්ධ කර සම්පූර්ණයෙන් යාවත්කාලීන කර නොමැති බව කාරක සභාව විසින් අවධාරණය කරන ලදී .එහි ප්‍රතිඵලයක් වශයෙන්, රජයේ නවීන මූල්‍ය ක්‍රියාවලීන් සහ පසුගිය වසරවල සම්මත කර ඇති නව නීති සම්පාදන මෙවලම් හමුවේ එම රෙගුලාසි ප්‍රමාණවත් නොවන බව සඳහන් කෙරිණි .යාවත්කාලීන කරන ලද මුදල් රෙගුලාසි මේ වන විට සම්පාදනය කෙරෙමින් පවතින බවත්, ඉදිරි මාස කිහිපය ඇතුළත එම සම්පාදන කටයුතු අවසන් කිරීමට අපේක්ෂිත බවත් මහා භාණ්ඩාගාර ලේකම්වරයා විසින් කාරක සභාවට දැනුම් දෙන ලදී .

**නිර්දේශ :**

1. ඒ අනුව, මුදල් අමාත්‍යාංශය විසින් සති හතරක කාල සීමාවක් තුළ, එනම් 2026 වසරේ මැයි මාසය අවසන් වීමට පෙර , මේ දක්වා සිදුවී ඇති සිදුවීම් සහ ඒ සම්බන්ධයෙන් ගෙන ඇති ක්‍රියාමාර්ග, වංචනික ගනුදෙනුව සිදුවූ ආකාරය හා ඊට හේතු වූ කරුණු, එහි දී හඳුනා ගනු ලැබූ ආයතනික ගැටලු, ණය කළමනාකරණය හා සම්බන්ධ ආයතනවල කාර්ය මණ්ඩල හා තාක්ෂණික හැකියාවන් මෙන්ම, නැවත එවැනි සිද්ධියක් සිදු වීම වළක්වා ගැනීමට ගෙන ඇති පියවරයන් ඇතුළත් සවිස්තරාත්මක කාලරාමුවක් සහිත සම්පූර්ණ වාර්තාවක් ඉදිරිපත් කළ යුතුය.
2. මුදල් අමාත්‍යාංශය විසින් එකී සම්පූර්ණ වාර්තාවට අමතරව, සියලුම විදේශ ණය ආපසු ගෙවීම සඳහා දැනට පවතින ගෙවීම් ක්‍රියාවලියට අදාළ මූල්‍ය පාලන බලතල පැවරීම තහවුරු කෙරෙන ලිපි ලේඛන ද ඉදිරිපත් කළ යුතුය.
3. තව ද, රාජ්‍ය ණය කළමනාකරණ පනතෙහි සඳහන් පරිදි, ණය කළමනාකරණ කටයුතු සියල්ලක්ම රාජ්‍ය ණය කළමනාකරණ කාර්යාලය වෙත මාරු කර ඇති බව ද මුදල් අමාත්‍යාංශය විසින් තහවුරු කළ යුතුය .
4. සයිබර් ආරක්ෂාව මූල්‍ය අවදානමක් ලෙස සලකා, මෑත වසරවල රාජ්‍ය ආයතන පුරා සාමාන්‍ය සිදුවීමක් බවට පත්ව ඇති ගෙවීම් පිළිබඳ ගැටලු සහ දත්ත සොරකම් කිරීම් නැවත සිදුවීම වළක්වා ගැනීම සඳහා මුදල් අමාත්‍යාංශය විසින් පුළුල් ක්‍රියාමාර්ග අනුගමනය කළ යුතුය.
5. යාවත්කාලීන කරන ලද මුදල් රෙගුලාසි, රාජ්‍ය මූල්‍ය කළමනාකරණ පනතට සහ රාජ්‍ය ණය කළමනාකරණ පනතට අනුකූල වන පරිදි සම්පාදනය කරමින් පවතින අතර, එය අවසන් කර හැකි ඉක්මනින් පාර්ලිමේන්තුව විසින් සමාලෝචනය කරනු ලැබීම සඳහා ඉදිරිපත් කළ යුතුය.



*Highly Confidential*

**Report of the Ministry of Finance to the Committee of Public Finance on  
Alleged Fraudulent Foreign Debt Repayment Transaction of  
approximately USD 2.5 Million**

*This report is submitted based on the request of Committee of Public Finance. The content in this report consists highly sensitive and confidential information and the investigations are on going, the document is considered as confidential and for limited sharing. The report contains details of individuals, institutions, banks, account numbers, and government agencies, therefore, exposing this information while there is an active investigation under judiciary supervision needs to be considered prior to sharing this content with any party.*

**Question No. 01**

Submit a comprehensive report, together with supporting documentary evidence, including a detailed timeline of events and actions taken to date, an explanation of how and why the fraudulent transaction occurred, the institutional shortcomings identified, and the measures implemented to prevent a recurrence.

**1.1 Detailed Timeline of the events and actions taken so far by Ministry of Finance,  
Planning and Economic Development**

**Background Information of the Incident**

- After the signing the MoU with Official Creditor's Committee (OCC MOU) in 24th June 2024, ERD was engaged with all bilateral lending partners; restructuring of the signed loan agreements as agreed by the OCC MOU. There were 402 loans to be restructured and as of now the restructuring process is being continued.
- Pursuant to the Public Debt Management Act No. 33 of 2024 (PDMA), the Public Debt Management Office (PDMO) was established on 02.12.2024.
- The functions handled by Debt Management Division of ERD with the Commonwealth Secretariat Debt Recording and Management System (CS-DRMS) and the attached staff were transferred to the newly established PDMO in December 2024 and staff assumed duties on 01.01.2025.

## ***Highly Confidential***

- During this transition period of Debt Management, legal and institutional reforms were introduced. Meanwhile, with regard to the Debt Restructuring process, the Back Office of the PDMO carried out only reconciliation and recording of loan agreements, while the coordination of Bi-lateral lenders was carried out by External Resources Department (ERD).
- After reviewing the organizational structure, cadre approval was obtained for the carrying out of PDMO's functions which are mandated under PDMA. Accordingly, the recruitment is being carried out since then.
- As per Section 37 of PDMA, an interim arrangement was made to undertake the Debt Management functions hitherto carried out by CBSL-PDD. As per the above requirement, to undertake all the debt management functions within 18 months from the appointed date (25.11.2024) of the PDMA.
- Then, a simultaneous process was commenced to train the newly recruited PDMO officials at the CBSL under their supervision from March to December 2025, under the direct supervision, the guidance of the PDD- CBSL officials at the CBSL premises. From Mid-October to December 2025, PDMO official were allowed to work in the CBSL systems under their guidance and direct supervision. In this arrangement, the approval process and the regulatory framework of the CBSL were followed.
- Subsequently, MoF noted that the CBSL had closed the functions of PDD from 01<sup>st</sup> January 2026.

### **Brief of the Events Occurred**

- The fraudulent activity (suspicious behavior of mail server system of ERD or email compromise) was first observed after bouncing back a payment of an invoice identical to that of the Indian Exim Bank with a fake payment details on 06<sup>th</sup> January 2026 (Annex I- A). Then the payment was done to the correct account and informed the activity to the Criminal Investigation Division on 09<sup>th</sup> January, 2026 and informed the CERT on the same day to investigate the system as the entire process of debt restructuring was conducted mostly via electronic communication such as virtual meetings and email communication had with the lenders, debt advisors, ERD, MOF, CBSL and also PDMO which joined at the later stage.
- After the incident, ERD took an immediate action to scrutinize the previous payments which have been made based on the invoices submitted after the restructuring process.
- Payment instructions received via email for several other due payments, including those to the United Kingdom (USD 1,294,605.99) (Annex I- B), Germany (EUR 4,059,987.81) (Annex I-C) and Belgium (EUR 60,974.88) (Annex I- D), were carefully

**Highly Confidential**

reviewed by ERD and subsequently identified as fraudulent. As a precautionary measure, the related payment to UK was immediately suspended. The communications initiated by the suspicious party were recognized and alerted the investigation authorities. Subsequently, the payment related to Belgium was made to the correct account.

- However, while investigating the previous transactions the following incident was identified.

Six invoices had been received from Export Finance Australia (EFA) in relation to the repayment of arrears interest payments on 13th November 2025 with the due date for payments on 15th November 2025. The invoices received by the ERD had been forwarded to the PDMO on 13rd November 2025 for processing of the payment through CBSL and the matter had subsequently been communicated to CBSL by the PDMO on 13rd November 2025.

- a) It was observed that out of six invoices (Annex I –E1-E6), 04 invoices had been processed by the CBSL/PDMO including the invoice for the payment of Legal Fee at the first instance (Annex I- E1-E4). However, later it was informed that, two invoices amounting to USD 1,375,459.74 have been returned to the CBSL account by the Federal Reserve Bank (FRB) on 24<sup>th</sup> November 2025 (Annex I E5-E6).

**Details of paid and unpaid invoices are as follows;**

- 03 invoices amounting to USD 713,758.88 submitted for arrears interest payment paid by CBSL on 14<sup>th</sup> November 2025 to the following account; (Annex I E1-E3)  
Mish Global LLC, in care of Export Finance and Insurance Corporation  
TD Bank  
National Association 1001, East Songsmith Drive Bear, Delaware, DE  
19701 USA
- An Invoice amounting to AUD 141,739.95 submitted for the payment of Legal Fee - Paid by CBSL on 14<sup>th</sup> November 2025 to the following account; (Annex I - E4)  
Mish Global LLC, in care of Export Finance and Insurance Corporation  
Commonwealth bank of Australia  
Martin Place, Sydney  
Australia
- 02 Invoices amounting to US \$ 1,375,459.74 submitted for the arrears interest payment – Rejected on 24<sup>th</sup> November 2025 by the intermediary bank to pay for the following account; (Annex I- F1-F2)



LMH Global LLC In care of Export Finance and Insurance  
Corporation  
US Bank N A, Minneapolis USA

- b) Subsequently, the returned two invoices had been resubmitted by amending the banking details on 26<sup>th</sup> November 2025 by the lender. The bank account which was successfully used for the previous fund transfer had been given for one payment with a new bank account in UAE for the other payment.

The new beneficiary details were as follows:

Sifra Watan Project Management Services EST  
WIO Bank PJSC  
Etihad Airways Centre, Floor 5, AL Raha Beach  
AL Muneera, Abu Dhabi UAE

- c) After making an attempt to make the payment to the above bank in UAE, the payment had been rejected by the intermediary bank. Then the CBSL has informed PDMO (in the e-mail trail exchanged between the CBSL and the PDMO) that since the beneficiary address is different and located in a different State it will be a matter regarding Anti Money Laundering (AML).
- d) 05 Invoices amounting to USD 420,211.96 for scheduled interest payment for 05<sup>th</sup> January 2026 had been paid to the beneficiary account in TD bank on 05<sup>th</sup> January 2026. (Annex I G1- G5)
- e) The invoice amounting to US \$ 997,799.48 which was rejected three times was paid to the same beneficiary account in TD bank on 20<sup>th</sup> January 2026 (Annex I -H)
- f) All of these payments were made to the TD Bank, for the SSI created in the NRM system on 15<sup>th</sup> November 2025 during the training period at PDD-CBSL by PDMO officials under direct supervision and approval process of CBSL.
- It is observed that, although the CBSL maintains that it acts solely as the banker to the Government, the Ministry of Finance (MOF) is of the view that adequate attention does not appear to have been accorded to transactions carrying potential Anti-Money Laundering (AML) implications, notwithstanding that such transactions had reportedly been identified by the CBSL. In this context, the MOF further, notes that, despite functioning as the Government's banker, the CBSL has stated in its letter dated 20 May 2026, that the provisions of the Financial Transaction Reporting Act No. 06 of 2006 are not applicable to the CBSL. This position on dealing with AML concerns noted by CBSL and the manner it was dealt raises concerns regarding the adequacy of regulatory oversight, internal compliance responsibilities, and the extent of accountability in relation to transactions identified as involving potential AML risks.

- In addition, CBSL has not provided the information requested by the MOF relating to the facts, observations, circumstances that led to the identification of potential AML-related concerns prior to the payment being effected in respect of the fraudulent transaction (Annex- II). In this regards, the CBSL has taken the position that the disclosure of such information may impede the effective execution of Government instructions and payment operations. However, the absence of such clarification limits the ability of the MOF to assess whether adequate due diligence, internal escalation procedures, and risk mitigation measures were appropriately considered before the transaction was processed particularly in light of other stakeholders engaged with CBSL such as intermediary banks - Federal Reserve Bank USA, City Bank USA, JP Morgan have notified the CBSL the existence of AML concerns, returning of funds and fraud involved (Annex – III).
- A copy of the response received from the CBSL, vide letter dated 20 May 2026, in reply to the MOF letter dated 18 May 2026, is attached herewith for reference as Annex IV.

#### **Transferring of Public Debt Management Functions of the CBSL to the PDMO – Legal background**

When CBSL Act was passed by parliament in 2023 it was envisaged that a separate law will be introduced to manage the Public Debt of the Government and to accommodate the new law CBSL Act introduces a temporary arrangement for Agency Functions of the CBSL on Public Debt Management.

Section 132 of the Central Bank Act No. 16 of 2023 stipulates that “.....the Central Bank shall continue to act as agent of the Government pursuant to sections 112 and 113 of the repealed Act, which shall be limited only in respect of the issuance of securities of the Government for the account of the Government and in respect of the management of public debt, until such date as the relevant law relating to public debt management agency or office comes into operation.”

However, when Public Debt Management Law was introduced, it was observed that interim period was required to transfer the functions of the CBSL to PDMO. Therefore, PDMO Act provides eighteen months of period from the appointment date of the PDMO Act. The relevant Section is as follows;

*“37. The applicability of section 132 of the Central Bank of Sri Lanka Act, No. 16 of 2023, shall come into operation on such date as the Minister may by Order published in the Gazette appoint within a period of eighteen months from the appointed date:*

*Provided that, notwithstanding the provisions of this section, the Office may perform its powers and functions under this Act.”*

***Highly Confidential***

As per the above section the Minister published the order by Gazette Notification No. 2489/68 on 22.05.2026 declaring that May 24, 2026 as the date on which the Central Bank of Sri Lanka shall cease, under the provisions of section 132 of the Central Bank of Sri Lanka Act, No. 16 of 2023, to act as the agent of the Government in respect of the issuance of securities of the Government for the account of the Government and in respect of the management of public debt (Annex V).

**Follow up actions taken by MOF ;**

- Reported to the Sri Lanka Computer Emergency Response Team with a copy to Sri Lanka Criminal Investigation Department – 09<sup>th</sup> January 2026 (Annex VI- A)
- Investigated the previous record and found suspicious emails within the emails exchanged between the ERD, EFA, PDMO and CBSL.
- Export Finance Company of Australia informed that the payment has not been received – 23<sup>rd</sup> March 2026 (Annex VI- B)
- Appointed an internal Technical fact finding committee for initial internal investigation – 23<sup>rd</sup> March 2026 (Annex VI- C)
- Made a written complaint to the Criminal Investigation Department – 24<sup>th</sup> March 2026 (Complaint number C51/26/CR) (Annex VI- D)
- Reported to the Financial Intelligence Unit (FIU) of CBSL by ERD– 01<sup>st</sup> April 2026 (Annex VI- E)
- Submitted the Committee Report to the Secretary to the Treasury – 10<sup>th</sup> April 2026 (Annex VI- F)
- Interdicted Two Officials in ERD and Two Officials in PDMO on 17<sup>th</sup> April 2026 to continue further investigation (Annex VI- G)
- MoF noted that CID has submitted the B Report to the Commercial High court, Colombo with ref. No. FRT/MC/PC/00193/26-B
- Reported to the Auditor General – 06<sup>th</sup> May 2026 (Annex VI- H)



appropriate degree of oversight, vigilance, and due diligence consistent with the objectives and underlying principles of the FTRA, particularly in relation to transactions identified as carrying potential AML-related risks.

### **1.3 Institutional Issues Identified**

#### **External Resource Department (ERD)**

- Though it was planned to upgrade the mail server system in the ERD, the implementation was delayed until the completion of the establishment process of the PDMO. Following the handing over the CS -DRMS system to PDMO, the procurement process of a new mail server system was commenced based on the revised system requirements identified thereafter. During this interim period, all communication relating to the debt restructuring process were carried out through the existing mail server system. As the exercise involved numerous external agencies operating from different locations and using various emails domains, certain limitations may have existed in the prevailing system with regard to security features required to verify and detect all forms of external threats of this nature.
- Further, as this period coincided with the institutional transition between the CBSL/ERD and the PDMO, together with the implementation of new operational arrangements under strict timelines for completion of debt restructuring activities, certain processes and responsibilities had not yet been fully formalized or clearly demarcated. Accordingly, the relevant institutions were in the process of developing and formalizing procedural manuals and operational guidelines.
- With regard to the observation that higher authorities had not been informed, it is observed that all documents connected with the debt restructuring process had been forwarded to the relevant authorities without delay. Further, immediately upon identification of the incident, all relevant authorities were duly informed and appropriate action was taken to facilitate the necessary investigations.

#### **Public Debt Management Office**

- The procedures followed by the PDD-CBSL, ERD, TOD over the decades was exactly followed by the PDMO after its establishment.
- The standard operational manual was in the drafting stage at the relevant time.

## **1.2 How and Why the Fraudulent Transaction Occurred**

- As per the MOU Bi-lateral loan restructuring process was in progress, in this exercise many external parties were engaged in the process and mostly the communication was done via electronically (emails, Virtual meetings and file sharing etc). Therefore, there was a risk to expose some communication to the external parties undetected.
- At the same time, regulatory environment of Public Debt Management was transformed and PDMO was established as a new entity to take over the entire Debt Management Functions of the Government. PDMO has to recruit and train the officials for the Public Debt Management tasks handled by the PDD of CBSL as well as for other debt management operations, most are newly introduced to the country.
- Relevant Debt Management functions carried out by other institutions were transferred to PDMO.
- The incident occurred during period when PDMO Officials were working under the guidance and supervision of PDD Officials of CBSL under their approval process by using their operational platforms. On the Request of MOF, opportunity to work in the CBSL actual platform was provided to the PDMO officials during the period of October to December 2025.
- The newly recruited Officials of PDMO may not have possessed adequate expertise on banking operations particularly in relation to the international fund transfer mechanisms, anti-money laundering activities, and international financial frauds associated with cyber-crimes. In this context, MoF is of the view that it was reasonably expected that the CBSL, in its capacity as the Banker to the Government and the regulator of the banking sector, would continue to discharge its banking and supervisory responsibilities in a manner consists with the spirits and objectives of the Financial Transaction Reporting Act No.06 of 2006.
- If CBSL is of the view that the provisions of the Financial Transactions Reporting Act No.06 of 2006 (FTRA) are not directly applicable to the institution, a significant concern arises as to which authority is responsible for ensuring compliance with AML-related obligations in respect of Government payment transactions processed through the banking system. In this regard, it is observed that the PDMO itself is not an institution falling within the direct regulatory scope of the FTRA, as the Act primarily imposes obligations on financial institutions to report suspicious transactions and accounts to the Financial Intelligence Unit (FIU), rather than on the Government in its capacity as a customer of the bank, which in this instance is the CBSL acting as the banker to the Government. Accordingly, in circumstances where the CBSL functions both as the banker to the Government and the regulator of the banking sector, it would reasonably be expected by the MOF that the CBSL should continue to exercise an



**Central Bank of Sri Lanka (CBSL)**

- It is observed that the BO of PDD has not properly guided trainee PDMO officials to use the account details of the beneficiary which has been recorded in the NRM instead has guided to change it based on the invoices received.
- The CBSL informed that the provisions of Financial Transaction Reporting Act No.06 of 2006 are not applicable to CBSL. Further, the response furnished by the CBSL dated 20<sup>th</sup> May 2026 did not provide the necessary details relating to the facts, observations, and circumstances identified in connection with the potential AML-related concerns arising from this transaction. Consequently, the absence of detailed clarification from the CBSL has limited the ability of the PDMO to fully ascertain the circumstances surrounding the incident and the basis upon which such AML-related concerns were identified.

**1.4 Measures taken by Ministry of Finance to strengthen the External Debt Servicing Process**

**Actions taken by PDMO to strengthen the External Debt Servicing Process**

- Actions was take to take over lender coordination from the External Resources Department regarding debt servicing.
- Actions were undertaken to establish formal communication channels with relevant lenders
  - Obtaining Authorized Officials, their Contact Details and account details for the relevant debt servicing from the respective Lenders
  - Obtaining the Lender's Invoice (LI) from the above authorized officials through their formal contact channels (emails, formal letters, if available via phones, through diplomatic missions, and country offices, through their web portals)
- At least ten days prior to the due date of the first payment indicated in the list, the monthly debt service forecast shall be submitted to the ST for payment approval
- Sought specialized technical assistance from the International Monetary Fund (IMF) to strengthen internal procedures relating to debt servicing. In this regard, several virtual discussions have already been conducted, and an IMF mission is scheduled to be fielded in mid-June 2026 to assist in finalizing the already drafted standard operating procedures for the PDMO, including debt servicing operations.
- Strengthening internal controls
  - Processes established for the purpose of verification of the LIs through at least two channels above mentioned, and via phone if accessible (using a PDMO phone with recording facility)

***Highly Confidential***

- Processes introduced to verify the authentication of accuracy of the account numbers given in the LI by cross checking with the original loan agreement (LA), if account number is available in the existing original LA/ addendum to the LA or through a document authorized by the Lender. In the new loan agreement including account details is compulsory requirement.
  - Restrict the overwrite or amend the existing bank details recorded in the NRM without proper authorizations and verified supporting documents i.e, amendments to the loan agreements, letters from authorized officials from financial institutions etc. ( It was observed that this incident was occurred as a result of amendments and overwriting of existing records in the system during the period of the PDMO officials, under the supervision of officials of the CBSL).
  - Actions were taken to introduce maintaining a manual file to verify the payment details with a check list specified to each authorized level.
  - A process was introduced for reconciliation of payments made to the lenders during the period July 2025 – up to now through direct communication with lenders. It is expected to complete this process by 30<sup>th</sup> June 2026.
- Requests are made to the respective lenders for the confirmation of receipt of payments immediately after processing the payment, and the update the database accordingly upon receipt of such confirmation.
  - Actions are being taken to streamline and resolve the issues with the NRM system in coordination with CBSL. The NRM system was upgraded to the new NRM MX system in mid-January 2026. Under the new system, PDMO officials were unable to access all historical records from the previous NRM system, possibly due to incomplete migration of records to the new platform. Although certain past SSIs (Standard Settlement Instructions) were visible in the system, those entries had been created by “test users.” Consequently, in many instances, PDMO had to create new SSIs despite the fact that some payments had previously been processed successfully.
  - Actions taken to provide additional staff to PDMO and ERD where assistance of the Secretary to the Ministry of Public Administrations was requested to priorities the needs of PDMO and ERD.
  - Assistance of Ministry of Digital Economy obtained to ensure strengthening cyber security in consultation with relevant parties through which MOF and Treasury Departments are being connected to National Cyber Security Operational Center (NCSOC) Further, through the Digital Ministry a programme is being arranged to impart knowledge on cyber threats migratory measures and proactive identification, escalation and recording of incidences.

**Actions taken by ERD to strengthen the processes and internal controls**

- A process has been commenced to procure a latest version of mail server with advanced security features.
- The selected vendor has been informed to prioritize the activities to enhance the end point security and process is expected to complete shortly.
- A Process has been initiated to enhance the mail security through SL-CERT.
- In order to strengthen the coordination of activities and demarcation of responsibilities relating to Public Debt Management, ERD has handed over all the lender coordination activities related to Debt Servicing to the PDMO.
- Sought specialized technical assistance from the International Monetary Fund (IMF) to strengthen internal procedures of ERD. After the establishment of PDMO and enactment of the PDMA, the functions, authorities and responsibilities of ERD had changed. Therefore, in accordance with the provisions of PDMA, role of the ERD need to be reviewed.

**Actions taken by TOD to improve the processes**

Strengthening the process for the verification of the account details in the Monthly debt servicing forecast shared by PDMO with the details in the signed loan agreements and addendum to the original loan agreements. TOD will allocate required fund for the debt service only if the verification process is clear.

**Question No. 02**

**Documentary evidence confirming the delegation of financial control authority underpinning the existing payment process for all foreign debt repayments.**

- As per the past practice over the decades several departments of the Treasury including the departments of ERD, TOD, SAD and NBD, have contributed for the debt servicing process at different stages. Currently, the Debt Servicing vote is under the head of the TOD while repayment mechanism and contact with the relevant lenders being managed by ERD through PDD-CBSL and subsequently by PDMO.
- In terms of Section 6 (h) of the Public Debt Management Act No. 33 of 2024, the PDMO has been given authority to service the debts of the government on a timely basis.
- In terms of Section 5(2) of the said Act, the Director General of the PDMO is responsible for performing those functions.



**Highly Confidential**

- Accordingly, a set of guidelines has been issued on 19/09/2025, by the Minister in charge of the subject of finance in accordance with the authority vested in him by Section 7 of the Public Debt Management Act No. 33 of 2024 to ensure the internal control of those functions.
- In line with the above guidelines, the PDMO Back Office (BO) has been entrusted with debt servicing responsibilities. The functions are carried out under Directors responsible for the Debt Recording Unit (DRU) and Debt Servicing Unit (DSU), all of which are overseen by an Additional Director General (ADG/ BO).
- The debt servicing is totally processed through the Non Reserve Management (NRM) system and the authority levels has been clearly defined and implemented. The authority levels defined in NRM system as follows,
  - Entry Level - Development Officer
  - Verification Level - Assistant Director/ Deputy Director
  - Authorization Level - Director (Debt Servicing Unit)
- Debt servicing is done through the account of the Deputy Secretary to the Treasury (DST Account). Since this account is used to make payments in the form of the government debt servicing and other foreign exchange-denominated payments, it is assigned to the Treasury Operations Department (TOD) and maintained by the Central Bank of Sri Lanka. Therefore, the relevant section for the debt servicing vote is assigned under the budget head of the TOD.

**Question No. 03**

**Ensure that the debt management function have been fully transitioned to the Public Debt Management Office (PDMO), in accordance with the provisions of the Public Debt Management Act, No. 33 of 2024 (PDMA)**

According to the provisions of PDMA, all the debt management operations have been transferred to the PDMO to operationalize independently. As per the provisions of Section 6(b) of the PDMA, PDMO will coordinate with ERD for the negotiation with the bilateral and multilateral organizations.

**Question No. 04**

**Recognize cyber security as a fiscal risk and take comprehensive measures to prevent the recurrence of payment related issues and data breaches, which have become increasingly prevalent across public institutions in recent years.**

The required actions are being undertaken in consultation with CERT for the formulation and enforcement of a comprehensive cyber security policy framework. The measures being implemented include, the following:

- Enforcing compliance by all institutions under the Ministry with minimum cyber security standards, protocols, and regular security audits.
- Conducting technical awareness sessions and capacity-building programmes to enhance the understanding and technical knowledge of officials in relation to cyber security risks and preventive measures.
- Strengthening the capacities of the information Technology and Management Department of the Ministry of Finance to provide the necessary IT infrastructure, facilities, and technical expertise required within the Ministry.

**Question No. 05**

**Finalize the updated Financial Regulations currently being compiled to align with the Public Financial Management Act and the Public Debt Management Act, and submit the same for Parliamentary review at the earliest possible opportunity.**

Regulations under Public Financial Management Act No. 44 of 2024 (PFMA), which will replace the existing financial regulations, is in the process of finalization and expected to submit to Parliament prior to end July 2026.

Under the newly drafted regulations and the PFMA, provisions for the borrowings, loan guarantees, debt reduction objectives and debt sustainability have been included. Accordingly, Section 46 of the PFMA read as follow;

*"The policy framework on management of public debt and government guarantees shall be in accordance with the provisions of the Part III of this Act and subject to the related laws."*

Accordingly, the relevant regulations for regulate the debt servicing procedures will be issued under Public Debt Management Act No. 33 of 2024. Further, the detailed procedures will be documented in the Standard Operational Procedure Manual.



**Dr. P Nandalal Weerasinghe**

**GOVERNOR**

**Central Bank of Sri Lanka**

**30, Janadhipathi Mawatha, Colombo 1, Sri Lanka**

15 June 2026

Mr. Kamal Udapola

Secretary to the Committee

Committee on Public Finance (CoPF)

Department of Legislative Services – Committee Office 1

Parliament of Sri Lanka

Dear Mr. Udapola,

**Committee on Public Finance (CoPF)**

**Re: Meeting held on 08.06.2026**

This refers to the meeting of the Committee on Public Finance (COPF) held on 08 June 2026 concerning the report submitted by the Ministry of Finance on the alleged fraudulent foreign debt repayment transaction amounting to USD 2.5 million, and your letter dated 09 June 2026 requesting a detailed report on matters relating to foreign debt repayments and the transition of functions from the Public Debt Department (PDD) of the Central Bank of Sri Lanka (CBSL) to the Public Debt Management Office (PDMO) of the Ministry of Finance (MOF).

As requested, I hereby forward the following reports together with the relevant annexures:

1. A comprehensive report on the role of CBSL in effecting foreign debt repayments and the transition of functions from the PDD of the CBSL to the PDMO of the MOF
2. A report addressing the incorrect and incomplete information contained in the report submitted by the MOF and the statements made at the COPF meeting held on 08 June 2026

In view of the significance of these matters and to facilitate a comprehensive understanding of the facts and circumstances, we respectfully request an opportunity to meet with the members of COPF at the Committee's earliest convenience to discuss the contents of the attached reports.

Yours sincerely,

Cc: Dr. Harshana Suriyapperuma, Secretary to the Treasury and Ministry of Finance,  
Planning and Economic Development

## **Comprehensive Report of the Central Bank of Sri Lanka to the Committee on Public Finance**

### **(A) Preamble**

- (i) This has reference to the letter dated 9 June 2026 from Secretary to the **Committee on Public Finance** (COPF) requesting a comprehensive report from **Central Bank of Sri Lanka** (CBSL) as directed by the Hon (Dr) Harsha de Silva, Chair of the COPF, and the deliberations of the meeting of the COPF held on 8 June 2026 regarding the fraudulent foreign debt repayment transactions involving USD 2.5 million, and the Report submitted to the COPF by the Ministry of Finance (MOF) on the same.
- (ii) The aforementioned letter further requested the comprehensive report to detail the sequence of events, actions taken and applicable provisions relating to the issues surrounding foreign debt repayments, including the fraudulent transactions, rejected payments and the transition of functions from the Public Debt Department (PDD) of the CBSL to the Public Debt Management Office (PDMO).
- (iii) Accordingly, Section B of this Report provides a Background, Section C appraises the transition of functions from the PDD of the CBSL to the PDMO, Section D describes the role of CBSL in relation to foreign debt repayments and, Section E states the legal applicability of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) frameworks and Suspicious Transaction Reporting (STR) to Financial Intelligence Unit (FIU) of CBSL.
- (iv) It is pertinent to note that the PDMO was established to centralise the debt management functions carried out by departments of MOF such as External Resources Department (ERD) and Treasury Operations Department (TOD) in addition to the functions of PDD of the CBSL. This has also been recognised under the press release dated 18 December 2024 of MOF and Guidelines dated 19 September 2025 issued by H.E. the President (**Annex IA, Annex IB**).

## **(B) Background**

1. Under the Memorandum of Economic and Financial Policies (MEFP) entered into by the authorities with the International Monetary Fund (IMF) under the Extended Fund Facility programme (EFF) in March 2023, the Government committed to the following to restore public debt sustainability,

*‘Currently, public debt is managed by the CBSL’s Public Debt Department, the MOF’s External Resources Department and Treasury Operation Department. To improve debt management, we will complete necessary legislative requirements to establish a public debt management agency (PDMA) in line with international best practices by December 2023 and complete the establishment of the agency by December 2024. ‘*

2. The Government had already identified the requirement to ‘complete necessary legislative requirements to establish a public debt management agency (PDMA)’ under the MEFP of IMF-EFF in March 2023. The Central Bank of Sri Lanka Act, No. 16 of 2023 (CBSL Act) was enacted in September 2023.

3. Under ‘Transferring of Public Debt Management Functions of the CBSL to the PDMO – Legal Background’ in the report (page 5) submitted to the COPF by the MOF, it is stated that,

*‘When CBSL Act was passed by Parliament in 2023 it was envisaged that a separate law will be required to manage the Public Debt of the Government and to accommodate the new law CBSL Act introduces a temporary arrangement for Agency Functions of the CBSL on Public Debt Management.’*

4. In view of the above, the premise that such a requirement arose only after the enactment of the CBSL Act in September 2023 is not accurate. Rather, as per the programme objectives of the IMF-EFF, the authorities committed to the establishment of an operationally independent debt management agency to improve public debt management and debt transparency in March 2023.
5. During 2023 and 2024, the MOF obtained services of several technical assistance (TA) missions comprising experts from the IMF and the World Bank in drafting the Public Debt Management Bill and the regulations issued thereunder. The CBSL officials zealously and extensively contributed to these TA mission meetings, elaborating the then-existing frameworks, practices, and systems.
6. In 2025, the CBSL officials supported the PDMO by contributing to TA missions on ‘Enhancing the Primary Debt Market and Support to the Establishment of the Public Debt



Management Office’, ‘Developing an Investor Relations Strategy with Focus on Communication Policy’ and ‘Developing a Procedures Manual for Public Debt Management’ in January, March and June 2025, respectively.

7. The PDMO was established in December 2024 under the Public Debt Management Act, No. 33 of 2024 (PDM Act). At the initial discussions held with MOF attended by PDMO officials, CBSL was requested by MOF to provide PDMO officials with on-the-job training to take over public debt management operations performed by the PDD.
8. The PDMO by a letter dated 16 December 2024 requested the CBSL to facilitate an on-the-job training programme for its officers to take over debt management-related functions within the year 2025 (**Annex 2**).

*‘... we would be grateful if you could direct relevant officials to facilitate the on-the-job training for PDMO officials enabling them to takeover debt management functions carried out by CBSL as per the PDMA.’*

9. The PDMO by a letter dated 10 January 2025, requested that on-the-job training programme commence in March 2025 (**Annex 3**).

*‘We would like to extend our sincere gratitude for considering the our request to provide on-the-job training to the officials of the Public Debt Management Office...’ ‘...the training period is anticipated to be 2 to 3 months, commencing from March 2025.’*

10. **It has to be emphasized that the training provided to PDMO officials by PDD of CBSL had been carried out with due care, while performing time-critical operations in a strictly controlled environment and while maintaining strict precision of its operations.**
11. **The on-the-job training provided by PDD inter-alia covered operations of Front Office, Middle Office and Back Office of the PDD, namely;**
  - a. Conducting Domestic Debt Management Committee meetings, announcement of auction calendars, conducting of pre-bid meetings, issuance process of T-bills and T-bonds, dissemination of secondary market trade summary
  - b. Recommendation of maturity mixes for the T-bill and T-bond auctions, dissemination of secondary market quotes and statistics
  - c. Creation of Standard Settlement Instructions (SSI) and entering required information to the Non-Reserve Management (NRM) system in relation to the foreign debt servicing
  - d. Providing necessary information in relation to domestic debt servicing to the respective departments within the CBSL

12. However, it is important to note that the above on-the-job training programme didn't cover any of the functions, such as verifying the contents in the invoices, including payment instructions which had been hitherto carried out by ERD or any other MOF department. In any event, it was not possible for PDD to provide on-the-job training on any function carried out by ERD or any other department in the MoF.
13. The MoF requested CBSL to release one senior officer of the CBSL to the PDMO (**Annex 4**) and having considered the said request, one of the two Deputy Superintendents of Public Debt was released to the PDMO on a secondment basis, effective from 17 March 2025. The purpose of this secondment of a senior officer of PDD to the PDMO was to assist the process of transition through efficient coordination at the policy level between the PDD and the PDMO. Further, this was expected to facilitate the subsequent operational-level transition.
14. In May 2025, PDD wrote to three international rating agencies informing them of the establishment of the PDMO and that PDMO would be taking over the responsibility of liaising with international rating agencies (**Annex 5A, 5B, and 5C**).
15. Further, CBSL kept the market participants informed of the developments throughout the transition period transparently and proactively. Accordingly, at the Primary Dealer CEOs' meeting held on 20 March 2025, DG/PDMO was introduced to the primary dealer community. Meeting minutes are attached in **Annex 6**.

### **(C) Training provided to the PDMO by the CBSL**

16. PDD informed PDMO of the following arrangements relating to on-the-job training programme in January 2025 (**Annex 7**).
- a. on-the-job training to be provided in 2 successive groups consisting of 6 PDMO officials each,
  - b. the programme is expected to commence in March 2025 as requested, and
  - c. each group to undergo the training for a period of up to 2 months
17. On 25 February 2025, PDD informed that on-the-job training programme for PDMO officers can commence on 03 March 2025 (**Annex 8**). Meanwhile, to replicate the actual working conditions to the extent possible during on-the-job training programme, PDD took several measures with the support of the relevant departments where applicable, including but not limited to
- a. assigning a laptop to each PDMO official during the on-the-job training programme,

- b. creating individual login credentials for each PDMO official,
  - c. assigning a test system/ folder access,
  - d. maintaining attendance records, and
  - e. the PDMO officers were made aware of the Code of Conduct applicable to PDD officers and PDMO officers signed a declaration under a role specific Code of Conduct confirming their adherence to the requirements therein.
18. PDD conducted the on-the-job training programme for the first batch of PDMO officials from 03 March 2025 – 30 April 2025. The full list of participants is attached in **Annex 9**.
  19. On 14 May 2025, PDD informed the PDMO that the on-the-job training programme for the second batch of PDMO officials could commence on 15 May 2025. Further, it was informed that nominated PDMO officials from the first batch could also join the programme on need basis, as requested by the PDMO (**Annex 10**).
  20. PDD conducted the on-the-job training programme for the second batch of PDMO officials from 15 May 2025 to 30 June 2025. The full list of participants is attached in **Annex 11**.
  21. During the on-the-job training programme, at the request and coordination of PDD, all relevant departments within the CBSL that interact with PDD in its debt management-related and data dissemination activities conducted awareness sessions for PDMO officers on their respective roles (**Annex 12 and 13**). The purpose of this exercise was to ensure continued cooperation between PDMO and CBSL after PDD ceased its operations. For example, departments including Economic Research, Finance, Domestic Operations (Market Operations), International Operations (Investment Management), and Statistics made presentations on their operations to the PDMO.
  22. To facilitate the transition, two committees had been formed on 06 June 2025 namely, the Documentary Committee and the Establishment Committee (**Annex 14, 15 A and 15 B**) comprising officials from CBSL and the MOF. These two committees were chaired by one of the Additional Director Generals of PDMO. The Documentary Committee was tasked with reviewing, updating, and reissuing the relevant legal and procedural documentation necessary for the transition while the Establishment Committee was tasked with providing directions on IT and security infrastructure arrangements to the transition.
  23. At PDMO's request, the PDD shared its Operational Manual, Risk Register, and Code of Conduct with PDMO on 20 May 2025 (**Annex 16**).
  24. PDD initiated a Special Programme on "Valuation of Treasury Bonds" training programme at the Centre for Banking Studies, Rajagiriya, which was held from 12 - 13

June 2025 (**Annex 17**). At the invitation of PDD, several PDMO officials participated in this training.

25. On 04 August 2025, PDMO requested on-the-job training for a third batch of PDMO officials (**Annex 18**). Prior to providing such on-the-job training, PDD requested feedback on the effectiveness of the on-the-job training programme provided thus far, on 06 August 2025 (**Annex 19**).

26. On 18 August 2025, PDMO provided extremely positive feedback on the training provided by the PDD (**Annex 20**). Among others, it was mentioned that,

*'The opportunities provided under the well-deigned on-the-job training to PDMO officials with first-hand exposure to functions, operational procedures, and working culture of the PDD, which will be instrumental for the envisaged delivery of operations by the PDMO once it becomes fully operational.'*

*'Feedback from the participants highlights the high quality and openness of the training. They commended the PDD staff for their willingness to share knowledge without restriction, readiness to provide additional reading materials, and their practice of engaging in frequent insightful discussions to broaden understanding.'*

*'Participants further expressed appreciation for the inclusivity and professionalism demonstrated by all officers of the PDD, from senior management to the most junior staff, as well as the valuable contributions from other CBSL departments who supported the training. They emphasised that continuous practice and early adaptation of the knowledge gained are vital to ensure practical effectiveness.'*

*'In conclusion, we thank the PDD for conducting a program that not only transfers technical knowledge but also showcases a model of high efficiency, effective delegation, and excellent work ethics.'*

27. At the request of PDMO, PDD conducted another on-the-job training programme for a third batch commencing 02 September 2025 for a period of one month (**Annex 21**).

28. A specialized training programme on the Bloomberg trading and trade reporting platform was conducted at PDD premises for the benefit of officials in the PDMO during August - September 2025. The sessions were facilitated by a panel of Bloomberg experts based in Mumbai, India, and Hong Kong. The comprehensive curriculum delivered vital insights into the critical functionalities of the Bloomberg platform including the Bloomberg auction process and introduced several of Bloomberg's latest AI-driven initiatives. To ensure widespread capacity building, the programme was made accessible to all PDMO staff.

Following the virtual sessions, participants underwent practical, hands-on training via the Bloomberg terminal at PDD to deepen their operational knowledge of both the platform's advanced tools and Government securities mechanics.

29. At the Coordination Council meeting held on 23 September 2025, the Secretary to the Treasury informed the intention of taking over auction related responsibilities from PDD starting December 2025. Specifically, the relevant action point reads as follows:

***Action Point***

- *PDMO to independently carry out the auction process at PDD from mid-October 2025 under the existing approval procedures, while conducting auctions at PDD premises under its own approval process from November 2025. Subsequently, from December 2025 onwards, PDMO to conduct the entire auction process at the PDMO premises.*

30. The relevant extracts of the minutes are attached at **Annex 22**. It was further stated that it would be supportive if an experienced team from the CBSL were identified as a standby arrangement in the event of a requirement once the PDMO was fully operationalised. The Secretary to the Treasury, by a letter dated 25 September 2025 addressed to the Governor, informed the timeline to take over PDD operations pertaining to issuance and servicing of domestic Treasury securities (**Annex 23**).

- a. Auctions at PDD by PDMO officers from 13 October 2025 under the CBSL approval process
- b. From 1st week of November, PDMO was expected to completely takeover issuance process at PDD premises under the MOF approval process, and
- c. Operations at PDMO premises under the MOF approval process from the 1st week of December 2025.

31. With regard to debt servicing,

- a. **domestic debt servicing** was transferred to PDMO on 15 October 2025 (**Annex 24**), and
- b. **external debt servicing** - login credentials were created for PDMO officers granting access to the NRM system for:

- entering payment instructions on 13 October 2025, and
  - creation of SSI on 24 October 2025.
32. It must be noted that the NRM System is used by CBSL to generate SWIFT compatible payment messages to make foreign payments and it is not a debt management system.
  33. The Secretary to the Treasury, through a letter dated 31 October 2025 addressed to the Governor, while thanking the CBSL for the continued cooperation extended, particularly in supporting the transition of processes related to Government securities issuance and debt servicing, informed that PDMO would assume full responsibility for Government securities issuance process and debt servicing operations at the PDMO premises from the first week of December, not the first week of November as previously informed, as fulfilling necessary regulatory requirements, including Primary Dealer regulations to be issued under the PDM Act were not completed yet (**Annex 25**).
  34. From 02 December 2025 the officers of PDMO started conducting Government securities auctions at CBSL premises under MOF approval process. From the second week of December 2025, officers of PDMO commenced operations pertaining to Government Securities auctions at its own premises at MOF. PDD officers visited the PDMO to assist the PDMO with auction-related matters pertaining to issuance of Government Securities, in several instances, at its request. However, onsite assistance was not sought from PDD by PDMO in relation to Middle Office and Back Office functions, which entailed NRM related activities.
  35. During the first week of December 2025, at the request of PDMO, CBSL allowed PDMO officials to access PDD premises as the necessary infrastructure, including personal computers, that was not yet fully available at the PDMO premises. During the remainder of December 2025, PDD completed the administrative arrangements.
  36. Having completed administrative processes, PDD was closed down on 31 December 2025 and in this regard a closing down event was held at the CBSL attended by senior officials of MOF including PDMO and representatives from the Primary Dealer industry.
  37. Attendance records extracted from the Security Services Department of CBSL on the PDMO officials who participated in the on-the-job training programmes (**Annex 26 and 27**) and the areas covered under the on-the-job training programme (**Annex 28, 29 and 30**) are attached.
  38. In addition to on-the-job training programme, PDMO officials had received training not only through the CBSL but also through training programmes facilitated by international

organizations, such as IMF, Commonwealth Secretariat, and the World Bank, and foreign counterparts such as Thailand Debt Management Office, etc, both in physical and virtual form, providing exposure to global best practices, advanced technical knowledge, and emerging developments in public debt management throughout the transition period.

**(D) The role of CBSL in relation to foreign debt repayment**

39. CBSL, being the banker to the Government of Sri Lanka as per section 81 of the CBSL Act, No. 16 of 2023 effects foreign loan repayments of GoSL, complying with the following procedure:

- a. **During the time debt servicing was handled by PDD**, the Back Office of PDD received invoices from ERD of MoF through email with ERD's written authorisation on the Payment Invoice to effect the payment. The Back Office of PDD, using the invoice shared by ERD as the authorised source document enters the information into the NRM System to effect the payment. In the case where the authorised invoice sent by ERD contains new account details of the lender, based on the contents of such invoice, the Middle Office of PDD creates the SSI for such new account in the NRM System following a two-step entry and authorisation process. Once the completion of the entry, verification and authorisation of the transaction details in the NRM System against the authorised Payment Invoice received from ERD, the transaction flows to the FD through NRM System. After that Back Office of PDD generates the payment advice through NRM System and sends the email to the FD attaching the authorised invoice/ supporting documents received from ERD of MOF. On the value date, Back Office of PDD generates the respective payment voucher through the NRM System and forward it to the FD through email to debit the respective DST account.
- b. Once the PDMO took over the external debt servicing function in October 2025, the above-mentioned processes handled by PDD was discontinued.
- c. Thereafter, for each transaction, the FD of CBSL receives payment advice, which includes payment instructions of the lender, via email from the authorized signatories of PDMO. It is expected to receive the said documents two days before the value date of the loan repayment. **The responsibility of ensuring the accuracy of the said payment instructions falls strictly within**



**the responsibility of the ERD function that has been transferred to PDMO, and therefore the MOF.**

- d. FD checks the SWIFT message generated in the NRM System by the PDMO in relation to the payment, with the payment instructions provided in the authorized invoice/ supporting documents via email. If the data is in order, FD authorizes the SWIFT message in NRM System, based on the authorised limits in terms of the CBSL Manual. If there is any discrepancy in the data between the SWIFT message in NRM System and the authorized invoice/supporting documents, FD promptly informs PDMO of the same. (In instances where NRM System fails to generate SWIFT messages in the correct format, FD maps the payment details to the SWIFT format manually, checks the accuracy with the supporting documents and authorizes same SWIFT message).
- e. The authorized SWIFT message by FD is then transmitted automatically to the SWIFT system placed at the Payments & Settlements Department (PSD) of CBSL through NRM System. Subsequently, PSD releases the SWIFT message in the SWIFT system to effect the payment.
- f. FD records effected transactions in the General Ledger on the value date (or preceding working day, if a holiday) and recovers funds from relevant DST accounts (LKR via Account No. 50516 or USD via Account No. 45013) strictly in accordance with PDMO instructions.
- g. FD checks whether the processed loan repayments are reflected in the bank statements of CBSL's nostro accounts received on the following day. In case of the return of funds, FD informs PDMO promptly and transfers the returned funds back to the relevant DST's account, which was initially recovered on the value date/date of payment of each loan repayment.

40. CBSL's role as the Banker to the Government **does not** entail the following tasks which have been the Borrower's (Payer's) function, historically carried out by ERD, in relation to external debt servicing (bilateral, multilateral and syndicated loans) and continues to remain within the responsibility of MOF.

- a. Maintaining lender/country wise loan desks, maintaining authorized contact details of lenders and communications with lenders

- b. Verification of account details and accuracy of payment amount, value date of each loan repayment in line with the loan agreements or any other sources (eg. Previous payments).
  - c. Authorizing invoices of the lender, prior to sending the same to CBSL for effecting the payments.
  - d. Obtaining confirmations from the lenders on receipt of each loan repayment through a proper communication channel with the lender.
41. Loan repayments processed through CBSL under Export Finance Australia - Table 01 depicts all the said loan repayments; in the sequence they were processed through CBSL following the procedure mentioned in 39 (c to g) above.

**Table 01 - Loan Repayments processed through CBSL under Export Finance Australia**

| S/N | Payment Reference | Payment Date | Payment Amount   | Beneficiary Bank                                                   | Account Name                                                        | Account No. | Payment Advice and Invoice Auth orised by                                                          | Status                                                                                      |
|-----|-------------------|--------------|------------------|--------------------------------------------------------------------|---------------------------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1   | LR900             | 2025.11.14   | AUD 141,739.95   | Commonwealth Bank of Australia Sydney CTBAUAU25XXX                 | Mish Global LLC in care of Export Finance and Insurance Corporation |             | Payment Advice authorized by- PDMO (Annex 31.1a) Invoice authorized by- PDMO (Annex 31.1b)         | Completed                                                                                   |
| 2   | LR901             | 2025.11.14   | USD 713,758.88   | TD Bank NRTHUS33XXX                                                | Mish Global LLC in care of Export Finance and Insurance Corporation |             | Payment Advice authorized by- PDMO (Annex 31.2a) Invoice authorized by- PDMO (Annex 31.2 c,d,e)    | Completed                                                                                   |
| 3   | LR902             | 2025.11.14   | USD 1,375,882.11 | US Bank N.A. USBKUS441MT                                           | LMH Global LLC in care of Export Finance and Insurance Corporation  |             | Payment Advice authorized by- PDMO (Annex 31.2a) Invoice authorized by- PDMO (Annex 31.2b,f)       | Returned Note 1                                                                             |
| 4   | LR907             | 2025.11.28   | USD 377,660.26   | TD Bank NRTHUS33XXX                                                | Mish Global LLC in care of Export Finance and Insurance Corporation |             | Payment Advice authorized by- PDMO (Annex 31.3a) Invoice authorized by- PDMO (Annex 31.3b)         | Completed                                                                                   |
| 5   | LR913             | 2025.12.17   | USD 997,799.48   | WIO Bank WIOBAEADXXX (Intermediary Bank- Citibank USA CITIUS33XXX) | Sifra Watan Project Management Services EST                         |             | Payment Advice authorized by- PDMO (Annex 31.4a) Invoice authorized by- PDMO (Annex 31.4b)         | Funds Recalled by lender and intermediary bank returned the funds on request of CBSL Note 2 |
| 6   | LR944             | 2026.01.05   | USD 420,211.96   | TD Bank NRTHUS33XXX                                                | Mish Global LLC in care of Export Finance and Insurance Corporation |             | Payment Advice authorized by- PDMO (Annex 31.5a) Invoice authorized by- PDMO (Annex 31.5b,c,d,e,f) | Completed                                                                                   |

|   |       |            |                |                       |                                                                           |            |                                                                                                     |           |
|---|-------|------------|----------------|-----------------------|---------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------|-----------|
| 7 | LR957 | 2026.01.20 | USD 997,799.48 | TD Bank<br>NRTU533XXX | Mish Global LLC in care<br>of Export Finance and<br>Insurance Corporation | [REDACTED] | Payment Advice authorized by-<br>PDMO (Annex 31.6a)<br>Invoice authorized by- PDMO<br>(Annex 31.6b) | Completed |
|---|-------|------------|----------------|-----------------------|---------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------|-----------|

**Note 1:**

After processing the payment (LR902) by Federal Reserve Bank, the Beneficiary Bank (U.S Bank) has requested additional details on 18.11.2025 for which CBSL responded with the already available information on 18.11.2025. However, funds have been returned to CBSL nostro account with Federal Reserve Bank on 24.11.2025, as per the bank statements received on 25.11.2025. This return of funds was informed to PDMO on 25.11.2025. Meanwhile, a SWIFT message was sent to Federal Reserve Bank on 25.11.2025, requesting reason for returning funds, but no response was received. Returned funds were credited back to the relevant DST account (i.e. DST's Account No.50516).

**Note 2:**

On 26.11.2025, an email was received from PDMO to PDD-CBSL with resubmitted payment instructions by the lender as separate two invoices for the returned payment (LR902) for review with two sets of invoices carrying two different banking details. PDD-CBSL forwarded this email to FD-CBSL inquiring whether an intermediary bank is required for account details in one of the invoices (Sifra Watan Project Management Services EST (a/c [REDACTED]) with WIO Bank of UAE). on the same day, FD-CBSL informed PDD-CBSL that intermediary bank is required for this account with other concerns (the fact that the beneficiary address is in UAE and this may raise concerns regarding the debtor creditor relationship by the beneficiary bank) and requested to be informed to PDMO to communicate with the lender (Annex 32). This account details including an intermediary bank with an Australian beneficiary address has been submitted by PDMO (LR913). After processing the payment (LR913) by Federal Reserve Bank, the Intermediary Bank (Citibank) has informed on 23.12.2025 that they were unable to apply funds in the absence of related original initial payment reference. CBSL then verified that the payment reference (LR913) has been correctly placed in the SWIFT message and thus, informed PDMO on 24.12.2025 of this concern and to check this issue from the beneficiary's end. However, on 29.12.2025, PDMO requested to facilitate lender's request to recall the funds. Accordingly, CBSL sent a SWIFT message to Citibank requesting to recall the funds as instructed by Ministry of Finance on 29.12.2025. The funds were returned to CBSL nostro account with Federal Reserve Bank on 13.01.2026.

42. To assist with the investigations carried out concerning this incident, the aforesaid payments were matched with the respective invoice numbers in the emails as requested, and the summary is given in **Annex 33**. However, for FD of CBSL, as the banker to the Government, each foreign loan repayment is **a fresh transaction**, and loan repayments are processed based on the instructions given by the authorized officers of PDMO for each loan repayment. These invoices, including the amounts and account details of the lender, certified by officers of the Ministry of Finance indicating 'please pay' are considered as authorised payment instructions given by the authorized officers of PDMO.

#### **(E) Legal Applicability of AML/CFT Frameworks and Suspicious Transaction Reporting (STR)**

43. The Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) has been enacted with objectives including to facilitate the prevention, detection, investigation and prosecution of the offences of Money Laundering (ML) and Terrorism Financing (TF), respectively. Accordingly, Institutions coming under the purview of FTRA are required to undertake due diligence measures to combat money laundering and the financing of terrorism. In terms of Section 7 of the FTRA, where an "Institution" has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of the offences of money laundering, offences of financing of terrorism, any unlawful activity or any other criminal offence, such institution shall submit a Suspicious Transaction Report (STR) to the FIU at CBSL.

44. The compliance obligations under section 7 of the FTRA are applicable to the Institutions as defined in section 33 of the FTRA, i.e., "any person or body of persons engaged in or carrying out any finance business or designated non-finance business".

45. The CBSL established under the CBSL Act, No. 16 of 2023 does not come within the definitions of finance business or designated non-finance business. Accordingly, CBSL does not come within the scope of Section 7 of the FTRA, in any manner whatsoever.

46. Section 5 of the Prevention of Money Laundering Act, No. 5 of 2006 as amended (PMLA) states as follows;

47. “Any person who knows or has reason to believe from information or other matter obtained by him in the course of any trade, profession, business or employment carried on by such person, that any property has been derived or realised from any unlawful activity, shall disclose his knowledge or belief as soon as is practicable, to the Financial Intelligence Unit.”
48. In this background, as Section 5 universally applied to any person, the CBSL is also obliged to disclose such knowledge or belief to the FIU acting in terms of Section 5 of the PMLA. Since the funds in relation to the payment transaction under reference belonged to the Government, and thereby no suspicion would arise as to the origin, that would necessitate any reporting to the FIU.
49. Furthermore, each and every transaction which has mismatches, for instance, a debt repayment where the beneficiary is different from the lender, does not warrant submission of an STR to the FIU under section 7 of the FTRA.
50. The concerns raised by the officials of the FD of CBSL in relation to the particular payment is based on the due diligence aspects of the ongoing transaction scrutiny that would be carried out by the intermediary or beneficiary bank. Therefore, the comment made by the CBSL officer is based on the likelihood of the perception by the beneficiary bank of its compliance obligations, rather than any suspicion of ML for CBSL from an authorised invoice sent by MOF. Hence, the CBSL officers have informed the MOF “to communicate with lender to obtain the account details of Export Finance Australia for repayment of foreign loan successfully without being returned” (Annex 32). It is unfortunate that the MOF has inquired the above from the scammer instead of the actual lender.

**Report of the Central Bank of Sri Lanka in response to the  
Report of the Ministry of Finance to the Committee on Public  
Finance on Alleged Fraudulent Foreign Debt Repayment  
Transaction of approximately USD 2.5mn**

This report is submitted at the request made by the Committee on Public Finance (COPF) at its meeting held on 08.06.2026. This report is limited in scope to the extent of addressing incorrect and incomplete information contained in the Report submitted by the Ministry of Finance (MOF) and the statements made at the COPF meeting on 08 June 2026. This report shall be in addition to the comprehensive report filed of the same date by the Central Bank of Sri Lanka (CBSL) and shall not be construed as limiting, restricting or superseding the contents, findings, observations, or recommendations contained therein.

15.06.2026



## **1. Executive summary**

- 1.1. The diversion of the funds intended for a debt repayment to an Australian lender agency, into multiple accounts of criminal actors, is directly precipitated by tampered payment instructions been generated from the compromised email system at the Ministry of Finance (MOF).**
- 1.2. The enabling conditions that facilitated the said cyber theft arose from fundamental operational, governance, and process failures within the MOF. In particular, the officials entrusted with the critical responsibility of verifying and authenticating the accuracy of the payment instructions against the underlying loan documentation maintained by the External Resources Department (ERD) of the MOF failed to discharge their duties and functions. It is, therefore, evident that the compromise of the email system and the subsequent failure of the requisite verification controls by the MOF, enabled the fraudulent transactions to be executed unscrupulously.**
- 1.3. The Finance Department (FD) of CBSL as the banker to the Government had executed the payment instructions authorized and provided by the MOF to effect payments of the Government. The duty and responsibility to submit valid, accurate, and complete payment instructions are vested in the MOF.**
- 1.4. CBSL has not at any time, whether at the time of existence of the Public Debt Department (PDD) or after the closure thereof, carried out any functions of the ERD of the MOF pertaining to external debt servicing. This is evident in the allocation of duties to the Public Debt Management Office (PDMO) through the Guidelines issued by H.E. the President.**
- 1.5. CBSL has, at all times, facilitated the smooth transition of functions carried out by the PDD of the CBSL to PDMO established in the MOF. Comprehensive, structured, and systematic training and assistance was given to the officers attached to the PDMO by the officers of CBSL. Having obtained the relevant training, PDMO officers started entering transaction details into the Non-Reserve Management (NRM) System to effect foreign**

loan repayments from 13 October 2025 and creating Standard Settlement Instructions (SSIs) in the NRM System from 24 October 2025. Hence PDMO officers independently carried out both, SSI creation and transaction entering in the NRM system independently from 24 October 2025 using their own log-in credentials. Further, the training provided by PDD enabled the PDMO to independently carry out the auctions and issuance of domestic Treasury bills and Treasury bonds from the second week of December 2025, enabling PDMO to carry out independently all operations previously carried out by PDD from this date.

- 1.6. The evidence demonstrates that the root cause of the incident was totally outside of the CBSL and lays in the failure of ERD of MOF to properly and clearly transfer to PDMO the relevant knowledge and the responsibility of verifying the account details of the Payment Invoice with relevant source documents, prior to authorizing the Payment Invoice to effect the payment. This function was never a responsibility of PDD of CBSL. This failure of the governance framework within the MOF led to the failure to detect and prevent the submission of fraudulent payment instructions to PDMO officers who were creating SSIs in the NRM System, thereby allowing the diversion of public funds to fraudulent accounts. The creation of new SSIs of the fraudulent transactions by PDMO officers occurred just one month after the new loan agreements entered into between the lender (Export Finance Australia) and the MOF which was on 27 October 2025.
- 1.7. In essence, the cyber theft was not enabled by the processing of the payment by CBSL, training given by PDD to PDMO officers, or by any activity or function carried out by the CBSL, but by the breakdown of the fundamental verification safeguards within the MOF, which allowed a fraudulent payment instruction to be treated as an authentic instruction of the lender.

**2. Responses of the CBSL to the MOF statements quoted in the boxes below:**

**2.1. Question No.01 - 1.1 Detailed timeline of the events and actions taken so far by  
Ministry of Finance, Planning and Economic Development**

**2.1.1. Background information**

**(i) Bullet point 4 on page 2**

MOF stated....*"Then, a simultaneous process was commenced to train the newly recruited PDMO officials at the CBSL, under their supervision, from March to December 2025, under the direct supervision, the guidance of the PDD, CBSL officers, at the CBSL premises. From mid-October to December 2025, PDMO officials were allowed to work in the CBSL systems under their guidance and direct supervision. In this arrangement, the approval process and the regulatory framework of the CBSL were followed."*

**The above statement is factually incorrect.**

There was no direct supervisory involvement or any role for the CBSL to perform, with respect to entering transactions in the NRM System from 13 October 2025 onwards and with respect to creation of SSIs in the NRM System from 24 October 2025 onwards whereas those functions, (which entailed entering, verification and authorization) were carried out by the officials of the PDMO as evidenced by the NRM System logs. However, officials of PDD remained available to provide assistance and clarifications to PDMO officials whenever such assistance was requested. Therefore, any suggestion that CBSL continued to exercise supervisory control or bore responsibility for authorization or approval of activities undertaken within the NRM System in relation to external debt repayments after 24 October 2025 by the PDMO officers is factually incorrect.

**(ii) Bullet point 5 on page 2**

MOF stated .....Subsequently, MOF noted that the CBSL had closed the functions of PDD from 1st January 2026.

**The above statement is misleading.**

The closure of PDD of CBSL took place following the full operationalization of the PDMO of the MOF in December 2025. As recognized in the Memorandum of Understanding (MoU) between CBSL and MOF, *“the PDMO has taken over all related functions, responsibilities, and the authorities in issuing government securities and debt servicing since 1st December 2025 from the Public Debt Department of CBSL.”*<sup>1</sup> Accordingly, upon the transfer of debt management and servicing functions to the PDMO, there were no further functions or responsibilities relating to debt servicing being performed by the PDD of CBSL. Consequently, following the completion of the internal administrative procedures, the officers attached to the PDD were assigned to other departments of CBSL in order to ensure the effective utilization and deployment of the Bank’s human resources.

Nevertheless, as further recognized in the aforesaid MoU, *“Subject to service exigencies at their respective CBSL attachments, officers attached to the front and middle office of PDD, at the time of its cessation, shall continue to assist the PDMO on an as needed basis. This arrangement remains effective until the conclusion of the 18-month transition period, which commenced on 25 November 2024.*

Therefore, closure of the PDD as an administrative arrangement, and posting of the staff in PDD to other departments of the CBSL, were effected consequent to the PDMO becoming fully operationalized and the transfer of the relevant functions and responsibilities to the said Office as evidenced by the attached documents including the recitals in the MOU referred to above (**Annex 1**). An event to mark the official

---

<sup>1</sup> See reverse of page 58, paragraph 3 second sentence of the Report submitted to COPF by MOF

closure of the PDD was held on 29 December 2025 which was attended by a Deputy Secretary to the Treasury and Director General of PDMO.

### 2.1.2 Brief of the Events Occurred

#### (i) Item No. ( c ) on page 4

MOF stated .....*"After making an attempt to make the payment to the above bank in UAE, the payment had been rejected by the intermediary bank. Then the CBSL has informed PDMO, in the email trail exchange between the CBSL and the PDMO), that since the beneficiary address is different and located in a different State, it will be a matter regarding Anti-Money Laundering (AML)."*

#### **The above statement is factually incorrect.<sup>2</sup>**

With regard to the reference to the term "AML" in the same paragraph, the concerns raised by the officials of the Finance Department (FD) of CBSL in relation to the particular payment were based on the due diligence considerations applicable to the scrutiny of the transaction by the intermediary and/or beneficiary bank as part of their respective compliance processes. Accordingly, the observations made by the CBSL officer are premised on the potential perception or requirements of the beneficiary bank in fulfilling its AML compliance obligations, rather than any suspicion of money laundering arising on the part of CBSL in relation to an **authorised invoice** submitted by the MOF.

In this regard, the CBSL officers advised the MOF *"to communicate with lender to obtain the account details of Export Finance Australia for repayment of foreign loan successfully without being returned."* It is, therefore, of significant concern that, instead of obtaining confirmation of the relevant account details directly from the legitimate lender, the MOF proceeded to seek such information from the fraudulent source.

---

<sup>2</sup> The sequence of events stated in the paragraph is also incorrect. It will be explained in detail in the comprehensive report.

It is unfortunate that the precautionary measure raised by CBSL was not acted upon by the MOF through direct verification with the legitimate lender; instead, reliance was placed on the fraudulent source.

**(ii) Item No. ( e ) on page 4**

MOF stated .....*“The invoice amounting to US \$ 997,799.48, which was rejected 3 times, was paid into the same beneficiary account in TD Bank on 20th January 2026”*

**The above statement is factually incorrect.**

During the processing of the payments mentioned, only one payment (LR902) has been returned by the beneficiary’s bank, and another payment (LR913) has been recalled as requested by the lender through MOF. Therefore, the claim that the payments have got rejected three times is inaccurate. Accordingly, the assertion that the payments were repeatedly rejected three times has no factual basis and appears as an attempt of misrepresentation of events, rather than an accurate reflection of the actual payment processing history.

**(iii) Item No. (f) of page 4**

MOF stated.....*All of these payments were made to the TD Bank for the SSI created in the NRM system on 15th November 2025, during the training period at PDD, CBSL, by PDMO officials, under direct supervision, and approval process of CBSL*

**The above statement is factually incorrect.**

This SSI was created by the PDMO officials after completion of the training given on NRM activities and after the elapse of one full month from the date on which access to the NRM System had been provided to the PDMO officers, i.e. 13 October 2025. In fact, four SSIs have been created by the PDMO officers and seven transactions have been carried out, prior to the creation of the contentious SSIs in relation to the

Australian lender commencing 14 November 2025. This clearly demonstrates the effectiveness of the training and assistance provided by CBSL and confirms that PDMO officers had acquired the requisite knowledge and operational capability to independently perform their assigned functions. Furthermore, as evident by the system logs maintained by the CBSL (**Annex 2**), the activities related to creation of SSIs and entering transactions on the NRM System, have all been carried out by PDMO including entry, verification and authorization functions. At no stage was there any supervisory, approval, or intervention role exercised by CBSL in relation to these functions, as such functions had been fully transitioned to and were being independently performed by PDMO.

Therefore, the facts unequivocally demonstrate that the relevant functions had been fully transitioned to PDMO and were independently performed by its officers; any attempt to attribute responsibility to CBSL for processes that were exclusively within the operational control of PDMO would be inconsistent with the actual sequence of events and the evidence available. We further wish to point out that even though the report states that the SSI was created on 15 November 2025, a transaction had already been completed on 14 November 2025 using the same SSI created by PDMO officers on 14 November 2025.

**(iv) Last paragraph on page 4**

MOF stated.....*"It is observed that although the CBSL maintains that it acts solely as the banker to the government, the Ministry of Finance (MOF) is of the view that adequate attention does not appear to have been accorded to transactions, carrying potential Anti-Money Laundering (AML) implications, notwithstanding that such transactions had reportedly being identified by CBSL. In this context, the MOF further notes that despite functioning as the Government's banker, the CBSL has stated in its letter dated 20 May 2026 that the provisions of the Financial Transactions Reporting Act No. 6 of 2006 are not applicable to the CBSL. This position on dealing with AML concerns noted by CBSL, and the manner it was dealt raises concerns regarding the adequacy of regulatory oversight, internal compliance responsibilities, and the extent of accountability in relation to transactions identified as involving potential AML risks."*

**The above statement contains a legally untenable interpretation**

It is reiterated that in foreign debt servicing, the function performed by the CBSL is strictly limited to the role of the banker to the Government. While discharging its duties diligently, CBSL has always paid due attention to the completion of Government external debt service payments on time, without any delay or disturbance. Observations made by the CBSL officers from this perspective should not be construed as partial performance of AML related activities. It is emphasized that within the provisions of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA), or the Central Bank of Sri Lanka Act, No. 16 of 2023 (CBSL Act), there is no responsibility whatsoever for the CBSL, in the capacity of the banker to the Government, to exercise reporting requirements under the FTRA.

In such circumstances, any failure by the MOF, as the payment initiating party, to exercise the requisite due diligence cannot be attributed to CBSL or remedied by making unfounded allegations against CBSL, particularly where the responsibility for the accuracy and authenticity of the payment instructions rested with the MOF.



### 2.1.3 How and Why the Fraudulent Transaction Occurred

#### (i) Bullet 4- Pg 7

MOF stated.....*"The incident occurred during period when PDMO officials were working under the guidance and supervision of PDD officials of CBSL, under their approval process by using their operational platforms."*

#### **The above statement is factually incorrect.**

The incident in question arose from the failure of the responsible officers of the MOF to exercise the most fundamental verification and due diligence measures expected in relation to an external debt repayment transaction. The said officers of MOF had not identified the fraudulent email communication and, more critically, failed to authenticate the accuracy of the account details against the underlying debt agreement entered into with the Australian lender, which had been executed on 27 October 2025, less than one month prior, to the receipt of the Payment Invoices from the lender on 13 November 2025.

It is of particular significance that this failure occurred at the stage of initiation and validation of the payment instructions at the MOF, well before any creation of SSIs or entry of transaction details into the NRM System. Therefore, any attempt to attribute responsibility to processes or functions within the NRM System, or to CBSL officers who were earlier associated with such NRM processes, is fundamentally misplaced and unsupported by the sequence of events, since the incident occurred due to the negligence of the MOF officers who had the responsibility to verify the details of the Payment Invoice they received from the lender and failed to effectively carry out that activity.

**(ii) Bullet 5 – Pg.7**

MOF stated ....*“The newly recruited officials of PDMO may not have possessed adequate expertise on banking operations, particularly in relation to the international fund transfer mechanisms, Anti-Money laundering activities, and international financial frauds associated with cybercrimes. In this context, employees of the view that it was reasonably expected, that the CBSL, in its capacity as the banker to the Government, and the regulator of the banking sector, would continue to discharge its banking and supervisory responsibilities in a manner consists with the spirits and objectives of the Financial Transaction Reporting Act, No. 6 of 2006.”*

**The above statement is untenable.**

The attempt to associate CBSL’s regulatory, supervisory, banking, or Financial Intelligence Unit (FIU) functions with an incident originating from the failure of internal controls at loan desks of the MOF reflects a fundamental misunderstanding or misrepresentation of institutional mandates and accountability structures. The root cause of the incident lies within the processes and responsibilities of the institution that is originating the payment instruction, and the responsibilities for same cannot be displaced onto an institution performing entirely separate statutory functions. It is pertinent to emphasize that the failure to verify the credentials of the actual payee has taken place exclusively within a function that has been carried out in the MOF both before and after the establishment of the PDMO. In those circumstances, any duty to train officers of PDMO in that specific area was squarely within the mandate of the MOF. In these circumstances, this statement exemplifies the lack of understanding on the part of the MOF, of the functions of different departments of CBSL, as well as the functions of MOF’s own departments, specifically, that of ERD and PDMO and the demarcation of their internal responsibilities with regard to external debt repayments.

#### **2.1.4 Institutional Issues Identified**

##### **(i) Bullet 1 Page 9 on Central Bank of Sri Lanka (CBSL)**

MOF stated.....*"It is observed that BO of PDD has not properly guided trainee PDMO officials to the use the account details of the beneficiary, which has been recorded in the NRM, instead has guided to change it based on the invoices received."*

##### **The above statement is categorically denied.**

With regard to transactions for Export Finance Australia, PDMO has created four new SSIs in the NRM Systems, based on the account details on the invoices authorized by MOF. It is to be specifically highlighted that the NRM System merely facilitates the execution of authorized payment instructions received from MOF (having passed through the MOF's internal processes). By design, the NRM System is not intended to replace or duplicate the verification responsibilities of the MOF. As stated above, the issue has arisen because MOF had failed and neglected to verify the contents of the said invoices so authorized by them, against the agreements. The training provided by PDD was only with regard to functions carried out by PDD, and it did not cover the verification functions carried out by MOF. The critical failure was the absence of adequate verification at the point of origination of the payment instruction at the MOF.

### **2.1.5 Measures taken by Ministry of Finance to strengthen the External Debt Servicing Process**

**(i) Bullet 2 page 10 on actions taken by ERD to strengthen the process and internal controls.**

*MOF stated.....Restrict the override or amend the existing bank details recorded in the NRM without proper authorizations, and verified supporting documents. i.e. amendments to the loan agreements, letters from authorised officials from financial institutions, etc. **(It was observed that this incident was occurred as a result of amendments and overwriting of existing records in the system during the period of the PDMO officials under the supervision of officials of the CBSL.)***

**The above statement in parenthesis is categorically denied.**

With regard to transactions for Export Finance Australia, PDMO has created four new SSIs in the NRM Systems, based on the account details on the invoices authorized by MOF. Based on system logs, there was no amendment or overwriting of any single SSI already existing in the NRM system (Annex 2). We reiterate that the incident occurred because MOF had failed and neglected to carry out such verifications against the supporting documents, such as loan agreements, and amendments to the loan agreements which are available with the MOF.

**Accordingly, the critical failure did not occur at the stage of processing the payment instruction through the NRM System; it occurred at the very first line of defense, where the MOF had the responsibility and the necessary documentation to verify whether the instruction reflected a genuine contractual obligation. Once an unauthenticated instruction was authorized by the MOF, subsequent processing systems could not reasonably be expected to detect a defect that originated outside their operational mandate.**



SRI LANKA  
CERT/CC

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංඝයා  
இலங்கை கணினி அவசர தயාර்நிலை அணி  
Sri Lanka Computer Emergency Readiness Team

කාමර අංක. 4-112, ඩී.එම්.ආයි.සී.එම්, බෞද්ධාලෝක මාවත, කොළඹ 07.  
அறை இல. 4-112, பி.எம்.ஐ.ஸி.எச், பெளத்தாலோக மாவத்தை, கொழும்பு 07.  
Room No. 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07.

Consultants, LOPE

I'm sending herewith 13 annexures  
received from CERT for your perusal  
and due analysis p/r. SSS

Our Ref: CERT/106/ADMIN/Mode/003 (ADA/G)

10/06/2026

09<sup>th</sup> June 2026

Secretary to the Committee  
Committee on Public Finance (CoPF)  
Parliament Secretariat  
Parliament of Sri Lanka

Through

Secretary  
Ministry of Digital Economy

09/06/2026



Dear Chairperson and Members of the CoPF Committee,

**Committee on Public Finance: Submission of Cyber Security Reports and Clarification on the Status of the ERD Email Server**

This is with reference to the CoPF meeting held on 8 June at Parliament. As directed by the Committee, Sri Lanka CERT wishes to submit the cyber security reports prepared for the Ministry of Finance.

We also wish to provide further clarification on the status of the Email Server of the External Resources Department (ERD) as presented in the Section 2 of this letter.

**1. Reports Prepared by Sri Lanka CERT and Cyber Security Guidelines**

**A. Cabinet-Approved Information and Cyber Security Policy for Government Organizations.**

This policy defines the baseline security standards required to protect the digital infrastructure and information assets of government organizations. The Cabinet of Ministers has directed all government organizations designated as Public Authorities under the Right to Information Act to implement this policy and ensure compliance with the prescribed baseline security standards.

| # | Document Title                                                                                  | Date of Issue                                         | Annexures  |
|---|-------------------------------------------------------------------------------------------------|-------------------------------------------------------|------------|
| 1 | Cabinet Decision on Information and Cyber Security Policy (Policy) for Government Organizations | Cabinet Decision 22/1173/630/001, Date 2022 August 31 | Annexure I |

|   |                                                                                                                         |                                                  |             |
|---|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-------------|
| 2 | Circular issued for Government Organizations to implment the Policy, and the tist of Critical Information Infrastrcture | 2023 May 2, Issued by the Ministry of Technology | Annexture 2 |
| 3 | Cabinet approved Information and Cyber Security Policy for Government Organizations                                     | Date 2022 August 31                              | Annexture 3 |
| 4 | Cabinet Approved Information and Cyber Security Strategy (2025: 2029)                                                   | 22 July 2025                                     | Annexture 4 |

**B. Instructions to Critical Government Organizations (including the Ministry of Finance) to Connect to the National Cyber Security Operations Centre (NCSOC)**

The Cabinet of Ministers has directed all critical government organizations, including the Ministry of Finance, to establish connectivity with the National Cyber Security Operations Centre (NCSOC) to strengthen the monitoring and protection of government digital infrastructure. The NCSOC aims to monitor real-time cyber threats affecting subscribing government organizations on a 24/7 basis.

| # | Document Title                                                                                                                                                               | Date of Issue                                                      | Annextures  |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------|
| 5 | Cabient Decsion: Connecting Government Organizations that maintain Critical National Information Infrastrcture to the National Cyber Security Operations Centre (NCSOC)<br>* | Cabinet Decsion: 25/1429/805/014, Date 2025 August 26              | Annexture 5 |
| 6 | Instructions to the Critical Government Organizations (including Ministry of Finance) to the NCSOC                                                                           | Letters sent: 24-03-2025<br>03-10-2025<br>21-01-2026<br>26-03-2026 | Annexture 6 |

\*The Ministry of Finance is currently in the process of establishing connectivity with the NCSOC.

**C. Security Assessments Conducted by Sri Lanka CERT to the Ministry of Finance (Prior to incidents)**

The following reports were prepared to assess and identify cyber security gaps within the Ministry of Finance. The Ministry is expected to remediate the identified vulnerabilities and implement the recommended measures to strengthen its overall cyber security posture.

Note: The systems listed in Item 9 of the above Table were selected based on a request from the Treasury's Information Technology Management Department (ITMD), and the reports were subsequently submitted to the ITMD of the Ministry of Finance.



| # | Document                                                                                                                                                                                                                                                                                                                                              | Date of Issue                       | Annexures   |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------|
|   | As per the Section 6 of the Cabinet Approved Information and Cyber Security Policy (Reference: Item 1, Subsection A), the government organizations are required to conduct a self assessment on the implmenation of the Policy.                                                                                                                       | On annual basis, from October, 2023 | Annexture 3 |
| 7 | Information Technology Governance Controls (ITGC) Review by KPMG in consultatation with Sri Lanka CERT (Final Report)                                                                                                                                                                                                                                 | 24 December 2024                    | Annexture 7 |
| 8 | Closure Meeting Report (summary) ITGC. KPMG Report prepared in consultation with Sri Lanka CERT                                                                                                                                                                                                                                                       | 24 December 2024                    | Annexture 8 |
| 9 | ITGC Control Review Observation Log for Selected Systems of Ministry of Finance <ul style="list-style-type: none"> <li>o Department of Development Finance (DFD): LMS Senior Citizen SystemDepartment</li> <li>o Treasury Operations Department (TOD): TFMS, GFLSMS</li> <li>o Department of State Accounts (SAD): CIGAS, E-Payroll, ITMIS</li> </ul> | 19th January 2026                   | Annexture 9 |

**D. Confidential Reports Submitted to the External Resources Department (ERD) Between February and April 2026 Regarding Email Incidents.**

The reports were prepared based on information provided by the ERD, and each report contained actionable recommendations that should be implemented by the ERD to prevent similar email-related incidents.

| Document                                                                      | Date of Issue                  | Remarks                  |
|-------------------------------------------------------------------------------|--------------------------------|--------------------------|
| Preliminary Report for the Email Incident (Belgium)                           | 19 <sup>th</sup> February 2026 | Reports submitted to ERD |
| Forensic Investigation Report on the Email Impersonation Incident (Australia) | 30 <sup>th</sup> March 2026    |                          |
| ERD Report - France Communication                                             | 10 <sup>th</sup> April 2026    |                          |
| Higlevel Note – German Embassy email Incident                                 | 30th April 2026                |                          |

Following the reporting of the incident to Sri Lanka CERT in January, a discussion was held with the ERD, and recommendations were provided to address the identified issues and strengthen the security of its email systems.

#### **E. Technical Reports Submitted to the Ministry of Finance Between March and April 2026 Regarding the Security Posture of the ERD and the Ministry of Finance.**

Following the identification of the email-related incidents, Sri Lanka CERT conducted assessments of internet-facing systems and identified several security vulnerabilities. The findings and recommendations were submitted to the ERD and the Ministry of Finance for appropriate remediation and risk mitigation.

| #  | Document                                                                       | Date of Issue   | Annextures   |
|----|--------------------------------------------------------------------------------|-----------------|--------------|
| 10 | External Attack Surface Scanning Report for Ministry of Finance                | 23rd April 2026 | Annexture 10 |
| 11 | External Attack Surface Scanning Report for ERD                                | 23rd April 2026 | Annexture 11 |
| 12 | Public Observable Security Vulnerability Assessment Report for erd.gov.lk      | 24th April 2026 | Annexture 12 |
| 13 | Public Observable Security Vulnerability Assessment Report for Treasury.gov.lk | 24th April 2026 | Annexture 13 |

## **2. Clarification of Microst Exchange Server 2016 of ERD**

Sri Lanka CERT wishes to respectfully clarify a statement made during the Committee proceedings regarding Microsoft Exchange Server 2016. During the discussion, it was inadvertently stated that the product had reached End-of-Life (EOL) in 2019. The intended reference was to the end of the product's Mainstream Support phase, which concluded in October 2020. Microsoft Exchange Server 2016 remained within Microsoft's support lifecycle under the Extended Support phase and continued to receive security updates until October 2025. Accordingly, it would not be technically accurate to state that the product reached End-of-Life in 2019, and Sri Lanka CERT wishes to correct the record in this regard.

### **Exchange Server 2016 Lifecycle**

Microsoft Exchange Server 2016 was released in October 2015 and follows Microsoft's Fixed Lifecycle Policy. Microsoft's official lifecycle records show:

| Lifecycle Stage          | Date            | Significance                                               |
|--------------------------|-----------------|------------------------------------------------------------|
| Product Release          | October 2015    | General Availability                                       |
| Mainstream Support Ended | 13 October 2020 | No further feature updates; transition to extended support |
| Extended Support Ended   | 14 October 2025 | End of regular security updates and technical support      |



|                      |                 |                                                                   |
|----------------------|-----------------|-------------------------------------------------------------------|
| End of Support (EOL) | 14 October 2025 | Product became unsupported unless covered by special arrangements |
|----------------------|-----------------|-------------------------------------------------------------------|

From a cybersecurity perspective, however, the concern being highlighted by Sri Lanka CERT related to the fact that the affected platform was operating in the latter stages of its lifecycle. Following the end of Mainstream Support, enterprise systems require increased attention to security maintenance, patch management, vulnerability management, and technology refresh planning.

Accordingly, the observation made during the Committee proceedings was intended to emphasize the cybersecurity implications associated with operating an older enterprise messaging platform, rather than to suggest that the product had formally reached End-of-Life in 2019.

We regret the inadvertent reference to 2019 and respectfully request that this clarification be reflected in the Committee's records to ensure technical accuracy.

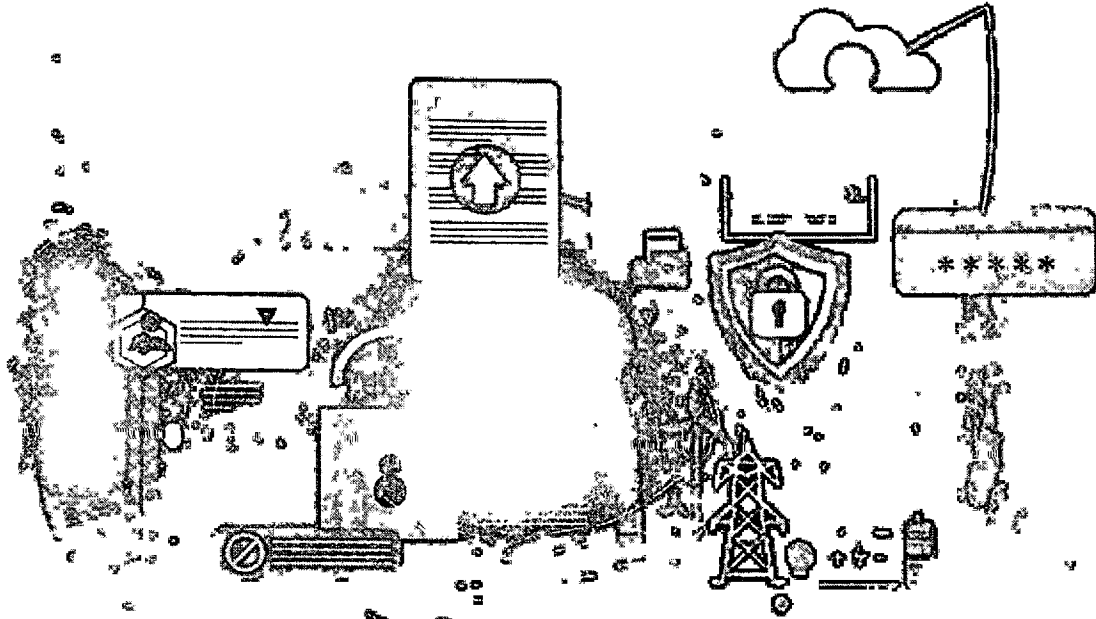
Thank you

Yours faithfully,  
Sri Lanka CERT

  
Dr. Kanishka Karunasena  
Chief Executive Officer (Actg.)

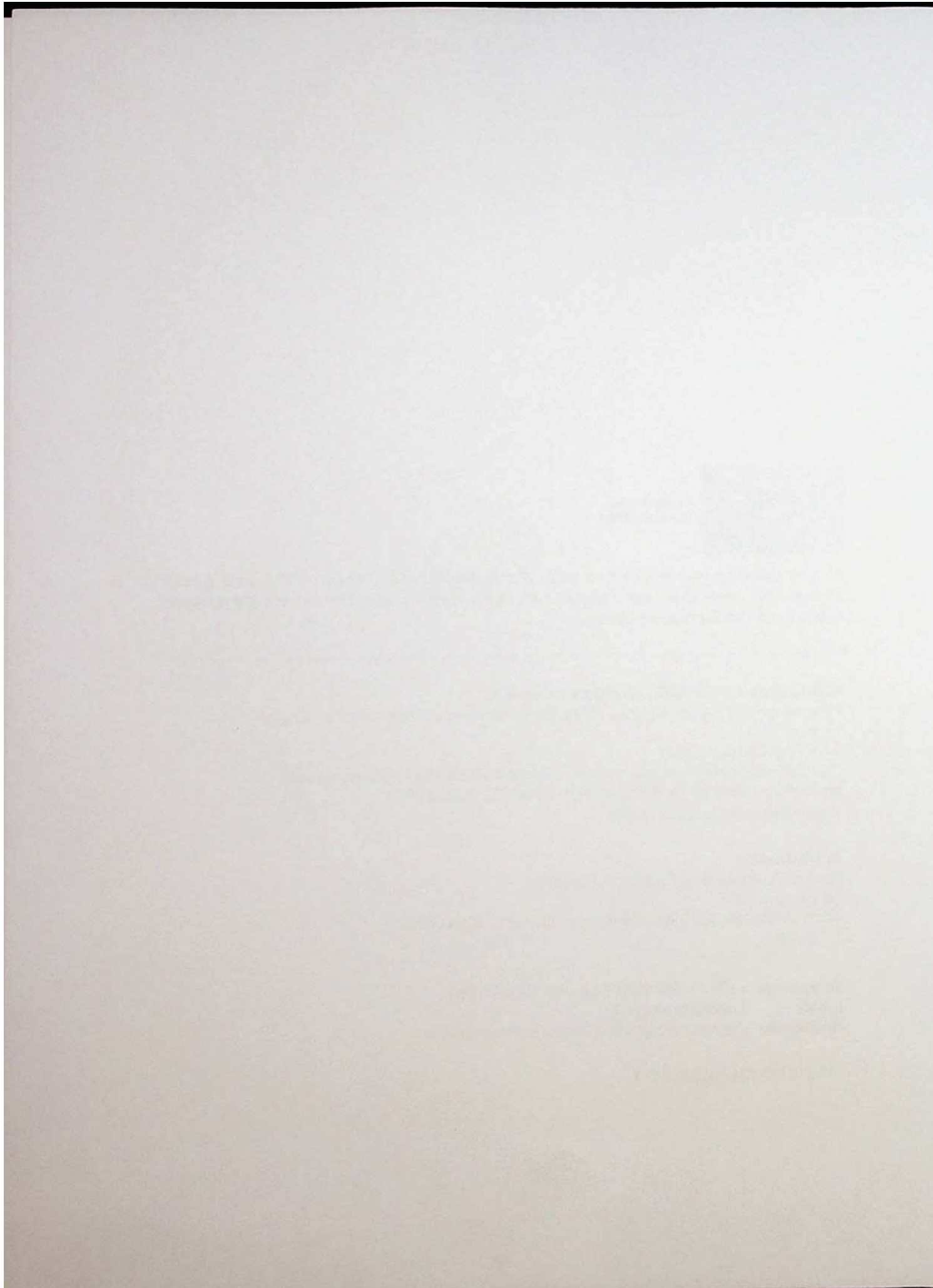
**Dr. Kanishka Karunasena**  
Acting Chief Executive Officer  
**SRI LANKA CERT I CC**  
Room No. 4-112, BMICH  
Buddhaloka Mawatha,  
Colombo 07

## Annex 6

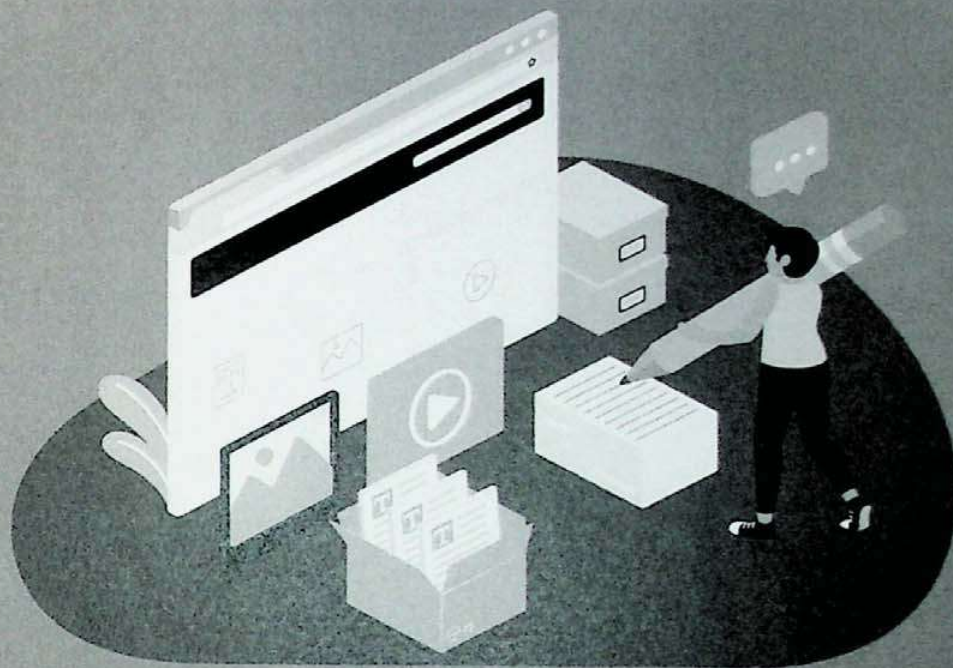


### INFORMATION AND CYBER SECURITY POLICY FOR GOVERNMENT ORGANIZATIONS

அரசாங்க நிறுவனங்களுக்கான  
தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கை







# Contents

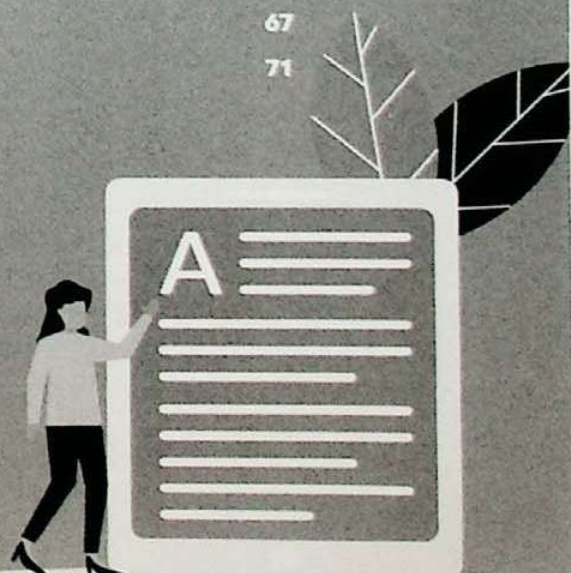
|        |                                                        |    |
|--------|--------------------------------------------------------|----|
| 1.     | <b>Introduction</b>                                    | 7  |
| 2.     | <b>Information and Cyber Security Policy Framework</b> | 9  |
| 3.     | <b>Information and Cyber Security Policy</b>           | 12 |
| 3.1.   | <b>Objectives</b>                                      | 12 |
| 3.2.   | <b>Scope of the Policy</b>                             | 13 |
| 4.     | <b>Policy Statements</b>                               | 18 |
| 4.1.   | <b>Information and Cyber Security Governance</b>       | 18 |
| 4.1.1. | <b>Leadership</b>                                      | 19 |
| 4.1.2. | <b>Security Organization Structure</b>                 | 19 |
| (a)    | Role of Information Security Officer (ISO)             | 20 |
| (b)    | Role of Chief Innovation Officer (CIO)                 | 20 |
| (c)    | Role of (Chief) Internal Auditor (IA)                  | 20 |
| 4.1.3. | <b>Information Security Committee (ISC)</b>            | 21 |
| 4.1.4. | <b>Risk Management Committee (RMC)</b>                 | 21 |
| 4.1.5. | <b>Responsibilities of End Users</b>                   | 21 |
| 4.1.6. | <b>Capacity Building</b>                               | 22 |
| 4.1.7. | <b>Security Clearance of Staff</b>                     | 22 |



|      |         |                                                                       |    |
|------|---------|-----------------------------------------------------------------------|----|
|      | 4.1.8.  | Strategic Alignment                                                   | 23 |
|      | 4.1.9.  | Action Plans and Resource                                             | 23 |
|      | 4.1.10. | Compliance                                                            | 23 |
| 4.2. |         | <b>Identify Assets, Owners, Users and Risks</b>                       | 24 |
|      | 4.2.1.  | Identification of Information and Information Technology Assets       | 24 |
|      | 4.2.2.  | Identification of Critical National Information Infrastructure (CNII) | 25 |
|      | 4.2.3.  | Responsibilities of Asset Owners, Custodians and Users                | 25 |
|      | 4.2.4.  | Maintaining Information and IT Assets                                 | 26 |
|      | 4.2.5.  | Assessments Risk                                                      | 27 |
|      | 4.2.6.  | Classification of Assets                                              | 27 |
| 4.3. |         | <b>Protect Assets</b>                                                 | 28 |
|      | 4.3.1.  | Protection of Data-at-Rest                                            | 28 |
|      | 4.3.2.  | Protection of Data-in-Transit                                         | 29 |
|      | 4.3.3.  | Physical Protection                                                   | 29 |
|      | 4.3.4.  | Identity Management and Access Control                                | 30 |
|      | 4.3.5.  | Strong Authentication                                                 | 31 |
|      | 4.3.6.  | Data Sovereignty and Cloud Computing                                  | 32 |
|      | 4.3.7.  | Licensed Software and Patch Updates                                   | 34 |
|      | 4.3.8.  | Antimalware                                                           | 34 |
|      | 4.3.9.  | Official Emails                                                       | 35 |
|      | 4.3.10. | Security of Emails                                                    | 35 |
|      | 4.3.11. | Digital Signatures                                                    | 36 |
|      | 4.3.12. | Perimeter Security Controls                                           | 36 |
|      | 4.3.13. | Secure Remote Access                                                  | 36 |
|      | 4.3.14. | Backup Strategy                                                       | 37 |
|      | 4.3.15. | Security of Assets Supplied by Government Organizations               | 38 |
|      | 4.3.16. | Security-by-Design                                                    | 39 |
|      | 4.3.17. | Secure Disposal of Assets                                             | 39 |



|         |                                                                                     |    |
|---------|-------------------------------------------------------------------------------------|----|
| 4.3.18. | Internal Information and Cyber Security Audit Process                               | 40 |
| 4.3.19. | Audits Prior to Deployment                                                          | 41 |
| 4.3.20. | Systems Hardening                                                                   | 41 |
| 4.3.21. | Work from Home                                                                      | 42 |
| 4.3.22. | Using Personal Devices for Official Work                                            | 43 |
| 4.3.23. | Using Non-Secure Networks                                                           | 44 |
| 4.3.24. | Management of Suppliers                                                             | 44 |
| 4.3.25. | Change Management                                                                   | 44 |
| 4.4.    | Detect Incidents                                                                    | 45 |
| 4.4.1.  | Reporting Incidents                                                                 | 45 |
| 4.4.2.  | Reviewing Logs                                                                      | 46 |
| 4.4.3.  | Continuous Monitoring of Incidents                                                  | 47 |
| 4.4.4.  | Reporting Incidents to Sri Lanka CERT                                               | 47 |
| 4.5.    | Respond to Incidents                                                                | 47 |
| 4.5.1.  | Incident Response Plan                                                              | 48 |
| 4.5.2.  | Activating Incident Response Plan                                                   | 48 |
| 4.5.3.  | Forensic Investigations                                                             | 49 |
| 4.6.    | Recover Normal Operations                                                           | 50 |
| 4.6.1.  | Disaster Recovery Plan                                                              | 51 |
| 4.6.2.  | Activating Disaster Recovery Plan                                                   | 51 |
| 4.6.3.  | Crisis Communication                                                                | 51 |
| 5.      | Policies to be Implemented on a Priority Basis                                      | 52 |
| 6.      | Methodology for Monitoring and Evaluating the Information and Cyber Security Policy | 56 |
|         | Glossary                                                                            | 67 |
|         | References                                                                          | 71 |



## Acronyms

|                  |                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AMC</b>       | Audit and Management Committee                                                                                                            |
| <b>CCTV</b>      | Closed-circuit Television                                                                                                                 |
| <b>CD</b>        | Compact Disk                                                                                                                              |
| <b>CERT</b>      | Computer Emergency Readiness Team                                                                                                         |
| <b>CNII</b>      | Critical National Information Infrastructure                                                                                              |
| <b>CIO</b>       | Chief Innovation Officer                                                                                                                  |
| <b>DVD</b>       | Digital Video Disc                                                                                                                        |
| <b>HOO</b>       | Head of Organization                                                                                                                      |
| <b>HTTPS</b>     | Hypertext Transfer Protocol Secure                                                                                                        |
| <b>ICTA</b>      | Information and Communication Technology Agency                                                                                           |
| <b>IA</b>        | Internal Auditor                                                                                                                          |
| <b>IPS/IDS</b>   | Intrusion Prevention System/Intrusion Detection System                                                                                    |
| <b>ISC</b>       | Information Security Committee                                                                                                            |
| <b>ISO</b>       | Information Security Officer                                                                                                              |
| <b>ISO 27002</b> | International Organization for Standardization for Information Technology – Security Techniques - Information Security Management Systems |
| <b>IT</b>        | Information Technology                                                                                                                    |
| <b>LGC</b>       | Lanka Government Cloud                                                                                                                    |
| <b>LGN</b>       | Lanka Government Network                                                                                                                  |
| <b>MFA</b>       | Multifactor Authentication                                                                                                                |
| <b>MISS</b>      | Minimum Information Security Standards                                                                                                    |
| <b>NDA</b>       | Non-Disclosure Agreement                                                                                                                  |
| <b>NIST</b>      | National Institutes of Standards and Technology                                                                                           |
| <b>PIN</b>       | Personal Identification Number                                                                                                            |
| <b>RMC</b>       | Risk Management Committee                                                                                                                 |
| <b>RPO</b>       | Recovery Point Objective                                                                                                                  |
| <b>RTO</b>       | Recovery Time Objective                                                                                                                   |
| <b>SFTP</b>      | Secure File Transfer Protocol                                                                                                             |
| <b>SIEM</b>      | Information and Event Management                                                                                                          |
| <b>SSD</b>       | Solid-state Drive                                                                                                                         |
| <b>SLA</b>       | Service Level Agreement                                                                                                                   |
| <b>SSL</b>       | Secure Socket Layer                                                                                                                       |
| <b>TLS</b>       | Transport Layer Security                                                                                                                  |
| <b>USB</b>       | Universal Serial Bus                                                                                                                      |
| <b>VPN</b>       | Virtual Private Network                                                                                                                   |





## 1. Introduction

---

- 1.1 Many government organizations in Sri Lanka now depend on the reliable functioning of digital systems and infrastructure. Malicious actors, however, can exploit these digital systems to cause harms such as theft of sensitive information, disruption of day to day operations, damage to the reputation of organizations which in turn can lead to the loss of public trust and confidence in government systems, and place nation's security, economy, safety and wellbeing at a risk.
- 1.2 To effectively address these information and cyber security risks and to protect the information, digital systems and infrastructure (hereinafter, information and information technology assets) of government organizations from various threats, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the organization which has the mandate to protect the cyberspace of Sri Lanka, has developed an Information and Cyber Security Policy for the use of government organizations. The Policy provides a risk-based



approach for implementing an information and cyber security program at the organizational level. It also provides a set of actions that organizations should implement to identify and protect assets, detect information security incidents in a timely manner, respond to incidents and recover from cyberattacks in an efficient and effective manner.

- 1.3 The Information and Cyber Security Policy for Government Organizations is developed in line with the implementation of the Information and Cyber Security Strategy of Sri Lanka (2019: 2023). It is developed based on the international standards and best practices such as International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) of the United States of America, and has been extensively reviewed by information security experts and senior officers of the government.
- 1.4 All government organizations that are defined as 'Public Authorities' in the Right to Information Act No 12 of 2016, are required to comply with this Policy. The heads of government organizations shall be responsible and accountable for the implementation of the Policy to ensure safe and efficient service delivery within their organizations. Sri Lanka CERT shall facilitate and provide recommendations to all government organizations in implementing the Policy, and shall assess the performance of organizations in implementing the Policy on an annual basis.





## 2. Information and Cyber Security Policy Framework

---

- 2.1 The Information and Cyber Security Policy Framework introduces the guidance material required by government organizations to implement information and cyber security programs in an efficient and effective manner. It includes (a) the Information and Cyber Security Policy, (b) the Minimum Information Security Standards, (c) the Information and Cyber Security Implementation Guide, and (d) a methodology to monitor and evaluate the implementation of the Information and Cyber Security policy at government organizations. Figure 1 presents an overview of the Information and Cyber Security Policy Framework.



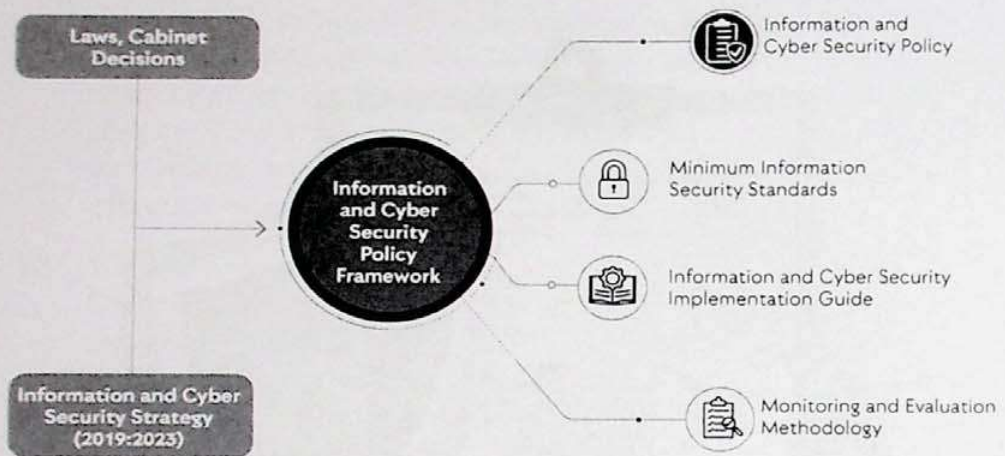


Figure 1: Information and Cyber Security Policy Framework

2.2 The Information and Cyber Security Policy framework includes the following:

- a. The Information and Cyber Security Policy: The main component of the Policy Framework is the Information and Cyber Security Policy. It provides a set of policies that the government organizations shall comply with, outlines the essential controls, and provides direction to government organizations in protecting information and information technology assets from information security events.
- b. Minimum Information Security Standards: This document outlines the minimum acceptable standards of information security controls that shall be adhered to by the government organizations. Minimum Information Security Standards are available for the reference on [www.onlinesafety.lk](http://www.onlinesafety.lk) website of Sri Lanka CERT.
- c. Information and Cyber Security Implementation Guide: This provides a comprehensive set of instructions to staff and stakeholders who require specific details on the implementation of the Policy. This guide includes instructions on the establishment of an information security governance structure, classification of assets, management of risks, protection of assets, methods of disaster recovery and backups,

management of incidents, management of identity and access control and so forth. This document is available for reference on [www.onlinesafety.lk](http://www.onlinesafety.lk) website of Sri Lanka CERT.

- d. **Monitoring and Evaluation Methodology:** This provides assessment criteria for evaluating the readiness of government organizations in adopting the Policy and for evaluating the progress of its implementation. Sri Lanka CERT uses the methodology mentioned in Section 6 of this document to evaluate the maturity of the information and cyber security activities of government organizations within a predefined time frame.

- 2.3 The Information and Cyber Security Policy Framework is governed by the relevant laws and regulations, Information and Cyber Security Strategy of Sri Lanka, policies on e-government and cabinet directives.







### 3. Information and Cyber Security Policy

---

#### 3.1 Objectives

- 3.1.1 Information and cyber security refers to the protection of information assets from unauthorized access, use, modification, and destruction to ensure the confidentiality, integrity and availability of information. It includes the protection of IT assets that contain information assets from malicious actions of individuals with the use of cyber technology or other means, and protection of assets from other natural disasters such as floods and fires.
- 3.1.2 In this context, the main objective of the Information and Cyber Security Policy is to introduce a set of rules and guidelines to be followed by the government organizations to protect information and IT assets from damage caused by malicious activities of individuals and natural disasters.

3.1.3 The other objectives of the Policy are to,

- a. establish a common information and cyber security standard across the public sector,
- b. strengthen government organizations' resilience to information and cyber security events by mandating security standards, rules and processes related to the design, implementation, use and operations of information systems and digital infrastructure,
- c. establish a mechanism to detect information and cyber security incidents in a timely manner, to minimize the impact of such incidents to organizations, and to efficiently restore any capabilities or services that were impaired due to such incidents, and
- d. educate staff on the rules, best practices, standards and processes of information and cyber security, and build the confidence of staff in the security status of the organization.

3.1.4 This Policy is written in simple language. All staff and relevant third-party service providers, regardless of their knowledge of the subject, will be able to understand their responsibilities and accountabilities in relation to the implementation of the Policy.

3.1.5 This document will be updated periodically to provide technical and security guidance for government organizations to support good information security practices.

## **3.2 Scope of the Policy**

3.2.1 This Policy is applicable to any government organization including Ministries, Departments, Public Corporations, Local Government Institutions, and any organization defined as 'Public Authorities' in the Right to Information Act No 12 of 2016. The Policy shall also be applicable to the relevant third-party service providers who manage IT services on behalf of government organizations.

3.2.2 Policies presented here are developed based on two levels. They are, (a) the policies applicable to all government organizations, and (b) the policies applicable to the Critical National Information



Infrastructure providers (CNII). CNII providers are required to comply with all the policies specified in this Policy. Other organizations are required to comply with the policies applicable to all government organizations. It is, however, recommended for other organizations to comply with the policies which are applicable to CNII for better security.

- 3.2.3 CNII providers are defined as the organizations that maintain information and IT assets whose incapacity or destruction would have a debilitating impact on national security, governance, economy, health and social well-being of a nation. A list of CNII providers will be published by the Sri Lanka CERT.
- 3.2.4 This Policy is developed based on the information and cyber security governance principles, and several concurrent and continuous information security functions proposed by the NIST of the United States of America. These functions include (a) identifying information and IT assets of the organization (e.g. data, information, computers and other digital infrastructure), (b) taking necessary actions to protect assets, (c) detecting information and cyber security incidents, (d) responding to incidents, and (e) recovering any service that was disrupted due to an incident. The Policy also includes the information and cyber security governance mechanism for directing and controlling activities related to information and cyber security within the government organization. Figure 2 presents activities that government organizations should follow to protect information and IT assets.



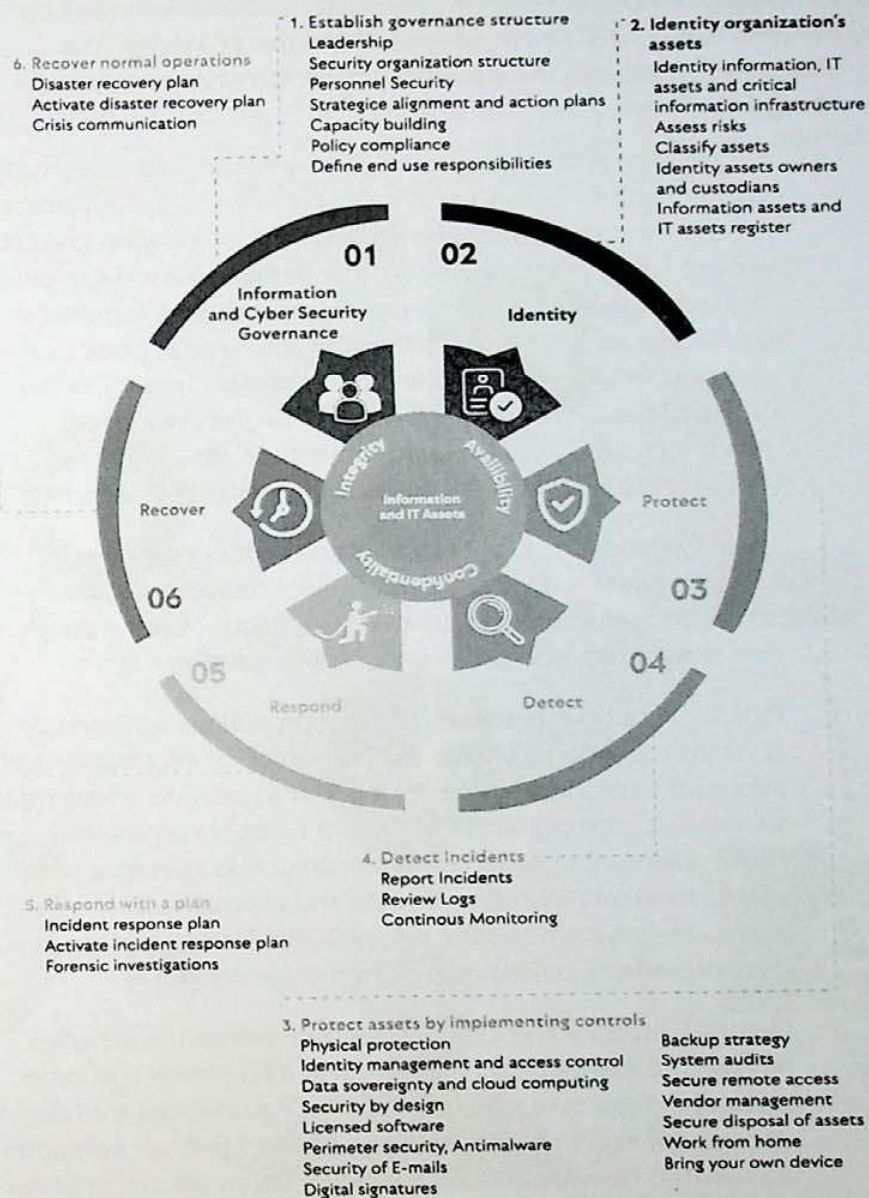


Figure 2: Steps to Information and Cyber Security.

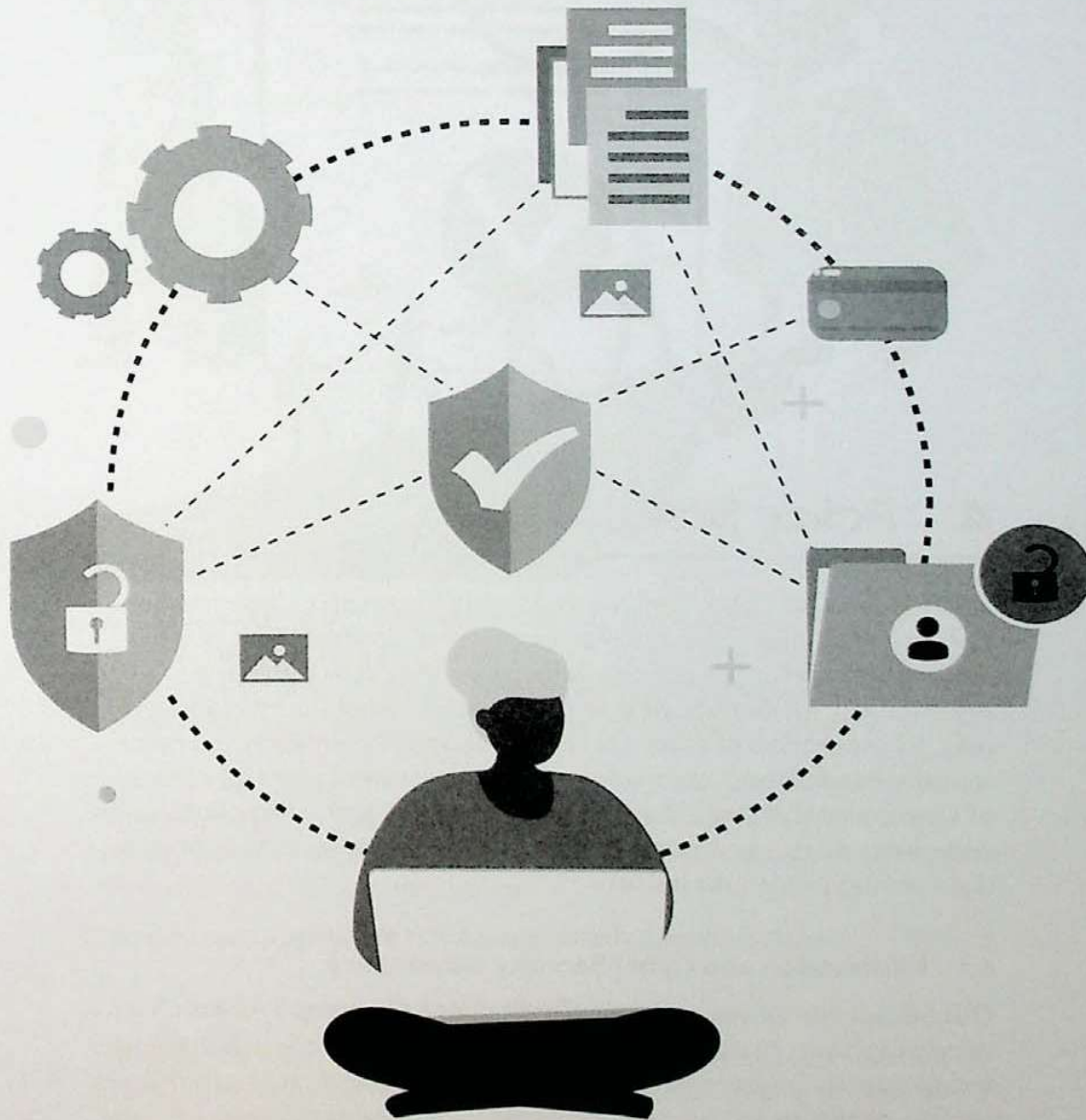




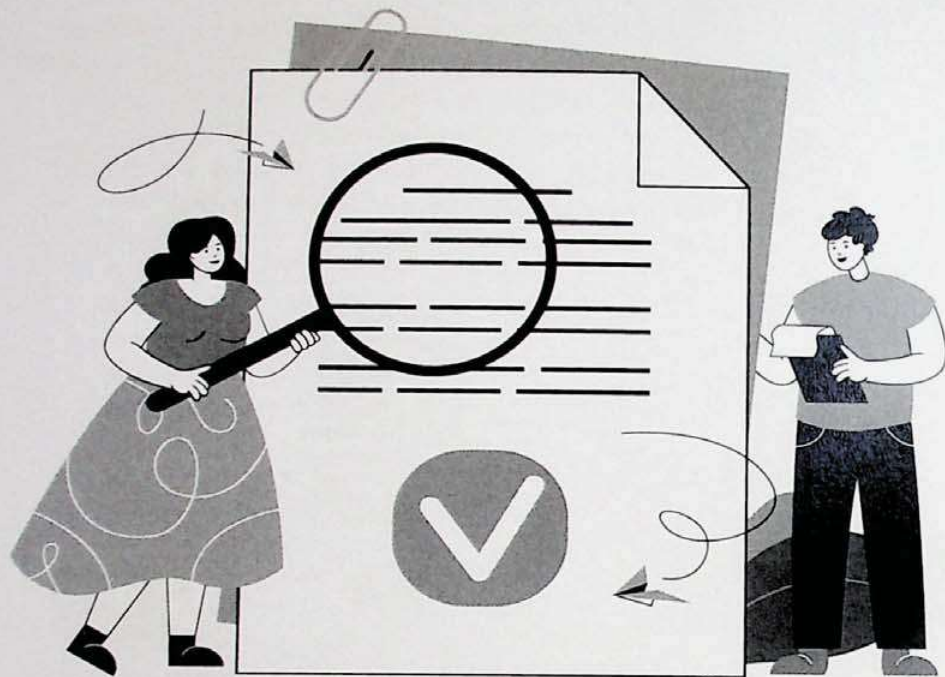
3.2.5 The steps to be taken by an organization to protect assets by implementing this Policy, which is developed based on the information security functions mentioned in 3.2.4, are described below.

- a. Information and Cyber Security Governance: Information and Cyber Security Governance generally refers to the governance mechanism that directs and controls the information and cyber security of an organization. In order to implement the information and cyber security governance, organizations are required to establish a security organizational structure and appoint officers responsible and accountable for information security, undertake capacity building of such officers, define the organizations' information and cyber security objectives, develop action plans, and allocate resources for related activities (Refer Section 4.1).
- b. Identify Function: It facilitates government organizations to identify assets such as data, information, computers, systems, and digital infrastructure and, to identify and effectively manage the risks associated with those assets (Refer Section 4.2).
- c. Protect Function: The Protect Function outlines appropriate controls required to ensure the protection of information and information technology assets in order to provide uninterrupted services. To comply with the Protect function, organizations shall implement appropriate controls such as managing user access to assets, installing firewalls and antimalware software, conducting systems audits, establishing a backup strategy, and shall implement policies mentioned in Section 4.3.
- d. Detect Function: The Detect Function defines the activities required to identify the occurrence of information and cyber security incidents in a timely manner. Organizations shall deploy appropriate tools to analyze logs generated through computers and related devices to detect incidents in an efficient manner (Refer section 4.4).
- e. Respond Function: The Respond Function defines the actions that should be taken in response to a detected incident. To respond to an incident in an efficient and effective manner, organizations shall develop and implement an Incident Response Plan as defined in Section 4.5.

- f. Recover Function: The Recover Function identifies appropriate activities to restore any capabilities or services that were impaired due to an information and cyber security incident. To comply with the Recovery Function, the organization shall develop a Disaster Recovery Plan and activate the Plan to recover normal operations in an event of incident (Refer Section 4.6).







## 4. Policy Statements

Information and Cyber Security Policy for Government Organizations consists of six main policy domains namely, (a) establishment of an information and cyber security governance structure within the organization, (b) identification of assets, asset owners, custodians, and risks, (c) protection of asset, (d) identification of information and cyber security incidents (e) responding to security incidents, and (g) recovery of operations that were disrupted due to an incident. The policies to be complied with by government organizations in relation to the above six domains are presented below.

### 4.1 Information and Cyber Security Governance

This Section proposes a mechanism to direct and control information security in the organization. It specifies the leadership and accountability framework which is necessary to ensure that information security activities are properly managed within the organization. It also

highlights the need of aligning information and cyber security activities to the vision and mission of the organization, the need for capacity building of responsible and accountable officials, effective information and cyber security planning, and the importance of government organizations adopting this Policy.

#### **4.1.1 Policy on Leadership**

The Head of the Organization (HOO) shall provide leadership to information security activities of the organization, and shall bear the ultimate responsibility and accountability for protecting information and assets of the organization.



HOO shall lead the implementation of the Information and Cyber Security Policy, set up information security goals and priorities that support the vision and mission of the organization, and ensure the availability of resources to implement the information security activities.

The HOO shall also provide leadership to create an information security culture within the organization, where users comply with information security policies and guidelines, and work proactively towards protection of information and systems they use.

***Compliance: Applicable to all government organizations***

#### **4.1.2 Policy on Security Organization Structure**

The organization shall establish an information security organizational structure. An effective information security organizational structure



shall include key roles such as (a) Information Security Officer, (b) Chief Innovation Officer, and (c) (Chief) Internal Auditor.

The said structure is essential to execute, direct and manage information security activities of the organization, and to protect the organization against information and cyber security breaches, intrusions and interruptions.

***Compliance: Applicable to all government organizations***

**a) Policy on the Role of Information Security Officer (ISO)**

The organization shall appoint an ISO. The ISO shall be a senior-level executive responsible for establishing the organization's information security objectives in consultation with HOO, managing information security risks, and implementing the Information and Cyber Security Policy to ensure that the organization's information and assets are adequately protected.

The role of the ISO shall be separated from the IT function, and the ISO shall directly report to the HOO with regards to the activities in relation to information security.

***Compliance: Applicable to all CNII providers***

**b) Policy on the Role of Chief Innovation Officer (CIO)**

CIO or the officer in charge of the subject of IT shall be trained and assigned responsibilities to take appropriate steps to protect information and other IT assets, and to ensure the continuity of the business operations of the organization.

Note: In the case of the organization not having a suitable officer to be appointed as the ISO, the CIO or the officer in charge of the subject of information technology shall be empowered to play the role of the ISO.

***Compliance: Applicable to all government organizations***

**c) Policy on the Role of (Chief) Internal Auditor (IA)**

(Chief) Internal Auditor shall be assigned the responsibilities of initiating and overseeing information security audits of the organization, assessing the progress of adopting the Information and Cyber Security Policy, and reporting information security related findings to the Audit and Management Committee (AMC) for further actions.

***Compliance: Applicable to all CNII providers***



#### **4.1.3 Policy on Information Security Committee (ISC)**

The organization shall establish an Information Security Committee to provide strategic directions to activities related to the implementation of the Information and Cyber Security Policy. This Committee shall be responsible for reviewing and approving all information security controls, action plans, assets classification schemes, incident response plans and disaster recovery plans and other activities carried out by the ISO in implementing the Policy. The HOO shall chair the Committee, and the Committee shall consist of the ISO, CIO, (Chief) IA, and Asset Owners. The policy on Asset Owners is presented in Section 4.2.3.

***Compliance: Applicable to all government organizations***

#### **4.1.4 Policy on Risk Management Committee (RMC)**

The organization shall establish a Risk Management Committee. This Committee shall be an independent committee directly reporting to the HOO, and holds the responsibility of overseeing the risk management of the organization with respect to information and IT assets.

The RMC shall identify and evaluate risks in relation to assets, and shall propose appropriate controls to ISC to take necessary actions to mitigate the risks. The Committee shall include Sectional Heads, Asset Owners, and the ISO. The Deputy Head of the organization shall be the chairperson of the Committee.

***Compliance: Applicable to all CNII providers***

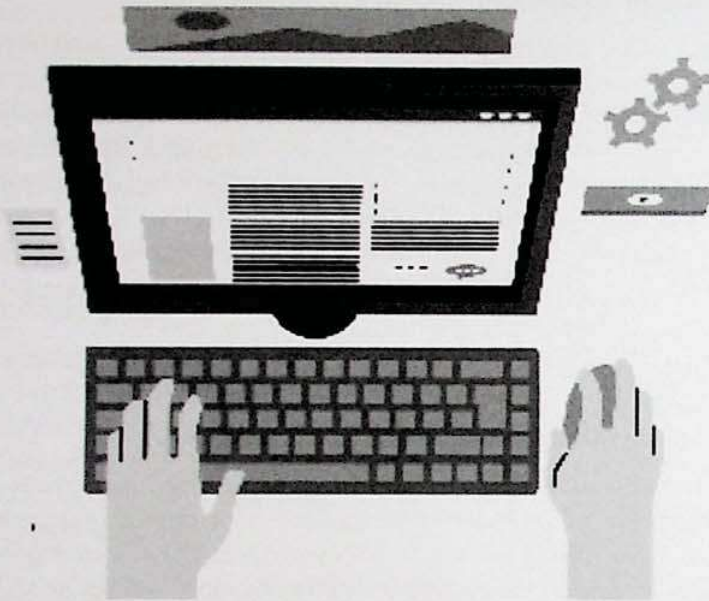
#### **4.1.5 Policy on Responsibilities of End Users**

Information security is everyone's responsibility. All end users are required to behave responsibly and comply with an organizational policy regarding the protection of information and IT assets which they have access to.

End user responsibilities shall include but not be limited to appropriate use of information, computing devices, emails, internet, social media, telephones, and faxes. All users shall understand and adhere to end user responsibilities outlined in the Information and Cyber Security Implementation Guide, and applicable information security practices required by this Policy.

Misappropriate use of such resources would lead to disciplinary actions as stipulated in the Establishment Code and the legal actions under the Computer Crimes Act or any other applicable Acts of Law.

***Compliance: Applicable to all government organizations***



#### **4.1.6 Policy on Capacity Building**

The organization shall build the capacity of the accountable individuals such as ISO, CIO, (Chief) IA, Assets Owners, end users through information and cyber security awareness raising, education and trainings.

Such capacity building activities of the relevant officials should be carried out in a proper manner, and such activities should be included in the Annual Training Plan of the organization.

**Compliance:** *Applicable to all government organizations*

#### **4.1.7 Policy on Security Clearance of Staff**

Anyone who has been assigned or transferred to a position that deals with information classified as "Secret" or "Confidential", or has access to CNII must undergo a security clearance check prior to appointment or transfer to that position.

Background checks and periodic security clearance checks shall be carried out during their service

**Compliance:** *Applicable to all CNII providers*





**Compliance:** Applicable to all government organizations

The organization shall develop and implement information security action plans (long, medium, and short term plans) which define the way in which security is to be guaranteed in realizing the vision, mission, and objectives of the organization. Those plans should be based on information security priorities determined by a risk assessment, and budgets should be allocated to implement plans.

#### 4.1.10 Policy on Compliance

Sri Lanka CERT shall conduct annual information and cyber security readiness assessments to determine the level of compliance, and the organization shall facilitate Sri Lanka CERT to conduct such assessments.

**Compliance:** *Applicable to all government organizations*

#### 4.2 Identify Assets, Owners, Users and Risks

The organization shall develop an understanding of their operating environment to manage the information security risks to organizational assets. The organization shall identify information, systems, and IT devices (assets) that are of value to the organization, owners and the users of the assets, their roles and responsibilities in protecting those assets, and current risks associated with assets. The following are the policies that the organization should adopt in this regard.



##### 4.2.1 Policy on Identification of Information and Information Technology Assets

The organization shall identify all of its important information assets. An information asset is any information that is of value to the organization in performing its organizational functions. Examples of information assets include trade secrets, tender documents, budget sheets, employees' personal records, data gathered by application software related to services offered by the organization, etc. Information assets may come



in many different forms such as paper documents, digital documents, databases, passwords or encryption keys or any other digital files.

The organization shall also identify IT assets. An IT asset is a software (e.g. operating systems, payroll systems, other software), hardware (e.g. computers, hard disks, servers, routers, firewalls), networks or other digital infrastructure facilities within an information technology environment.

The identification of assets (information and IT assets) shall be performed with the intention of protecting assets from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure integrity, confidentiality, and availability of assets.

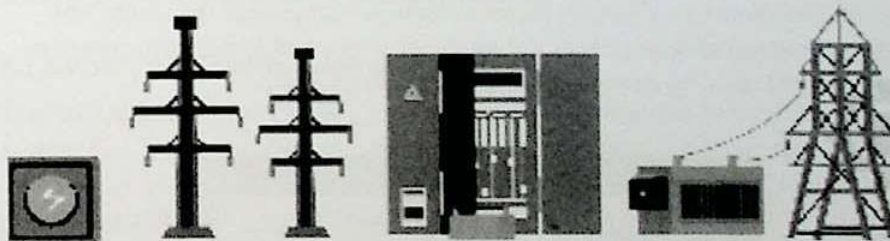
**Compliance:** *Applicable to all government organizations*

#### **4.2.2 Policy on Identification of Critical National Information Infrastructure (CNII)**

Critical National Information infrastructures are the systems or facilities, the failure or destruction of which would have a devastating impact on national security, governance, economy, health and social well-being of a nation.

Organizations which maintain CNII shall take appropriate measures to protect such infrastructure as specified in this Policy. Identification of CNII shall be carried out by Sri Lanka CERT.

**Compliance:** *Applicable to all CNII providers*



#### **4.2.3 Policy on Responsibilities of Asset Owners, Custodians and Users**

The organization shall identify Asset Owners and Custodians. The Asset Owner is a senior executive level officer or an entity who has the approved management responsibility of controlling the lifecycle of an asset. Asset Owner shall understand the risks to assets and shall propose appropriate controls to protect such assets. It is necessary to formally

assign ownership of the asset when it is created, or when assets are transferred to the organization or are acquired by the organization.

The Custodian is an officer or an entity who is responsible for the protection of the asset and for implementing the controls (as identified and approved by the owner of the information asset) related to the protection of the asset.

The Asset Owner and Custodian are also responsible for developing a Register of assets, classifying assets and protecting assets, defining and reviewing access restrictions to assets, ensuring appropriate handling when an asset is deleted or destroyed (adopted from ISO 27002).

The organization should also identify the users who use its assets. Users are the staff who use the assets for official purposes. Asset Owners must accurately identify the users who are required to use the assets for official purposes, and control access to those assets as specified in Section 4.3.4 and 4.3.5.

***Compliance: Applicable to all government organizations***

#### **4.2.4 Policy on Maintaining Information and IT Assets**

The organization shall record information assets in the Information Assets Register. An Information Assets Register is a formal inventory of the information assets that an organization holds and possesses. At a minimum, an organization shall record, the name of information asset, owner and custodian of the asset, level of classification, reason for the classification, date of classification, the computer system which processes assets, the storage location of asset, disposal method, impact of loss (compromise or disclose) and date to review the classification of asset.





The organization shall also record details of IT assets in the IT Assets Register. The IT Asset Register shall contain at a minimum, the type of the assets (e.g. hardware, software, server), location of the asset, operating system, license details, users, risk, classification level, estimated value and so forth. Assets Registries shall be accurate, up to date, and consistent with other inventories.

***Compliance: Applicable to all government organizations***

#### **4.2.5 Policy on Assessments Risk**

The organization shall conduct a formal risk assessment to determine the risks to the assets and their impact to the organization. The purpose of a risk assessment is to identify the risks to the assets and determine what security measures should be taken to minimize those risks. Risk ratings should be developed based on the impact, and risks should be recorded in the Risk Register.

The organization shall take appropriate safety precautions for the risks recorded in the Risk Register by taking into account the policy considerations specified in Section 4.3.

The risk assessment shall be carried out by the RMC of the organization. In the event, where the organization does not possess appropriate skills for carrying out a risk assessment, a qualified and experienced firm shall be hired for this purpose. Sri Lanka CERT shall assist CNILs to conduct Risk assessments.

***Compliance: Applicable to CNIL providers***

#### **4.2.6 Policy on Classification of Assets**

The organization shall classify assets and determine the sensitivity of assets. The objective of the classification is to ensure that an asset receives an appropriate level of protection in accordance with its value to the organization and its sensitivity.

Classification of information assets shall be performed based on accepted guidelines. The classification levels for information assets shall be "Secret", "Confidential", "Limited Sharing", "Public" and "Unclassified".

IT assets shall be classified into four levels namely, "Very Critical IT assets", "Critical IT assets", "Non-Critical IT assets", and "Unclassified IT assets".

A description of the process of assets classification is available in the Information and Cyber Security Implementation Guide (Refer Section 2.2. c).

**Compliance:** *Applicable to all government organizations*

### 4.3 Protect Assets



Upon identification of the assets, the organization shall implement appropriate controls to prevent, limit or contain the impact of a potential information security incident. Controls applied shall be based on the classification of each asset. To comply with the Policy, the organization shall control access to assets, enforce processes in place to secure data, define security controls for data- in- transit and data-at-rest, use licensed software, and deploy protective technology to ensure cyber resilience. The policies which the organization shall comply with are presented below.

#### 4.3.1 Policy on Protection of Data-at-Rest

The organization shall protect data-at-rest. Data at rest is the data that is not actively moving from device to device or network to network (e.g. data stored on a server, cloud, hard drive, laptop, flash drive, or data archived or stored).



It is essential to encrypt any data (information assets) which are classified as "Secret" or "Confidential" prior to storing. Other means of protecting data at rest include, controlling user access through Identity Management and Access Control mechanism, and providing physical protection to assets.

***Compliance: Applicable to all government organizations***

#### **4.3.2 Policy on Protection of Data-in-Transit**

The organization shall protect data-in-transit. Data in transit is the data that is actively moving from one location to another such as across the Internet or through a private network (e.g. data being transferred from site A to B through an organization owned private network, including Wi-Fi).

In order to protect data in transit, the organization shall encrypt sensitive information (information classified as "Secret" or "Confidential") prior to moving and, use secure connections (HTTPS, TLS, SFTP, etc.) for data transfer.

Further, the organization shall ensure that security parameters on Wi-Fi settings have been enabled.

***Compliance: Applicable to all government organizations***

#### **4.3.3 Policy on Physical Protection**

The organization shall provide physical protection to assets to prevent physical intrusion and unauthorized access.

Based on the protection requirements of assets, each organization shall define secure areas to store or process assets which are important to the organization. Information assets classified as "Secret" and "Confidential" are to be stored and processed in the stated secure areas.

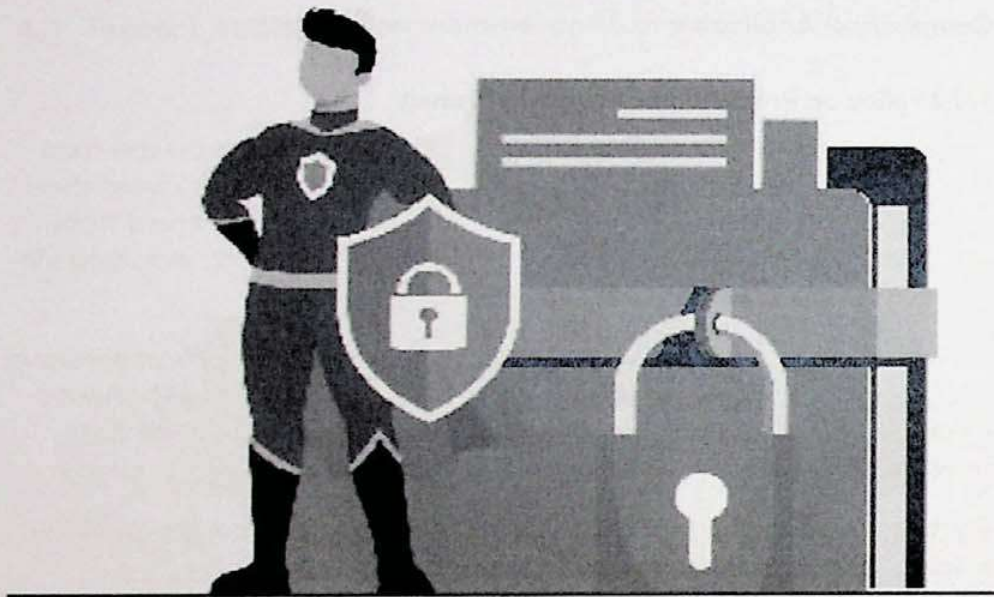
Further, IT assets which are classified as "(very) Critical" shall be stored and operated in secure areas.

Secure areas shall be protected by physical walls and lockable doors, and multi-factor entry systems, and shall be monitored through CCTV continuously to prevent physical intrusions and unauthorized access.

Secure areas shall be protected to prevent threats from fire, flood, humidity, electromagnetic fields and temperature.



Furthermore, the organization shall use various technologies to control user access to information and IT assets. Such technologies include but are not limited to user identity and passwords, access cards, PINs and biometrics.



Moreover, access to the computers, systems or any devices shall be controlled through implementing an Identity Management and Access Control process (Refer Section 4.3.4).

***Compliance: Applicable for all government organizations***

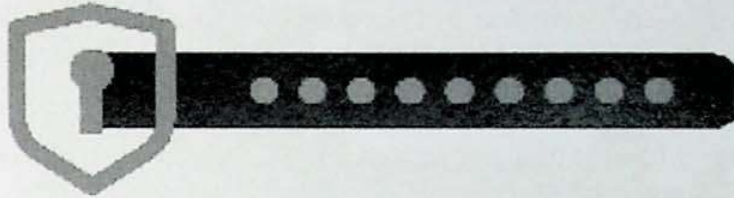
#### **4.3.4 Policy on Identity Management and Access Control**

The organization shall control user access to both Information and IT assets. Identity management and access control is an approach to managing access to information and IT assets to keep them secure.

Identity management and access control is focused on verifying a user's identity and their level of access before granting them access to systems and information. Users shall only be granted access to the assets which they need to perform their tasks (need-to-know), and assets they need to use to perform tasks (need-to-use). The users shall always be given minimum access to systems and information necessary for their role only.

Based on the given principles, the organization shall develop an Identity Management and Access Control Process for its usage. Sri Lanka CERT

has drafted an Identity Management and Access Control Process for government organizations which can be customized and adopted by the organization.



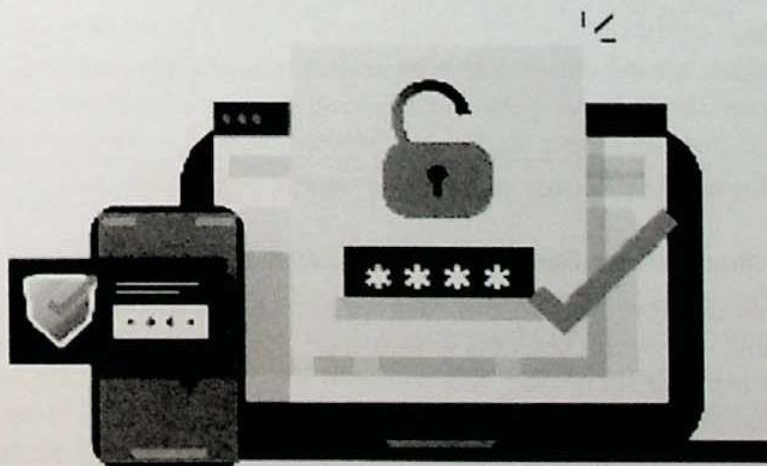
The organization shall ensure that the Identity Management and Access Control Process implemented by the organization is adequate and up-to-date. Further, all employees and all third-party service providers should adhere to the Identity Management and Access control process implemented by the government organization.

Any violations of the Identity Management and Access Control Process shall be reported to the ISC for necessary action. In a situation where an ISC is not established, such violations should be reported to HOO through ISO.

***Compliance: Applicable to all government organizations***

#### **4.3.5 Policy on Strong Authentication**

Authentication is the process of identifying a user. The authentication process provides access to the organization's assets through user identification (identification) and user verification (verification of identity) by evidence.





In accordance with the Organization's Identity Management and Access Control Process as presented in Policy 4.3.4, the organization must use strong authentication to verify a user's identity.

A combination of username and password, and the use of multifactor authentication (MFA) are recommended to authenticate user identity.

To ensure a strong authentication process, the organization shall address the following factors (but not limited to) in developing the organization's Identity Management and Access Control Process.

a) Strong Password:

- Passwords must be at least 8 characters long and must consist of both upper and lower case characters (e.g. a-Z), digits (0-9), and special characters (!@\$/).
- All passwords must be changed after predetermined intervals which is 90 days for regular access. Privilege access should only be granted on a need basis.

b) MFA:

- The organization shall implement MFA access for securing user accounts which have access to "Secret" and "Confidential" information.
- In designing MFA, organization shall take into account at least combination of user's knowledge (what you know, e.g. password), possession (what you have, e.g. token, access card), or inheritance (what you are, e.g. biometric-finger print).

Passwords and any other authentication credentials provided to an employee who is leaving the organization shall be withdrawn and removed from all assets to prevent further access by the employee.

**Compliance: Applicable to all government organizations**

#### **4.3.6 Policy on Data Sovereignty and Cloud Computing**

Data sovereignty refers to the data subject to the laws and governance structures within the country where such data is collected, processed and stored. In this context, the government organization shall pay a high level of attention to data sovereignty particularly when cloud services are obtained from other countries to store and process the collected data.



Cloud computing generally refers to the ICT resources (e.g. such as storage, processing, application development platforms) available for users on-demand without direct management by the user. Many organizations nowadays are moving to cloud services due to cost savings, scalability and increased performance.

The organization, however, must be cautious about the risk of using cloud services, particularly, when using public clouds (public cloud is a cloud service available to anyone who wants to purchase them). Limited control over the cloud as they are operated in different jurisdictions, limited visibility of architectures and limited transparency of operations, possible significant mismatches in service-level agreements (SLAs) are common cloud risks.

In fulfilling their cloud service needs, organizations shall give priority to obtaining services through the Lanka Government Cloud (LGC).

LGC is a government-owned private cloud service operated by the Information and Communication Technology Agency (ICTA), which was designed to fulfill the cloud service requirements of the government. It is, however, strictly recommended to the organizations to perform a proper risk assessment prior to obtaining services from any cloud service provider.

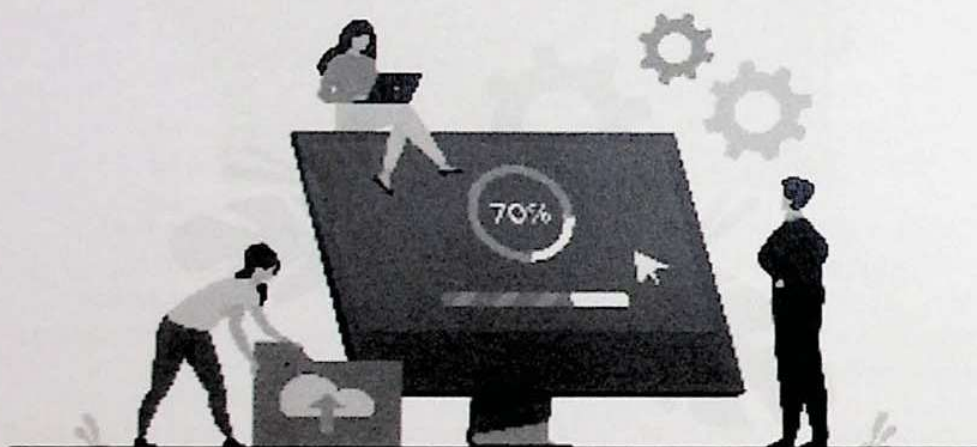


Furthermore, all activities of the organization in relation to collecting, storing and processing data or hosting software applications in other jurisdictions shall be performed in accordance with the relevant laws and regulations in Sri Lanka in relation to data protection.

**Compliance:** *Applicable to all government organizations*

#### **4.3.7 Policy on Licensed Software and Patch Updates**

The organization shall use licensed software with valid updates. This includes but is not limited to system software, utility programs, and application software (e.g. word processing packages, databases, browsers, antimalware, etc.).



Organization shall update operating systems and other relevant software with vendor supplied latest patches and fixes. Furthermore, organizations should enable automatic updates.

Further, prior to the installation of critical patches provided by the supplier, a proper assessment of the potential impact of their installation should be made (especially for IT assets classified as very critical and critical).

**Compliance:** *Applicable to all government organizations*

#### **4.3.8 Policy on Antimalware**

The organization shall install Antimalware software with a valid license. Antimalware tools shall remain active at any potential entry point, and malware signatures shall be up-to-date and automatic updates shall be enabled.

Malware detection must be configured for on-access scanning, including downloading or opening of files, folders on removable or remote storage, and web page scanning.

Users must be prohibited from changing the configuration of, uninstalling, deactivating or otherwise tampering with antimalware.

When a government organization communicates information to another organization or to the public, through electronic format sender shall ensure that the information is free of malware.

***Compliance: Applicable to all government organizations***

#### **4.3.9 Policy on using Official Emails**

The organization shall use official emails for official communications. Employees must not use official emails for personal communications.

Official emails are the email provided by the government with the domain name of "gov.lk". Official email accounts are official assets and the organization has the right to access the account, read emails or delete the account.

All email attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any government organization's computer system.

Organizations are also required to comply with the regulations and guidelines issued by the government from time to time regarding official emails.

***Compliance: Applicable to all government organizations***

#### **4.3.10 Policy on Security of Emails**

The organization shall configure their email accounts with all applicable security features. To ensure the security of information, the email server shall be hosted in line with the relevant laws in relation to data protection.

The organization shall set up email filters to remove emails known to have malware attached and prevent the inbox from being cluttered by unsolicited and undesired (i.e. "spam") email. Moreover, when sending sensitive information via emails, it must be encrypted.



In the case of email accounts provided by the Lanka Government Network (LGN), ICTA is required to ensure that the email service is securely configured, and security audit reports shall be obtained from Sri Lanka CERT on a periodic basis for supervisory or regulatory requirements.

***Compliance: Applicable to all government organizations***

#### **4.3.11 Policy on Digital Signatures**

Where appropriate, the organization shall implement digital signatures. Digital signatures should be used for emails to ensure authenticity, integrity and nonrepudiation.

***Compliance: Applicable to all government organizations***

#### **4.3.12 Policy on Perimeter Security Controls**

The organization shall install perimeter security controls such as Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), etc., to provide protection to assets (information, computers, networks and systems assets) against cyberattacks and prevent malicious software from accessing assets via the Internet.

The organization shall regularly update perimeter security threat databases, install antimalware with automatic updates enabled, update default settings with appropriate configurations, and disable default vendor supplied user accounts for such devices and systems.

An overview of the appropriate security configurations for perimeter security controlling devices is provided in the Information and Cyber Security Implementation Guide.

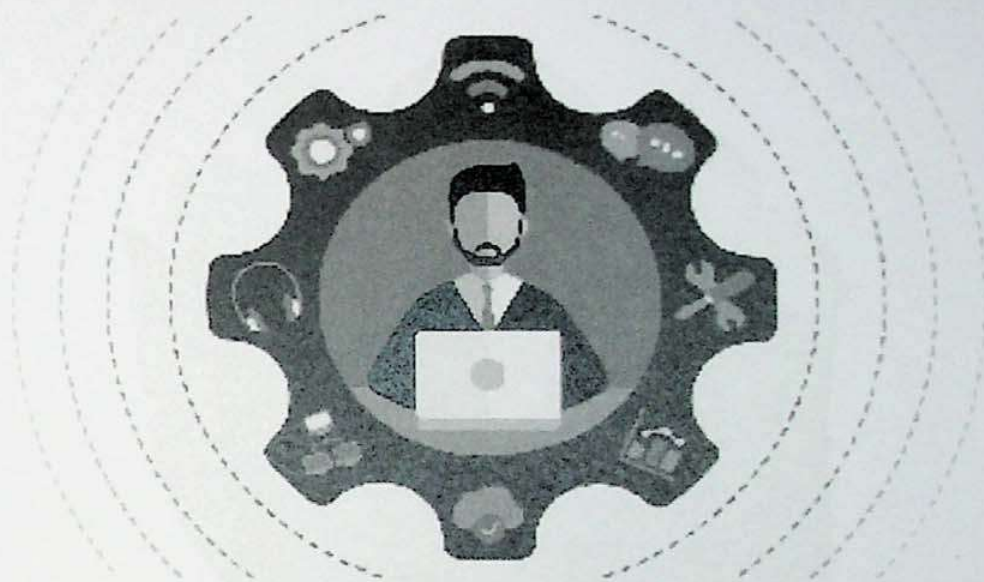
***Compliance: Applicable to all government organizations***

#### **4.3.13 Policy on Secure Remote Access**

The organization shall secure remote access to internal networks to prevent unauthorized access to assets through geographically distant locations.

Remote access brings many information security threats to the organization. Risk of eavesdropping as information travels over the public internet, unauthorized access to systems or data, monitoring and

manipulation of data and malware infections are common security risks associated with remote access.



To mitigate the risk of remote access, the organization shall use secure Virtual Private Networks (VPNs), allow only authorized users to access systems based on the identity management and access control policy of the organization, implement multi-factor authentication, secure remote access from client devices, and use trusted networks.

***Compliance: Applicable to all government organizations***

#### **4.3.14 Policy on Backup Strategy**

The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

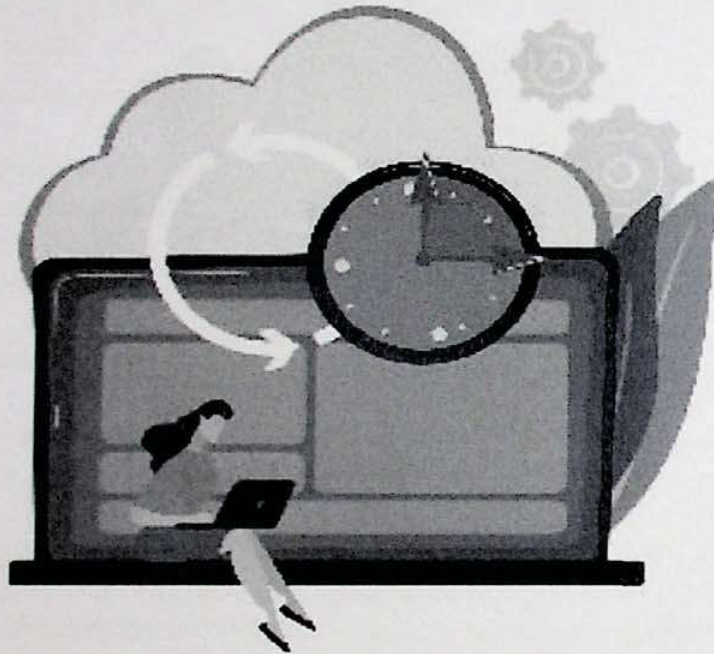
The organization must ensure that the backups can be used to fully restore or recover any disrupted services.

Data written onto backup media shall be preserved as per the regulatory requirements of the government.

The organization shall also define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to determine the frequency of backups.



It is recommended to have an air gap between the live data and backup data for protecting live data from any malicious attacks including ransomware.



It is further recommended that backups be stored at a secure location which is physically distant from the data processing site. There should also be a mechanism implemented to detect any changes made to the backups.

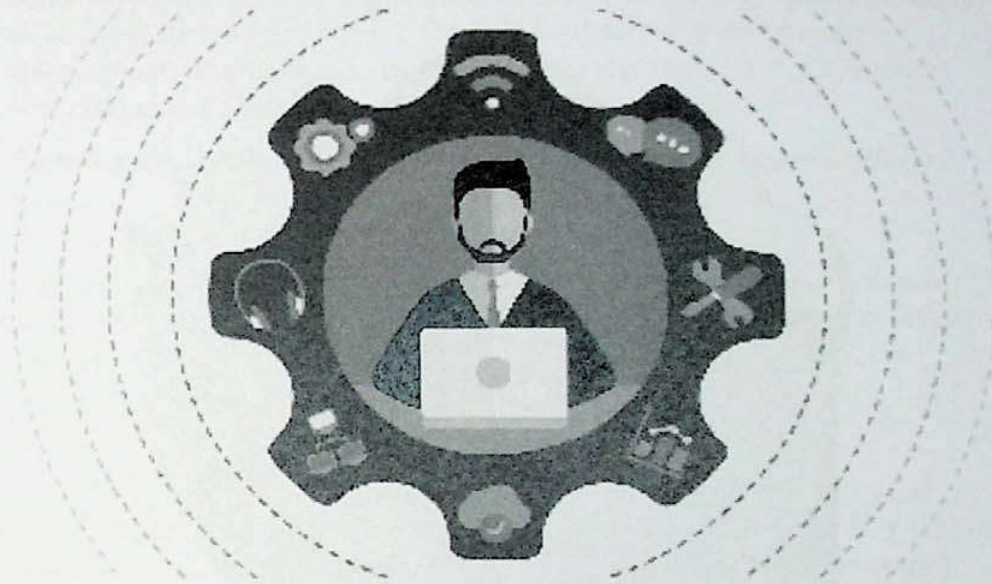
Backups containing information assets labeled as "Secret" and "Confidential" shall be stored as per the security requirements specified in the Assets Register.

***Compliance: Applicable to all government organizations***

#### **4.3.15 Policy on the Security of Assets Supplied by Government Organizations**

Today many government and non-government organizations operate on the information and IT assets provided by the government. In this context, ICTA or other government organizations must ensure the security, reliability, integrity, and accuracy of the information and IT assets developed by them. For example, the security of Lanka Government

manipulation of data and malware infections are common security risks associated with remote access.



To mitigate the risk of remote access, the organization shall use secure Virtual Private Networks (VPNs), allow only authorized users to access systems based on the identity management and access control policy of the organization, implement multi-factor authentication, secure remote access from client devices, and use trusted networks.

***Compliance: Applicable to all government organizations***

#### **4.3.14 Policy on Backup Strategy**

The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

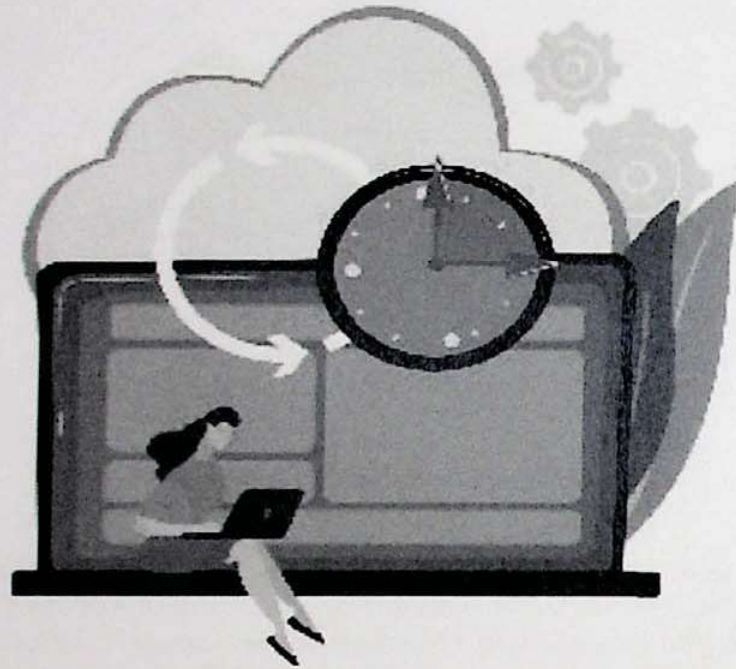
The organization must ensure that the backups can be used to fully restore or recover any disrupted services.

Data written onto backup media shall be preserved as per the regulatory requirements of the government.

The organization shall also define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to determine the frequency of backups.



It is recommended to have an air gap between the live data and backup data for protecting live data from any malicious attacks including ransomware.



It is further recommended that backups be stored at a secure location which is physically distant from the data processing site. There should also be a mechanism implemented to detect any changes made to the backups.

Backups containing information assets labeled as "Secret" and "Confidential" shall be stored as per the security requirements specified in the Assets Register.

***Compliance: Applicable to all government organizations***

#### **4.3.15 Policy on the Security of Assets Supplied by Government Organizations**

Today many government and non-government organizations operate on the information and IT assets provided by the government. In this context, ICTA or other government organizations must ensure the security, reliability, integrity, and accuracy of the information and IT assets developed by them. For example, the security of Lanka Government

Network, Lanka Government Cloud, Email Service, Lanka Government Payment System, SMS Service, Document Management System or other services should be guaranteed by the relevant organization that developed such infrastructure. The required security certificates for these infrastructures should be obtained by the relevant organizations from Sri Lanka CERT or from any other qualified institution.

***Compliance: Applicable to ICTA and all government organizations***

#### **4.3.16 Policy on Security-by-Design**

The organization shall follow a security-by-design approach in software acquisitions and in-house software development. The security-by-design approach extends the traditional software development approach by adding security considerations to each stage of the software development lifecycle.

In developing software (or acquiring software), the organization must consider security planning and conducting risk assessments at the project planning stage, defining security requirements in bidding documents, reviewing the security architecture in the design stage, reviewing code at the development stage for identifying security-related weaknesses (flaws), and performing vulnerability assessments in the implementation stage to identify security weaknesses in the systems. Finally, at the system decommissioning stage, the systems shall be securely disposed to ensure that its data and other information assets cannot be accessed and recovered by unauthorized individuals.

Further, in developing websites and web applications, government organization shall adhere to the "Website Security Guidelines", "Web Application Security Guidelines" and "Technical Guidelines for Web Application and Website Security" issued by Sri Lanka CERT. These guidelines can be downloaded from <https://www.onlinesafety.lk> website.

***Compliance: Applicable to all government organizations***

#### **4.3.17 Policy on Secure Disposal of Assets**

Assets shall be disposed securely using a formal procedure when no longer required.

It is required that the organization's storage media, which includes but is not limited to optical media (CDs or DVDs), magnetic media (tapes or diskettes), disk drives (external, portable, or removed from information



systems), flash memory storage devices (SSDs or USB flash drives) and documents (paper documents, paper output, or photographic media) are disposed securely.



If the media contains information that is no longer required, the information shall be deleted in an unrecoverable manner to prevent the retrieval of the original information. Low level sector-based formatting is a possible method of removing information assets contained in media. Shredding or punching are possible ways of permanently destroying media that contain information assets.

If the assets in the storage media are classified as "Secret" or "Confidential" the safest method of disposal is physical destruction of the media, after obtaining proper approval for the disposal action from ISC.

***Compliance: Applicable to all government organizations***

#### **4.3.18 Policy on Internal Information and Cyber Security Audit Process**

The organization shall have a formal internal information security audit program in place to conduct routine audits that includes but is not limited to IT security control audits, application security control reviews, network architecture reviews, IT process audits, security compliance reviews, internal and external vulnerability assessments, penetration testing, and web application penetration testing.

Assessments shall be performed periodically (at least annually), after an incident has occurred, after a change is introduced (to application or hosting environment), after changes to standard/guidelines, after spread of virus or malware, or as determined by the ISC.

The (Chief) IA of the organization shall coordinate the audit, and the Chief IA of each Ministry shall coordinate information security audits of the organizations under its purview.

A formal process to oversee the implementation of recommendations made in audit reports is to be established by the organization. The (Chief) IA of the organization shall take the leadership and bear the responsibility for this process.

Audits shall be performed by a party qualified to carry out such audits or the organization shall obtain the services of Sri Lanka CERT.

If the audits are to be carried out by a third party, it is essential that a Non-Disclosure Agreement (NDA) is to be signed to ensure the confidentiality of the organization's assets.

***Compliance: Applicable to all government organizations***

#### **4.3.19 Policy on Audits Prior to Deployment**

On par with the internal information security audit program, the organization shall perform vulnerability assessments and penetration tests prior to the deployment of any website, web application or system on the live environment.

The organization needs to obtain the services of Sri Lanka CERT to conduct these assessments or shall obtain the services of a qualified third-party organization in consultation with Sri Lanka CERT.

***Compliance: Applicable to all government organizations***

#### **4.3.20 Policy on Systems Hardening**

The organization shall harden IT assets (operating systems, servers, networks and network devices, databases, and virtual private networks) to reduce their surface of vulnerability by eliminating potential attack vectors and condensing the system's attack surface. Guidelines on systems hardening are presented in the Information and Cyber Security Implementation Guide.





Hardening systems shall only be carried out with the support of experienced and skilled personnel.

**Compliance:** *Applicable to all government organizations*

#### **4.3.21 Policy on Work from Home**

With the transition to working from home (or work from distant locations), there is an increase in information security threats. Therefore, employees shall adhere to "Information Security Guidelines for Working from Home" issued by Sri Lanka CERT which outline a set of security best practices when working remotely.

Further, officers responsible for IT activities shall adhere to the "Guidelines to Improve Cyber Security to Enable Work from Home: Minimal Guidelines for IT Administrators" issued by Sri Lanka CERT to ensure secure access to organization's IT assets when working remotely is permitted. These guidelines are issued in compliance with the work-from-home guidelines issued by the government. The guidelines are available for reference on [www.onlinesafety.lk](http://www.onlinesafety.lk) website of Sri Lanka CERT.

**Compliance:** *Applicable to all government organizations*

#### 4.3.22 Policy on Using Personal Devices for Official Work

The organization shall not allow employees to use their personal laptops, smartphones and tabs to carry out official duties. However, under specific circumstances determined by the ISC, the organization may allow selected employees to use their personal devices to perform official duties, under the supervision of the ISO. In such circumstances, it is imperative to appropriately register such devices with the organization and ensure that those devices comply with this Policy. However, Employees' personal devices shall not be used to process or store information classified as "Secret" and "Confidential" under any circumstance.



When employees' personal devices are used to perform official duties, the organization shall ensure that user accounts are set up to have limited privileges, accounts are protected with strong passwords and multifactor authentication, antimalware software is installed and automatic updates are enabled, operating systems, utility software and other application software that is used have valid licenses with necessary patch updates.

Further, the organization reserves the right to review or retain personal and organizational information on such devices, or to release the information to government agencies or third parties during an investigation or legal requirement. Security of the personal device shall be the responsibility of the owner of the device. The organization shall not be liable for any loss or damage to the device including loss of personal data due to the use of the device.

**Compliance: Applicable to all government organizations**



#### **4.3.23 Policy on Using Non-Secure Networks**

The staff of the organization shall avoid the use of non-secure networks, such as untrusted Wi-Fi networks (e.g. available in hotels, restaurants, bus stops), and the use of publicly shared personal computers, kiosks and other related devices to access official email and other official software solutions.

***Compliance: Applicable to all government organizations***

#### **4.3.24 Policy on Management of Suppliers**

The organization shall ensure appropriate measures are taken when external parties (providers of hardware, software, networks, hosting, and managed services etc.) are involved in developing and managing the information and IT assets.

In carrying out vendor management, the organization has to take into consideration the following as a minimum: (a) identifying the responsibilities and obligations of the contracted party including but not limited to backup, storage, recovery and contingency arrangements, security configurations, access to Information and IT Assets, etc., (b) adherence to established information security practices of the organization as defined by the government, (c) right to audit the contracted party processes and controls related to the agreement, and (d) monitoring and reporting on non-adherence to contractual terms and conditions. The responsibility for managing relationships with contracted parties shall be assigned to Asset Owners, designated officers or entities, as decided by the HOO.

***Compliance: Applicable to all government organizations***

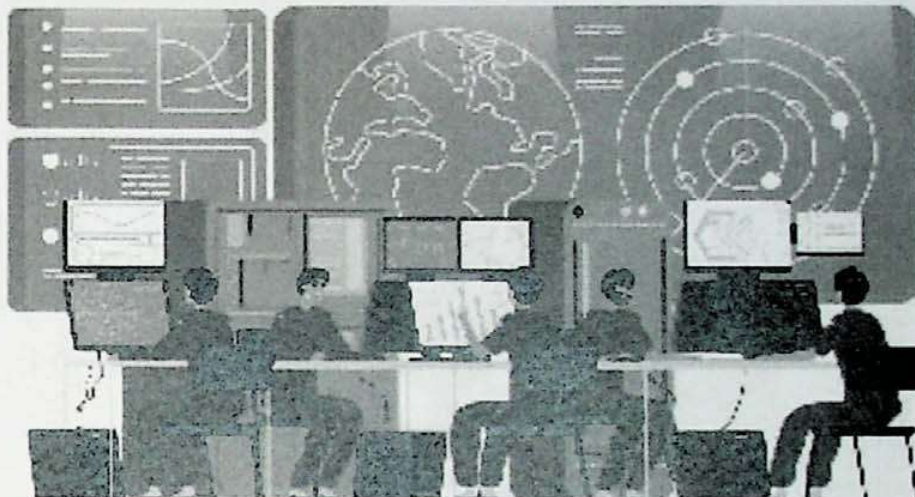
#### **4.3.25 Policy on Change Management**

The organization shall control all changes. Unmanaged changes pose risks to information and IT assets and have the potential to cause operational disruptions. For example, uncontrolled installations (or uninstallations), insertions, deletions, and modifications to systems may impact confidentiality, integrity and availability attributes of data or even result in vulnerabilities to systems that may lead to compromise of the system.

Further, personnel involved in changes may also pose threats to the confidentiality of operational information. ISC, therefore, shall implement a formal change management process to mitigate the overall security risk for the system.

***Compliance: Applicable to all government organizations***

## 4.4 Detect Incidents



The organization shall implement appropriate measures to identify information and cyber security incidents in a timely manner. The organization shall instruct staff to report any cyber security incidents, vulnerabilities or policy violations to relevant officials. Further, the organization shall deploy mechanisms for analyzing logs to identify incidents and adopt continuous monitoring solutions that detect anomalous activities and other threats to operational continuity.

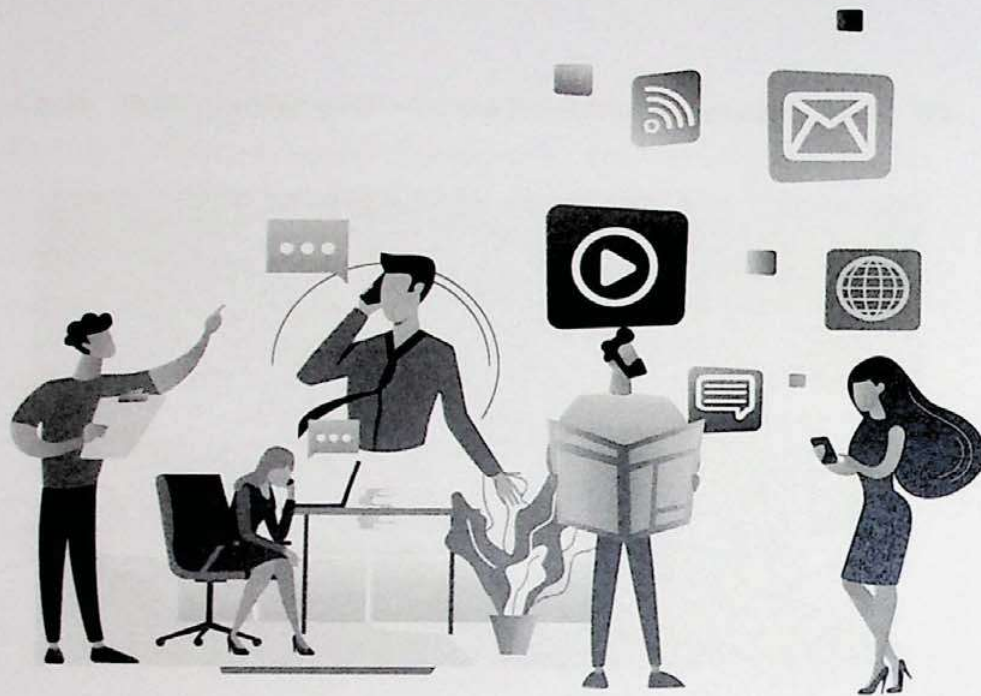
Policies which the organization shall comply with regards to detecting information and cyber security incidents are presented below.

### 4.4.1 Policy on Reporting Incidents

Staff shall be clearly advised to immediately report any suspicious activity or any security violation to the ISO. Security violations shall include but are not limited to unauthorized access to a network, telecommunication or computer system, the apparent presence of a virus on computers, the apparent presence of any asset prohibited by organizations, apparent tampering with any file by unauthorized user, and violations of these guidelines or security policy by another user or contractor.

Users shall also be instructed to report any vulnerabilities existing on IT assets.





The organization shall provide adequate awareness and trainings to staff on detection of incidents, reporting information security events detected, and preserving evidence.

**Compliance: Applicable to all government organizations**

#### **4.4.2 Policy on Reviewing Logs**

The organization shall maintain and review Logs (access logs, error logs, server logs, audit logs, firewall logs and antimalware logs) generated by systems and associated components to detect incidents.

The organization shall regularly review logs to detect malicious attacks on systems, and to determine the causes of errors or security breaches.

Logs shall be protected against tampering and unauthorized access. In the case of logs containing sensitive and personally identifiable information, appropriate privacy protection measures shall be taken prior to storing and analysis. Logs shall be retained for a period of 12 months or as determined by ISC.

**Compliance: Applicable to all government organizations**

#### **4.4.3 Policy on Continuous Monitoring of Incidents**

The organization shall monitor networks or systems for detecting malicious activities, and counter such activities through implementing Intrusion Detection Systems and Intrusion Prevention System (IPS/IDS). The organization can also use Security Information and Event Management (SIEM) systems for security monitoring, and advanced threat and incident detections.

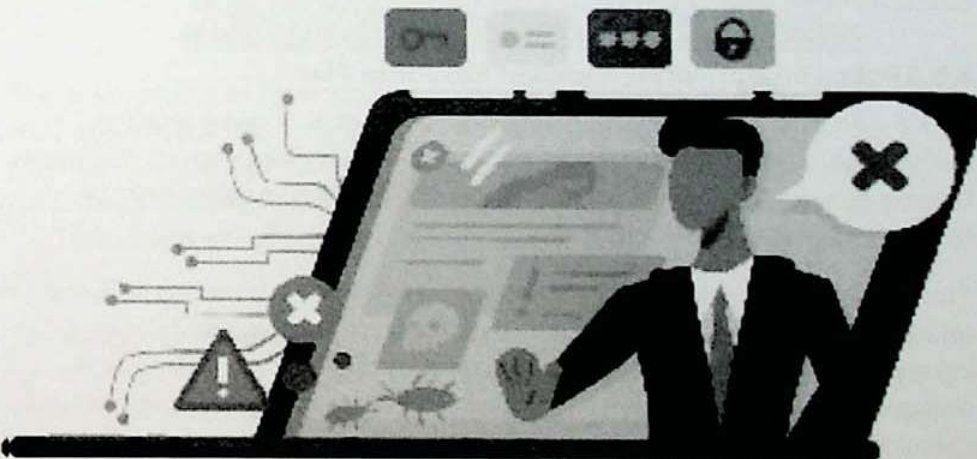
*Compliance: Applicable to all CNII providers*

#### **4.4.4 Policy on Reporting Incidents to Sri Lanka CERT**

As determined by the ISC, the organization is advised to report critical information security incidents to Sri Lanka CERT immediately for technical advice and handling.

*Compliance: Applicable to all government organizations*

### **4.5 Respond to Incidents**



In order to effectively respond to information and cyber security incidents, the organization shall develop an incident response plan, and activate the plan in the event of an incident. Policies that the organization shall comply in responding to information and cyber security incidents are presented below.



#### **4.5.1 Policy on Incident Response Plan**

The organization shall develop an Incident Response Plan which consists of a set of predetermined instructions and procedures to detect, respond, and limit the negative consequences of an information and cyber security incident against an organization's assets. This shall also include a clear set of instructions and procedures to effectively recover from the incident.

The Incident Response Plan shall contain, at a minimum, incident reporting procedures, strategies for detection, analysis and, containment of incidents (eradication or recovery), allocation of information security responsibilities to designated staff, and procedures related to post-incidents reviews.

The Incident Response Plan shall be tested time to time and communicated to all staff members of the organization.

Guidelines to develop an Incident Response Plan are presented in the Information and Cyber Security Implementation Guide.

***Compliance: Applicable to all government organizations***

#### **4.5.2 Policy on Activating Incident Response Plan**

In the event of an information security incident, the designated authorized person shall activate the incident response plan to minimize the impact on the organizational operations, and to resume normal operations after the incident.

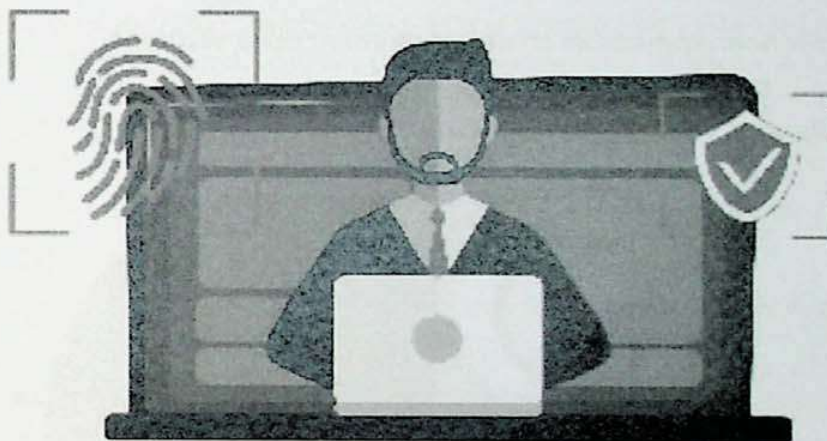
The organization shall maintain an Incident Register to record information related to the incidents. Incident Register shall contain the following information at a minimum: date and time of the incident, name and designation of the employee who reported the incident, description of the incident, nature of the impact, classification of the incident, action taken in response to the incident, officer in charge of handling the incident, current status of the incident and so forth.

Guidelines for responding to incidents are presented in the Information and Cyber Security Implementation Guide.

In the event of an information and cyber security incident, the organization has to initiate procedures to identify, collect and preserve information, which can serve as evidence that can be used in forensics investigations. The policies related to forensic investigation is presented in Section 4.5.3.

**Compliance:** *Applicable to all government organizations*

#### **4.5.3 Policy on Forensic Investigations**



In the event where forensic investigation is required, the organization shall follow a formal investigation process. The evidence related to forensic investigation can be captured through a wide range of electronic means such as physical documents, data on the hard disks, device logs, CCTV footage, email records, voice records and other electronic records, etc.

Since electronic evidence is different from traditional evidence as to its nature of intangibility, volatility and replicability, expert knowledge is essential to deal with such evidence. The organization shall obtain the technical assistance from Sri Lanka CERT or a relevant organization which has such technical capabilities.

In a forensic investigation, the chain of custody shall be maintained by the organization which requires the following information at a minimum: details of the incident and collected evidence, date and time of the evidence collected, the name and the designation from whom the evidence was obtained and the history of transferring the evidence. ISO shall maintain the chain of custody that shall be presented in an investigation.



It is required that the ISO of the organization has the responsibility of retaining and preserving all evidence that concerns ongoing, pending or foreseeable claims. This includes the responsibility of not to lose, destroy, or intentionally alter documents, electronic records, or similar instruments that can be used as evidence.

In a forensic investigation, legal frameworks related to personal data protection, computer crimes, payment device frauds, electronic transactions and any other relevant laws shall be applied.

**Compliance: Applicable to all government organizations**

#### 4.6 Recover Normal Operations



The organization shall develop and implement a plan of effective activities to restore any capabilities or services that were impaired due to a disaster.

Policies that the organization shall comply in recovering from disasters or information and cyber security incidents are presented below.

#### **4.6.1 Policy on Disaster Recovery Plan**

The organization shall have a Disaster Recovery Plan that will be activated in an event of a disaster (or incident) to facilitate recovery from such disaster (or incident).

The Disaster Recovery Plan shall contain activities to be performed to recover from a disaster, and roles and responsibilities of each team member in the plan.

Disaster Recovery Plan shall be designed by conducting a risk assessment and a business impact analysis of the information and IT assets, and the recovery activities shall be designed by considering the earliest point in time at which it is acceptable to recover the data (recovery time objective), and the earliest point in time at which the organization's operations and systems must be resumed after a disaster (recovery point objective).

The Disaster Recovery Plan shall be tested and updated on a periodic basis.

***Compliance: Applicable to all government organizations***

#### **4.6.2 Policy on Activating Disaster Recovery Plan**

In an event of a disaster, the designated authorized person shall activate the disaster recovery plan to minimize the impact on the organization's operations, and to resume normal operations after the event.

***Compliance: Applicable to all government organizations***

#### **4.6.3 Policy on Crisis Communication**

In the event of a major crisis (e.g. critical disaster, cyber security incident), as decided by the HOO, the organization shall communicate with internal and external parties such as the ministry in charge of the organization, Sri Lanka CERT, victims, media, clients, and law enforcement authorities according to a plan. The organization shall appoint a senior responsible officer to communicate the crisis to the relevant stakeholders.

***Compliance: Applicable to all government organizations***



## 5. Policies to be Implemented on a Priority Basis

In order to implement the Information and Cyber Security Policy within the organization, the following policies need to be implemented at the priority basis.

| Policy Area                                      | Policy No. | Policies to be Implemented on a Priority Basis                                                                                                   | All Organizations | CNII Providers |
|--------------------------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------|
| <b>Information and Cyber Security Governance</b> | 4.1.1      | Providing leadership to implement the Information and Cyber Security Policy by the HOO.                                                          | ✓                 | ✓              |
|                                                  | 4.1.2      | Establishment of an Information and Cyber Security Organizational Structure.                                                                     | ✓                 | ✓              |
|                                                  | 4.1.2 (a)  | Appoint an ISO and delegate information and cyber security responsibilities.                                                                     |                   | ✓              |
|                                                  | 4.1.2 (b)  | In the absence of an ISO, assign responsibilities to the CIO to protect information and IT assets.                                               | ✓                 |                |
|                                                  | 4.1.2 (C)  | Assign responsibilities to (Chief) IA to coordinate information and cybersecurity audits.                                                        | ✓                 | ✓              |
|                                                  | 4.1.3      | Appoint an ISC.                                                                                                                                  | ✓                 | ✓              |
|                                                  | 4.1.4      | Appoint RMC.                                                                                                                                     |                   | ✓              |
|                                                  | 4.1.5      | Identify user responsibilities and communicate to users.                                                                                         | ✓                 | ✓              |
|                                                  | 4.1.6      | Capacity building of officials responsible for information and cyber security.                                                                   | ✓                 | ✓              |
|                                                  | 4.1.7      | Perform security clearance and background checks on staff handling information assets classified as secret and confidential or staff using CNII. |                   | ✓              |

| Policy Area                                    | Policy No. | Policies to be Implemented on a Priority Basis                                                              | All Organizations | CNII Providers |
|------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------|-------------------|----------------|
|                                                | 4.1.8      | Align information and cybersecurity activities with the vision, mission and objectives of the organization. | ✓                 | ✓              |
|                                                | 4.1.9      | Develop and implement information and cyber security action plans.                                          | ✓                 | ✓              |
| <b>Identify Assets, Asset Owners and Risks</b> | 4.2.1      | Identify information, IT assets and CNII.                                                                   | ✓                 | ✓              |
|                                                | 4.2.3      | Identify Asset Owners, Custodians and assign responsibilities to protect assets.                            | ✓                 | ✓              |
|                                                | 4.2.4      | Maintain information and IT assets registers.                                                               | ✓                 | ✓              |
|                                                | 4.2.5      | Perform risk assessments for information and IT assets.                                                     |                   | ✓              |
|                                                | 4.2.6      | Classify information and IT assets based on their value and sensitivity.                                    | ✓                 | ✓              |
| <b>Protect Assets</b>                          | 4.3.1      | Protect data at rest.                                                                                       | ✓                 | ✓              |
|                                                | 4.3.2      | Protect data at transit.                                                                                    | ✓                 | ✓              |
|                                                | 4.3.3      | Ensure physical security of information and IT assets.                                                      | ✓                 | ✓              |
|                                                | 4.3.4      | Control user access to information and IT assets.                                                           | ✓                 | ✓              |
|                                                | 4.3.5      | Ensure strong authentication.                                                                               | ✓                 | ✓              |
|                                                | 4.3.6      | Ensure data Sovereignty in an appropriate manner.                                                           | ✓                 | ✓              |
|                                                | 4.3.7      | Use valid licensed software and update the latest patches.                                                  | ✓                 | ✓              |
|                                                | 4.3.8      | Install antimalware software.                                                                               | ✓                 | ✓              |



| Policy Area | Policy No. | Policies to be Implemented on a Priority Basis                                                                               | All Organizations | CNII Providers |
|-------------|------------|------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------|
|             | 4.3.9      | Use official email for official communications.                                                                              | ✓                 | ✓              |
|             | 4.3.10     | Ensure security of emails.                                                                                                   | ✓                 | ✓              |
|             | 4.3.11     | Use digital signatures as appropriate.                                                                                       | ✓                 | ✓              |
|             | 4.3.12     | Implement perimeter security controls.                                                                                       | ✓                 | ✓              |
|             | 4.3.13     | Use secure remote access methods.                                                                                            | ✓                 | ✓              |
|             | 4.3.14     | Use a backup strategy.                                                                                                       | ✓                 | ✓              |
|             | 4.3.16     | Ensure security by design principles in software development and acquisition.                                                | ✓                 | ✓              |
|             | 4.3.17     | Ensure secure disposal of Assets.                                                                                            | ✓                 | ✓              |
|             | 4.3.18     | Implement an internal information security audit process.                                                                    | ✓                 | ✓              |
|             | 4.3.19     | Perform risk assessments and penetration tests prior to the official launch of website, web application or any other system. | ✓                 | ✓              |
|             | 4.3.20     | Strengthen the security resilience of IT assets.                                                                             | ✓                 | ✓              |
|             | 4.3.21     | Follow work from home guidelines in remote working.                                                                          | ✓                 | ✓              |
|             | 4.3.23     | Prevent using untrusted networks.                                                                                            | ✓                 | ✓              |
|             | 4.3.24     | Manage suppliers.                                                                                                            | ✓                 | ✓              |
|             | 4.3.25     | Manage changes.                                                                                                              | ✓                 | ✓              |

| Policy Area                      | Policy No. | Policies to be Implemented on a Priority Basis            | All Organizations | CNII Providers |
|----------------------------------|------------|-----------------------------------------------------------|-------------------|----------------|
| <b>Detect Incidents</b>          | 4.4.1      | Instruct staff to report incidents.                       | ✓                 | ✓              |
|                                  | 4.4.2      | Review logs to identify incidents.                        | ✓                 | ✓              |
|                                  | 4.4.3      | Identify incidents by continuously monitoring the events. |                   | ✓              |
|                                  | 4.4.4      | Report incidents to Sri Lanka CERT.                       | ✓                 | ✓              |
| <b>Respond to Incidents</b>      | 4.5.1      | Develop Incident Response Plan.                           | ✓                 | ✓              |
|                                  | 4.5.2      | Activate Incident Response Plan in an event of incident.  | ✓                 | ✓              |
|                                  | 4.5.3      | Perform forensic investigations on incidents.             | ✓                 | ✓              |
| <b>Recover Normal Operations</b> | 4.6.1      | Develop Disaster Recovery Plan.                           | ✓                 | ✓              |
|                                  | 4.6.2      | Activate Disaster Recovery Plan in an event of disaster.  | ✓                 | ✓              |
|                                  | 4.6.3      | Develop Crisis Communication Plan.                        | ✓                 | ✓              |



## **6. Methodology for Monitoring and Evaluating the Information and Cyber Security Policy**

---

- 6.1 Prior to the implementation of the Policy, it is essential to understand the overall information and cyber security readiness of the government organization. This assessment tool is therefore designed to assess the overall information and cyber security readiness, and the progress of the adoption of the Policy by government organizations.
- 6.2 Accordingly, the Sri Lanka CERT shall perform a preliminary assessment of the readiness of government organizations in implementing the Policy based on the questions presented in Section 6.6. Based on the findings, recommendations will be made to government organizations in implementing the Policy.
- 6.3 Sri Lanka CERT shall evaluate the level of policy compliance by each government organization on an annual basis, and shall present the level of compliance on an Information Security Index. Based on the revaluation results, Sri Lanka CERT shall make recommendations to improve the overall information and cyber security readiness of the organization.
- 6.4 To evaluate the performance (or readiness) of implementing the Policy within the organization, the questionnaire presented in Section 6.6 which contains approximately 50 questions, will be used. ISO, CIO or Officer in charge of the subject of IT shall complete and submit the questionnaire to Sri Lanka CERT on or before October 30th of each year, with the signature of the HOO.
- 6.5 Should the respondent wish to provide a detailed response to each question, the respondent can provide details in the remarks section at the end of the survey questionnaire. Respondents can refer to the Glossary of this document for detailed explanation of relevant terms.
- 6.6 **Assessment Questionnaire**  
All government organizations are required to respond to every question up to the best of their knowledge.

| Policy Domains                            | Assessment Criteria                                                                                                                               | Policy    | Compliance |    | Remarks |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------|----|---------|
|                                           |                                                                                                                                                   |           | Yes        | No |         |
| Information and Cyber Security Governance |                                                                                                                                                   |           |            |    |         |
| Security Organization Structure           | 1. Has the organization appointed an ISO?                                                                                                         | 4.1.2 (a) |            |    |         |
|                                           | 2. Has the organization assigned information and cyber security responsibilities to ISO?                                                          | 4.1.2 (a) |            |    |         |
|                                           | 3. In an absence of ISO, has the CIO or the officer in charge of the subject of IT been assigned information and cyber security responsibilities? | 4.1.2 (b) |            |    |         |
|                                           | 4. Has the organization assigned information security audit responsibilities to (Chief) IA?                                                       | 4.1.2 (c) |            |    |         |
|                                           | 5. Does the organization have a Committee to make decisions on information and cyber security?                                                    | 4.1.3     |            |    |         |
|                                           | 6. Does the organization have a committee to make decisions on information and cyber security risks?                                              | 4.1.4     |            |    |         |



| Policy Domains            | Assessment Criteria                                                                                                                                                            | Policy | Compliance |    | Remarks |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                           |                                                                                                                                                                                |        | Yes        | No |         |
| End User Responsibilities | 7. Has organization explained the end user responsibilities to users?                                                                                                          | 4.1.5  |            |    |         |
| Capacity Building         | 8. Has the organization taken any steps to develop the information security capacity of accountable individuals?                                                               | 4.1.6  |            |    |         |
| Background Checks         | 9. Does your organization perform background checks and security clearance on officials dealing with "Secret" or "Confidential", information assets or having access to CNII ? | 4.1.7  |            |    |         |
| Strategic Alignment       | 10. In designing and implementing the organization's functions, policies, strategies or projects, has your organization taken information security into account?               | 4.1.8  |            |    |         |

| Policy Domains                            | Assessment Criteria                                                                                | Policy | Compliance |    | Remarks |
|-------------------------------------------|----------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                                           |                                                                                                    |        | Yes        | No |         |
| Action Plan                               | 11. Does your organization have financial provisions for information security activities?          | 4.1.9  |            |    |         |
|                                           | 12. Has your organization developed action plans to achieve its information security objectives?   | 4.1.10 |            |    |         |
| Identify Assets, Owners, Users, and Risks |                                                                                                    |        |            |    |         |
| Identification of Assets                  | 13. Has your organization identified information assets that have a value to the organization?     | 4.2.1  |            |    |         |
|                                           | 14. Has your organization assessed risk associated with information assets?                        | 4.2.5  |            |    |         |
|                                           | 15. Has your organization identified information assets that have a value to the organization?     | 4.2.1  |            |    |         |
|                                           | 16. Has your organization assessed risk associated with information assets?                        | 4.2.5  |            |    |         |
|                                           | 17. Has your organization classified information assets based on their sensitivity or other means? | 4.2.6  |            |    |         |



| Policy Domains             | Assessment Criteria                                                                                                      | Policy | Compliance |    | Remarks |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                            |                                                                                                                          |        | Yes        | No |         |
|                            | 18. Has your organization recorded IT assets in an IT Assets Register?                                                   | 4.2.4  |            |    |         |
|                            | 19. Has your organization classified IT assets based on their criticality?                                               | 4.2.6  |            |    |         |
|                            | 20. Has your organization identified the Owners of the assets?                                                           | 4.2.3  |            |    |         |
| <b>Protect Assets</b>      |                                                                                                                          |        |            |    |         |
| <b>Encryption</b>          | 21. Does your organization encrypt sensitive information prior to storage?                                               | 4.3.1  |            |    |         |
|                            | 22. Does your organization encrypt sensitive information prior to moving through electronic channels?                    | 4.3.2  |            |    |         |
| <b>Physical Protection</b> | 23. Does your organization process or store sensitive information in secure areas?                                       | 4.3.3  |            |    |         |
|                            | 24. Has your organization taken appropriate measures to protect secure areas from fire, flood, humidity and temperature? | 4.3.3  |            |    |         |

| Policy Domains                         | Assessment Criteria                                                                                                      | Policy | Compliance |    | Remarks |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                                        |                                                                                                                          |        | Yes        | No |         |
| Protect Assets                         |                                                                                                                          |        |            |    |         |
|                                        | 25. Does your organization prevent unauthorized entry to secure areas?                                                   | 4.3.3  |            |    |         |
| Physical Protection                    | 23. Does your organization process or store sensitive information in secure areas?                                       | 4.3.3  |            |    |         |
|                                        | 24. Has your organization taken appropriate measures to protect secure areas from fire, flood, humidity and temperature? | 4.3.3  |            |    |         |
|                                        | 25. Does your organization prevent unauthorized entry to secure areas?                                                   | 4.3.3  |            |    |         |
| Identity Management and Access Control | 26. Does your organization have an Identity Management and Access Control Policy?                                        | 4.3.4  |            |    |         |
|                                        | 27. Does your organization use strong authentication?                                                                    | 4.3.5  |            |    |         |

| Policy Domains                      | Assessment Criteria                                                                                                    | Policy | Compliance |    | Remarks |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                                     |                                                                                                                        |        | Yes        | No |         |
| Data Sovereignty                    | 28. Does your organization ensure Data Sovereignty?                                                                    | 4.3.6  |            |    |         |
|                                     | 29. Does your organization assess risk prior to obtaining cloud service?                                               | 4.3.6  |            |    |         |
| Licensed Software and Patch Updates | 30. Does the organization use operating systems (OSs) with valid License(s)?                                           | 4.3.7  |            |    |         |
|                                     | 31. Have the OSs (s) of the organization been updated with vendor supplied latest patches and fixes?                   | 4.3.7  |            |    |         |
|                                     | 32. Does your organization have a procedure in place to ensure vendor supplied critical patches are installed on time? | 4.3.7  |            |    |         |
| Antimalware                         | 33. Has the organization installed Antimalware software with a valid license in all machines?                          | 4.3.8  |            |    |         |



| Policy Domains             | Assessment Criteria                                                                               | Policy | Compliance |    | Remarks |
|----------------------------|---------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                            |                                                                                                   |        | Yes        | No |         |
| Email                      | 34. Does your organization restrict users from using personal emails for official communications? | 4.3.9  |            |    |         |
|                            | 35. Does your organization set up email filters to remove emails known to have malware attached?  | 4.3.10 |            |    |         |
|                            | 36. Does your organization use encryption when sending sensitive information via email?           | 4.3.10 |            |    |         |
| Perimeter Security Devices | 37. Does your organization have a Firewall in your computer network?                              | 4.3.12 |            |    |         |
| Secure Remote Access       | 38. Does your organization use secure Virtual Private Networks (VPNs) for remote access?          | 4.3.13 |            |    |         |
|                            | 39. Do all the users connecting remotely use VPN?                                                 | 4.3.13 |            |    |         |

| Policy Domains                              | Assessment Criteria                                                                                                                                                               | Policy | Compliance |    | Remarks |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                                             |                                                                                                                                                                                   |        | Yes        | No |         |
| Backup Strategy                             | 40. Does your organization backup data?                                                                                                                                           | 4.3.14 |            |    |         |
|                                             | 41. Are the backups stored at a fire proof, secure location which is physically distant from the data processing site?                                                            | 4.3.14 |            |    |         |
| Secure Disposal of Assets                   | 42. Does your organization follow any of the following to dispose electronic media that contain sensitive information?<br>- Shredding, punching, physically damaging, degaussing. | 4.3.17 |            |    |         |
| Internal Information Security Audit Program | 43. Does your organization have internal information security audit program?                                                                                                      | 4.3.18 |            |    |         |
|                                             | 44. Does your organization perform VAPTs through Sri Lanka CERT prior to any deployment of software applications?                                                                 | 4.3.19 |            |    |         |
|                                             | 45. Have you performed VAPT for your computer network?                                                                                                                            | 4.3.19 |            |    |         |



| Policy Domains                           | Assessment Criteria                                                                                                                                                                                                                            | Policy | Compliance |    | Remarks |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                                          |                                                                                                                                                                                                                                                |        | Yes        | No |         |
| Work from Home                           | 46. Does your organization adhere to the work from home guidelines issued by Sri Lanka CERT?                                                                                                                                                   | 4.3.21 |            |    |         |
|                                          |                                                                                                                                                                                                                                                |        |            |    |         |
| Using Personal Devices for Official Work | 47. Does your organization have a formal procedure to register personal devices?                                                                                                                                                               | 4.3.22 |            |    |         |
|                                          | 48. Does your organization allow personal devices to process or store critical data?                                                                                                                                                           | 4.3.22 |            |    |         |
| Detect Information Security Incidents    |                                                                                                                                                                                                                                                |        |            |    |         |
| Report Incidents                         | 49. Has the organization instructed staff to report any suspicious activity, contact, theft, virus, vulnerability, unauthorized access, tampering with files, or violation of security policy to the person in charge of Information security? | 4.4.1  |            |    |         |
|                                          | 50. Have you ever reported cyber security incidents to Sri Lanka CERT or any other party?                                                                                                                                                      | 4.4.4  |            |    |         |



| Policy Domains                               | Assessment Criteria                                                                                                                                                                        | Policy | Compliance |    | Remarks |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------|----|---------|
|                                              |                                                                                                                                                                                            |        | Yes        | No |         |
| Respond to Incidents                         |                                                                                                                                                                                            |        |            |    |         |
| Incident Response Plan and Activate the Plan | 51. Has your organization developed an Incident Response Plan?                                                                                                                             | 4.5.1  |            |    |         |
|                                              | 52. In the event of an information and cyber security event, does the organization activate an Incident Response Plan to minimize the impact on its operations and restore that operation? | 4.5.2  |            |    |         |
| Recover from Incidents                       |                                                                                                                                                                                            |        |            |    |         |
| Disaster Recovery Plan and Activate the Plan | 53. Does your organization have a Disaster Recovery Plan developed to facilitate the recovery in an event of a disaster?                                                                   | 4.6.1  |            |    |         |
|                                              | 54. In the event of a disaster (or event), does the organization activate its Disaster Recovery Plan to restore disrupted services?                                                        | 4.6.2  |            |    |         |

## Glossary

|                                       |                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Antimalware</b>                    | Anti-malware is a software designed to identify malware in devices or prevent malware from infecting computer systems or electronic devices. Malware is any software intentionally designed to cause damage to a computer, server, or computer network (e.g. viruses, worms, ransomware).                              |
| <b>Assets Classification</b>          | Classification is the process of categorizing information assets based on the level of sensitivity and criticality of that information. The primary objective of asset classification is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. |
| <b>Assets Custodian</b>               | Person in the organization who has the responsibility to protect an information asset throughout the lifecycle as it is stored, transported, or processed in line with the requirements defined by the information asset owner.                                                                                        |
| <b>Assets Owner</b>                   | An asset owner is a senior executive grade official responsible for the day-to-day management of assets. The asset owner controls the entire life cycle of the asset and must identify the risks to the assets and suggest appropriate security measures to protect them.                                              |
| <b>Availability of Information</b>    | Availability ensures timely and reliable access to and use of information.                                                                                                                                                                                                                                             |
| <b>Confidentiality of Information</b> | Confidentiality refers to the assurance that information is not disclosed to unauthorized people and organizations.                                                                                                                                                                                                    |
| <b>Sensitive Information Assets</b>   | Any information the loss, alteration, misuse, disclosure or failure of which could adversely affect the interests of the organization or relevant individuals or entities. These information assets can be classified as "secret" and "confidential" by the government organization.                                   |



|                                                            |                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Critical IT Assets</b>                                  | Critical IT assets are systems, the unauthorized access, misuse, or failure of which can adversely affect data, organization, or individuals. These IT assets can be classified as "very critical" and "critical" by the organization. Further, these IT assets require a high level of security and may also exist in the form of CNII as defined below. |
| <b>Critical National Information Infrastructure (CNII)</b> | Critical information infrastructure are the systems or facilities, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy, health and social well-being of a nation.                                                                                                                                 |
| <b>Digital Signature</b>                                   | Digital Signature is a mathematical scheme for verifying the authenticity of digital messages or documents. It provides sender authenticity (identity of the users), message integrity (guarding against improper modification or destruction), and nonrepudiation (the claimed sender cannot later deny generating the document).                        |
| <b>Encryption</b>                                          | Encryption is the process of converting a plaintext message into a secure-coded form of text, which cannot be understood without converting it back via decryption.                                                                                                                                                                                       |
| <b>Government Organizations</b>                            | The government organizations are the public authorities defined in the Right to Information Act No. 12 of 2016.                                                                                                                                                                                                                                           |
| <b>Information Security Controls</b>                       | Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to information and IT assets. Controls could be technologies, policies, procedures, or processors put in place to protect information assets.                                                                                                |
| <b>Information Security Officer (ISO)</b>                  | An Information Security Officer is a senior-level executive responsible for establishing and maintaining the organization's objectives, strategy, and action plans to ensure information assets are adequately protected.                                                                                                                                 |
| <b>Information Security Committee (ISC)</b>                | In implementing the policy, this committee is responsible for reviewing and approving all information security controls, action plans, asset classification schemes, incidents response plans and disaster recovery plans and other activities carried out by the ISO.                                                                                    |



**Information and Event Management systems (SIEM)**

SIEM is a solution that combines the collection data from log files for analysis and reports on security threats and events, and conduct real-time system monitoring, notifies network admins about important issues and establishes correlations between security events to provide real-time analysis of security alerts generated by applications and network hardware.

**Information and Cyber Security**

Information and cyber security is the protection of information assets from unauthorized access, use, modification, or destruction to ensure confidentiality, integrity and availability of the information. This includes protection of IT assets that contain or use informational assets from malicious actions of individuals with the use of cyber technology or other means, and from other natural disasters such as floods and fires.

**Information Assets**

Information asset is information or data that is of value to the organization. This includes the documents available in an electronic format, database records as well as the documents available in paper format. Examples for information assets: word file, images, employees personal record in a database.

**IT Assets**

IT asset is any IT equipment, information system, software, storage media that is of value to the organization. Examples for IT assets are computers, servers, routers, disks, networks, software, information systems and its components.

**Intrusion Detection and Prevention Systems (IPS/IDS)**

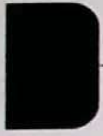
Intrusion Detection Systems are devices that analyze network traffic to identify known cyberattacks. Intrusion Prevention Systems devices analyzes network traffic to identify known cyberattacks, however, it can stop attacks by preventing packet from being delivered based on type of attacks it detects

**Integrity of Information**

Integrity refers to guarding information against improper modification. It ensures that information remains in its original form.

**Official Email**

Official emails are the email accounts supplied by the government with the domain name of "gov.lk"



|                                       |                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Private Cloud</b>                  | Services offered over the Internet or over a private internal network to only select users. E.g. Lanka Government Cloud                                                                                                                                                                                                                                                      |
| <b>Public Cloud</b>                   | Cloud service available to anyone who wants to purchase them                                                                                                                                                                                                                                                                                                                 |
| <b>Recovery Point Objective (RPO)</b> | RPO is a measure of how often the organization should take backups, and it gives an indication of how up to date the recovered data will be. It indicates the earliest possible time in which it is acceptable to recover the data. For example, if a disaster occurs between backups, can the organization afford to lose 2 minutes' worth of data, or 2 hours or full day. |
| <b>Recovery Time Objective (RTO)</b>  | RTO indicates the amount of downtime a business can tolerate. It is the earliest point in time at which the organization's operations and systems must be resumed after a disaster.                                                                                                                                                                                          |
| <b>Systems Hardening</b>              | System hardening is the process of securing a system through changing the default configuration and settings to reduce IT vulnerability and the possibility of being compromised. This can be done by reducing the attack surface and attack vectors which attackers continuously try to exploit for the purpose of malicious activity.                                      |
| <b>Virtual Private Network (VPN)</b>  | Virtual Private Network, establishes a secure connection by utilizing an encrypted tunnel for data communication over the internet.                                                                                                                                                                                                                                          |



## References

1. Information Security Implementation Guide. Published in 2022, by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through [www.onlinesafety.lk](http://www.onlinesafety.lk).
2. Minimum Information Security Guidelines. Published by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through [www.onlinesafety.lk](http://www.onlinesafety.lk).
3. Information and Cyber Security Strategy of Sri Lanka (2019:2023), Published in November 2019 by Research and Policy Unit, Sri Lanka CERT. Document can be accessed through <https://cert.gov.lk/documents/NCSSStrategy.pdf>.
4. NIST Cybersecurity Framework. Published by National Institute of Standards and Technology, U.S Department of Commerce. Resource can be accessed through <https://www.nist.gov/cyberframework/online-learning/five-functions>.
5. Information Security Guidelines for Working from Home. Published by Sri Lanka CERT. Document can be access through <https://www.onlinesafety.lk>.
6. Website Security Guidelines for Government Organizations. Published by Research, Policy and Projects Division of Sri Lanka CERT, in 2022. Document can be accessed through <https://www.onlinesafety.lk>.
7. Web Application Security Guidelines for Government Organizations. Published by Research, Policy and Projects Division of Sri Lanka CERT, in 2022. Document can be accessed through <https://www.onlinesafety.lk>.
8. Technical Guidelines for Web Application and Website Security. Published by Research, Policy and Projects Division of Sri Lanka CERT in 2022. Document can be accessed through <https://www.onlinesafety.lk>.
9. ISO 27002 (2013): Information Technology – Security Techniques – Information Security Management Systems – Requirements, International Standards Organization, Published by International Standard Organization. Document can be accessed through <https://www.iso.org>.



මගේ අංකය  
எனது இல.  
My No.

ඔබේ අංකය  
உமது இல.  
Your No.

දුරකථන අංක  
தொலைபேசி இல.  
Telephone No.

ඉලෙක්ට්‍රොනික් තැපෑල  
மின்னஞ்சல்  
E-mail

ෆැක්ස්  
தொலைநகல்  
Fax

E/252/2026

PS/LEG/CO/10/1/CoPF

2147888  
2433967  
2320800  
2327919  
2149001(2)

administration@attorneygeneral.gov.lk

2436421



නීතිපති දෙපාර්තමේන්තුව  
சட்டமா அதிபர் திணைக்களம்  
ATTORNEY - GENERAL'S DEPARTMENT



Annex 7

அஞ்சல் பெட்டி } 502  
P. O. Box No.

කොළඹ 12.  
கொழும்பு 12.  
Colombo 12.

15.June.2026.....

Attn: Mr. Kamal Udapola, Secretary to the Committee  
Committee on Public Finance

Secretary General of Parliament  
Parliament

**COMMITTEE ON PUBLIC FINANCE (COPF)**  
**RE: MEETING HELD ON 8 JUNE 2026**



I refer to your letter dated 9 June 2026 seeking certain clarifications.

Having considered the relevant laws in this regard, and having had discussions with the officers of the Ministry of Finance and the Central Bank, my observations on the matters upon which clarification has been sought are set out below.

**A. Scope of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA)**

1. The FTRA does **not explicitly list every Institution that falls within its ambit**, nor does it **expressly exclude or include the Central Bank of Sri Lanka ("CBSL") within the text of the FTRA itself**. As such, the question of whether the CBSL falls within the ambit of the FTRA as an Institution would have to be examined by considering the FTRA as a whole and the functions of the CBSL.

***Purpose of the FTRA***

2. The FTRA was enacted to **combat money laundering and terrorist financing**, as is evident from the Long Title of the FTRA, and required certain institutions to conduct customer due diligence, maintain records, and report suspicious transactions to the Financial Intelligence Unit (FIU) established under the Act.

4 Definition of an Institution under the FTRA

3. The FTRA provisions would be applicable to an "Institution" as defined therein. An Institution is defined as *"any person or body of persons engaged in or carrying out any finance business or designated non-finance business within the meaning of this Act"*.
4. The term "Finance Business" is defined as including any one of the following businesses or activities:
  - (a) banking business as defined in the Banking Act, No. 30 of 1988 ;
  - (b) finance business as defined in the Finance Companies Act, No. 78 of 1988 (irrespective of whether the person is licensed or registered under the Act);
  - (c) lending, including consumer credit, mortgage credit, factoring (with or without recourse) and financing of commercial transactions;
  - (d) financial leasing other than transactions relating to consumer products;
  - (e) the transfer of money or value;
  - (f) money and currency changing services;
  - (g) issuing and managing means of payment (i.e. credit cards, travellers' cheques, money orders and bankers' drafts and electronic money);
  - (h) issuing financial guarantees and commitments, including but not limited to consumer credit, factoring with or without recourse and financing of commercial transactions including forfeiting;
  - (i) trading for its own account or for the account of customers in money market instruments (i.e. cheques, bills, certificates of deposit and derivatives), foreign exchange, exchange, interest rate and index instruments, commodity futures trading and transferable securities;
  - (j) participating in securities issues and the provision of financial services related to such issues; and
  - (k) such other business as may be prescribed from time to time by the Minister taking into consideration the interests of the national economy.

5. Even though specific "activities" are also considered as "Finance Business", it would appear that an Institution should be engaged in a business relationship. Such approach is consistent with the definition of an "Institution" in the Financial Action Task Force Recommendations, which states that *"Financial institutions means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: ..."*

Functions of the CBSL

6. The CBSL is the central bank and apex monetary authority of Sri Lanka, established under its own statute (Central Bank of Sri Lanka Act, No. 16 of 2023). It has statutory authority over monetary policy, currency issuance, payment systems, bank supervision, and financial stability.
7. It is not a licensed commercial bank and does not provide any traditional "banking" services to the public or any institutions, other than the Government of Sri Lanka ("GOSL") and certain identified Government Funds. It does not receive any payment for the services rendered to the GOSL, though any expenses incurred on behalf of the GOSL is recovered from the GOSL. Thus, the services provided to the GOSL by the CBSL are not provided on the basis of a business relationship, but instead largely on the basis of statutory obligations.

8. In the aforesaid circumstances, it is unlikely that the CBSL could be categorised as an "Institution" under the FTRA.

#### *CBSL as a Supervisory Authority*

9. However, the CBSL's functions include supervising financial institutions. Consequently, the obligations imposed on supervisory authorities under Part IV of the FTRA (sections 22 and 23) would be directly applicable to the CBSL, and it would be required to comply with such obligations.

#### *The Reporting Obligations under the FTRA are geared towards Customers*

10. Furthermore, the obligations contemplated in Sections 2 - 5 of the FTRA are primarily concerned with regard to the "customers" of an Institution, and given that the sole "customer" of the CBSL is the GOSL, it is unlikely that the FTRA was intended to apply to the CBSL in the performance of its services to the GOSL. For instance, the obligations include identifying customers before conducting business, which is not applicable in the context of the GOSL as a customer.
11. The financial transaction limits referred to in Section 6 of the FTRA also reinforces such view, as mandatory reporting requirements would be triggered even in connection with State transactions upon such transactions exceeding the prescribed limits.

#### *The FIU and CBSL Relationship*

12. The Financial Intelligence Unit (FIU Sri Lanka) is established by the FTRA as the entity that receives reports and oversees compliance. The FIU has been administratively placed within the CBSL to operate and leverage the Bank's regulatory capabilities.
13. Such placement does not mean the CBSL is a reporting institution under the FTRA, but, rather, that it hosts the agency responsible for supervision and enforcement of the FTRA.
14. Under the FTRA framework, it is the FIU that monitors compliance; the CBSL as an institution does not itself report suspicious or currency transactions it undertakes for monetary policy purposes. Instead, it mandates compliance from other financial institutions. The FTRA's reporting duties are directed at those institutions that have customers and transactions to report.

#### *Conclusion*

15. In the aforesaid circumstances, the CBSL's statutory duties do not subject the CBSL to reporting obligations under the FTRA.
16. However, the question of whether any safeguards need to be imposed in respect of the services provided by the CBSL to the GOSL is a policy matter that would have to be decided upon. In doing so it would be prudent to carry out a comprehensive analysis of the functions carried out and the services provided and the attendant risks and prescribe appropriate reporting obligations.



**B. Section 132 of the Central Bank of Sri Lanka Act, No. 16 of 2023 (Central Bank Act) and the Order made under Section 37 of the Public Debt Management Act, No. 33 of 2024 (PDMA)**

17. In terms of Section 132 of the Central Bank Act, notwithstanding the absence of comparable provisions in the Central Bank Act, the CBSL was mandated to perform the services provided for in Sections 112 and 113 of the repealed Monetary Law Act, *"until such date as the relevant law relating to public debt management agency or office comes into operation"*.

18. The law relating to the Public Debt Management Office ("PDMO") came into effect on 25 November 2024, upon the publication of an "appointed date" by Order published in the Gazette of 21 November 2024, made in terms of Section 1(2) of the PDMA.

19. Accordingly, in the ordinary course, CBSL's functions in relation to the above would have ceased upon such publication. However, Section 37 of the PDMA read as follows:

*The applicability of section 132 of the Central Bank of Sri Lanka Act, No. 16 of 2023, shall come into operation on such date as the Minister may by Order published in the Gazette appoint within a period of eighteen months from the appointed date:*

*Provided that, notwithstanding the provisions of this section, the Office may perform its powers and functions under this Act.*

20. In terms of the above provisions of the PDMA the CBSL's requirement to perform such functions was further deferred. Such extension would ordinarily continue until such time as the Minister publishes a further Order, which in the present instance was on 22 May 2026. However, in view of the proviso to Section 37, the PDMO may perform its powers and functions under the PDMA *notwithstanding* the absence of a Gazette under Section 37.

21. From the material made available to me, it would appear that the CBSL had formally handed over the functions relating to the management of public debt to the PDMO with effect from 1 January 2026, and the PDMO had proceeded on such basis. In view of the proviso to Section 37 there is no legal impediment to the PDMO exercising its powers under the PDMA thereafter.

  
Oswald Perera  
State Counsel

Sgd./ Nirmalan Wigneswaran  
Deputy Solicitor General  
for Attorney General



මගේ අංකය }  
 எனது இல. }  
 My No.

ඔබේ අංකය }  
 உமது இல. }  
 Your No.

දුරකථන අංක }  
 தொலைபேசி இல. }  
 Telephone No.

ඉලෙක්ට්‍රොනික් තැපෑල }  
 மின்னஞ்சல் }  
 E-mail

ෆැක්ස් }  
 தொலைநகல் }  
 Fax

E/252/2026

PS/LEG/CO/10/1/CoPF

2147888

2433967

2320800

2327919

2149001(2)

administration@attorneygeneral.gov.lk

2436421

ජීනියම් දෙපාර්තමේන්තුව

சட்டமா அதிபர் திணைக்களம்

ATTORNEY - GENERAL'S DEPARTMENT

කොළඹ 12.  
 கொழும்பு 12.  
 Colombo 12.

25 June 2026



Attn: Mr. Kamal Udapola, Secretary to the Committee  
 Committee on Public Finance

Secretary General of Parliament  
 Parliament

**COMMITTEE ON PUBLIC FIANANCE**

**RE: MEETINGS HELD ON 08 JUNE 2026 AND 23 JUNE 2026**

I refer to your letter dated 23 June 2026 on the above subject.

In terms of the letter under reference, the Hon. Chairman of the Committee on Public Finance has sought a definitive legal opinion on the responsibility for the repayment of Sri Lanka's foreign debt/external debt on certain specified dates.

The repayment of Sri Lanka's external debt involves multiple functions, which includes the allocation of a budget by Parliament for the repayment of debts. Thus, multiple institutions play different roles in the repayment of public debt.

In order to identify the specific functions carried out by the complex web of government institutions, it would be necessary to obtain instructions from all the relevant government institutions involved in this process and to list the different steps/functions and sub-functions that will have to be carried out. Such a process will require significant time.

However, it would appear that the primary concern of the Committee is in connection with the functions that were being carried out by the Public Debt Department (PDD) of the Central Bank, which have been handed over to the newly created Public Debt Management Office (PDMO).

As indicated in my letter dated 15<sup>th</sup> June 2026, the public debt related functions were handed over to the PDMO by the Central Bank and in view of the proviso to Section 37 to

the Public Debt Management Act No. 33 of 2024 (PDMA), the responsibility for carrying out those functions will be with the PDMO upon such hand over. At paragraph 21 of my letter dated 15<sup>th</sup> June 2026, based on the limited instructions that were available at the time, it appeared that the functions had been handed over on 31-12-2025.

However, I am now informed that the functions were not handed over on a single date and that 31-12-2025 was the date on which the handing over process was concluded and that several sub-functions had been handed over on different dates prior to 31-12-2025. I have not been able to independently verify the handing over of such functions/tasks to the PDMO and the relevant dates, which would require significant time. However, at the level of principle, it is my opinion that upon the proper handing over of any function to the PDMO the responsibility for carrying out such specific function would thereafter be that of the PDMO. Without examining the evidence in detail it is not possible to opine on whether or not any specific function was properly handed over.

On the second issue relating to the applicability of the Financial Transaction Reporting Act No. 6 of 2006 (FTRA) to the Central Bank, as indicated in my letter dated 15<sup>th</sup> June 2026, the Central Bank's functions as a banker to the government cannot be equated to the functions of a Commercial Bank providing services to private individuals. The FTRA does not contemplate the Central Bank's statutory functions as falling within its scope. Thus, there is no specific reporting regime with regard to the Central Bank's role as a banker to the Government.

In the event it is decided that a specific reporting regime regarding the Central Bank's functions is needed, a special specific law will have to be introduced to cater for the specific type of the reporting requirements that would be necessary.



Oswald Perera  
State Counsel

Sgd./Nirmalan Wigneswaran  
Deputy Solicitor General  
for Attorney General





මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධන

நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு

MINISTRY OF FINANCE, PLANNING AND ECONOMIC DEVELOPMENT

මහලේකම් කාර්යාලය, කොළඹ 01,  
ශ්‍රී ලංකාව.

செயலகம், கொழும்பு 01,  
இலங்கை.

The Secretariat, Colombo 01,  
Sri Lanka.

කාර්යාලය } 011-2484500  
அலுவலகம் } 011-2484600  
Office } 011-2484700

ෆැක්ස් }  
தொலை நகல் } 011-2449823  
Fax }

වෙබ් අඩවිය }  
இணைய தளம் } www.treasury.gov.lk  
Website }

මගේ අංකය } MF5/PA/04/2026  
எனது இல }  
My No }

ඔබේ අංකය } PS/LEG/CO/10/1/CoPF  
உமது இல }  
Your No }

දිනය } 23.06.2026  
திகதி }  
Date }

Secretary,  
Committee on Public Finance,  
Parliament of Sri Lanka,  
Sri Jayewardenepura, Kotte.



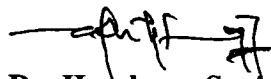
Dear Madam,

**Committee on Public Finance (CoPF)**

This refers to your number and letter dated 17.06.2026.

02. Accordingly, please kindly find attached herewith the document relating to the delegation of authority, for your attention and necessary action.

Yours faithfully,

  
Dr. Harshana Suriyapperuma  
The Secretary to the Treasury

**Delegation of authority of financial control that underline the existing payment process for all florigen debt repayment.**

### **Applicability of FR 135**

Debt service payments are mandatory contractual obligations of the Government and are governed by the terms and conditions of the respective debt instruments and financing agreements. Accordingly, the processing and settlement of such payments are carried out in accordance with the relevant provisions of the Public Debt Management framework and established debt servicing procedures, rather than through the delegation of financial powers under FR 135.

Therefore, over the decades the delegation of financial powers under Financial Regulation (FR) 135 has not been carried out for debt service payments. This was on the basis that debt service obligations, comprising principal repayments, interest payments, and related charges, arise from legally binding borrowing agreements entered into by the Government and therefore, do not constitute discretionary expenditures subject to the approval limits and delegated authorities prescribed under FR 135.

### **Existing Procedures for Debt Service Payments**

In terms of Section 6 (h) of the Public Debt Management Act No. 33 of 2024, the Public Debt Management Office has been given authority to service the debt of the government on a timely basis.

In terms of Section 5(2) of the said Act, the Director General of the Public Debt Management Office is responsible for performing those functions.

Accordingly, a set of guidelines has been issued on 19/09/2025, by the Minister in charge of the subject of finance in accordance with the authority vested in him by Section 7 of the Public Debt Management Act No. 33 of 2024 to ensure the internal control of those functions.

In line with the above guidelines, the PDMO Back Office (BO) has been entrusted with debt servicing responsibilities. The functions are carried out under Directors responsible for the Debt Recording Unit (DRU) and Debt Servicing Unit (DSU), all of which are overseen by an Additional Director General (ADG/ BO).

The debt servicing is totally processed through the Non Reserve Management (NRM) system and the authority levels has been clearly defined and implemented. The authority levels defined in NRM system as follows,

- Entry Level                      - Development Officer
- Verification Level            - Assistant director/ Deputy Director
- Authorization Level       - Director (Debt Servicing Unit)

Debt servicing is done through the account of the Deputy Secretary to the Treasury (DST Account). Since this account is used to make payments in the form of the government debt servicing and other foreign exchange-denominated payments, it is assigned to the Treasury Operations Department (TOD) and maintained by the Central Bank of Sri Lanka. Therefore, the relevant section for the debt servicing vote is assigned under the budget head of the TOD.

The processes have been further streamlined in accordance with the Standard Operating Procedures (SOPs) of the PDMO, which are currently being finalized.





**මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධන අමාත්‍යාංශය**  
**நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு**  
**MINISTRY OF FINANCE, PLANNING AND ECONOMIC DEVELOPMENT**

මහලේකම් කාර්යාලය, කොළඹ 01,  
ශ්‍රී ලංකාව.

කාර්යාලය } 011 - 2484500  
 அலுவலகம் } 011 - 2484600  
 Office } 011 - 2484700

செயலகம், கொழும்பு 01.  
இலங்கை.

ෆැක්ස් }  
 தொலைநகல் } 011 - 2449823  
 Fax }

The Secretariat, Colombo 01.  
Sri Lanka.

වෙබ් අඩවිය }  
 இணையத்தளம் } www.treasury.gov.lk  
 Website }

මගේ අංකය } MF5/PA/04/2026  
 எனது இல. }  
 My No. }

ඔබේ අංකය }  
 உமது இல. }  
 Your No. }

දිනය } 04 April 2026  
 திகதி }  
 Date }

Hon. (Dr.) Harsha de Silva, M.P.  
 Chairman of the Committee on Public Finance  
 Parliament of Sri Lanka  
 Sri Jayawardenepura Kotte

Honourable Chairman,

**Re: Coordination between fiscal and monetary authorities**

This refers to the letter dated 11 March 2025 from the Secretary to the Committee on Public Finance (CoPF), addressed to the Governor, under your direction, with a copy to the Secretary to the Treasury. Accordingly, a meeting is scheduled on 07 April 2026 on "A policy-level discussion with the officials of the Ministry of Finance, Planning and Economic Development (MoF) and the CBSL to address concerns regarding coordination between fiscal and monetary authorities".

In this context, we wish to present our observations on the existing framework and current practices of coordination between the fiscal and monetary authorities.

From the 1950s, following the establishment of the Central Bank of Sri Lanka (CBSL), a prudent coordination between fiscal authorities and CBSL was envisaged, with a view to achieving the envisaged objectives of fiscal and monetary policies. Over time, however, the persistence of large fiscal deficits eroded the effectiveness of this coordination and instead resulted in fiscal dominance of monetary policy. Increased reliance on monetary financing contributed to inflationary pressures and external imbalances, particularly when fiscal expansion exceeded the economy's absorptive capacity. The macroeconomic challenges that culminated in 2022 brought the issue of fiscal dominance sharply into focus and underscored the urgent need to ringfence monetary policy from fiscal developments, thereby safeguarding the operational

independence of monetary policy as well as the focus of the Central Bank on price stability and financial system stability.

Recognising the limitations of the Central Bank's independence and accountability, coordination between the authorities, and previous monetary policy frameworks, the Central Bank of Sri Lanka Act, No. 16 of 2023 (CBA) was enacted, in line with international best practices, to strengthen Central Bank autonomy while ensuring effective fiscal-monetary coordination mechanisms including following.

1. Coordination Council

Under the CBA, monetary-fiscal coordination has been structured in a more meaningful manner through the establishment of the Council for the Coordination of Fiscal, Monetary and Financial System Stability Policies (Coordination Council). The Coordination Council serves as the formal platform for information sharing and dialogue between the Ministry of Finance, Planning and Economic Development (MoF) and the CBSL on macroeconomic developments, outlook, and risks. With the Governor of the Central Bank and the Secretary to the Treasury (ST) as members, the Coordination Council brings together senior officials from both the fiscal authority and the CBSL. Convening quarterly, it facilitates the exchange of relevant monetary and fiscal information, thereby supporting more informed and coherent policy decision-making. As of now, ten quarterly meetings of the Coordination Council have been held successfully since late 2023. Since of late, in line with the Coordination Council meetings, technical-level meetings are also held among relevant officials of the fiscal and monetary authorities to facilitate the proceedings of the Coordination Council meetings and further strengthen analytical engagement and operational coordination between the CBSL and MoF.

2. Financial System Oversight Committee (FSOC)

The CBA provides effective inter-agency coordination in safeguarding financial system stability through the establishment of the FSOC under Section 71 of the Act. Chaired by the Governor of the CBSL, the FSOC comprises senior officials of the CBSL, a Deputy Secretary to the Treasury (DST) nominated by the ST, and the Chief Executive Officers of the Insurance Regulatory Commission of Sri Lanka and the Securities and Exchange Commission of Sri Lanka. This multi-institutional composition enables timely information sharing, policy dialogue, and coordinated

assessments of systemic risks within a macroprudential framework. Through the FSOC, fiscal authorities, monetary authorities, and financial sector regulators engage in structured collaboration, thereby supporting coherent policy responses and strengthening overall financial system stability.

3. Financial Sector Crisis Management Committee (FCCM)

Additionally, with a view to strengthening policy coordination between the CBSL and MoF to enhance crisis preparedness and minimise spillover effects of the recent economic crisis on the financial sector, the Financial Sector Crisis Management Committee (FCCM) was established under the Banking (Special Provisions) Act, No.17 of 2023. The Committee facilitated effective coordination among relevant authorities in addressing emerging risks.

4. Public Debt Coordinating Committee (PDCC)

Meanwhile, in accordance with the Public Debt Management Act, No. 33 of 2024 (PDMA), the public debt management functions previously undertaken by the CBSL were progressively and successfully transferred to the Public Debt Management Office (PDMO) established under the MoF. This transition was implemented in a phased and well-coordinated manner, with the CBSL providing technical assistance, operational support, and continuity arrangements to ensure the smooth transition of responsibilities by the PDMO. With this transition, a Public Debt Coordinating Committee (PDCC) has been established under the PDMA to support alignment between public debt management strategies and broader macroeconomic policies. Chaired by a Deputy Secretary to the Treasury and comprising nine members, including two representatives from the CBSL, the PDCC evaluates borrowing plans and assesses domestic and international market conditions, thereby facilitating ongoing fiscal-monetary coordination in the area of debt management while preserving a clear separation of institutional decision-making responsibilities.

5. International Monetary Fund's Extended Fund Facility (IMF-EFF) Coordination

Consequently, Sri Lanka's earlier-than-anticipated recovery from the economic crisis of 2022 highlights the critical role that effective fiscal and monetary policy coordination has played in restoring macroeconomic stability. Supported by the International Monetary Fund's Extended Fund Facility (IMF-EFF), the implementation of well-coordinated fiscal measures, prudent monetary policy, and key structural



reforms enabled the authorities to regain price stability, strengthen public finances, and gradually revive economic activity. Close and constructive coordination between MoF, other government institutions and CBSL was evident throughout IMF missions and programme review discussions, contributing to coherent policy formulation and consistent implementation. This coordinated policy approach proved instrumental in navigating a period of severe economic distress and has contributed to placing the economy on a more credible path towards long-term stability and sustainable growth.

6. Unified and credible policy narrative approach

Effective fiscal and monetary policy coordination is further reinforced through close and continuous engagement between the Governor of the CBSL and the ST on matters of macroeconomic significance. On key economic policy issues, both institutions maintain regular communication and coordination to ensure consistency and coherence in decision making. The CBSL and MoF also work collaboratively in external engagements, including investor interactions, credit rating-related discussions, and communications with international stakeholders, presenting a unified and credible policy narrative. In addition, the CBSL engages constructively, on various matters where coordination is required, with other line ministries and public sector institutions, reflecting a holistic approach to economic policy coordination. Importantly, during periods of heightened domestic or global uncertainty, such as US Tariff policy change, extreme weather-related disruptions caused by Cyclone Ditrwah and evolving geopolitical tensions in the Middle East, well-coordinated policy engagement between the Government and the Central Bank at the highest level was evident to assess risks and implement timely policy responses, thereby safeguarding macroeconomic stability and supporting economic resilience.

7. Close Coordination between the Government and CBSL

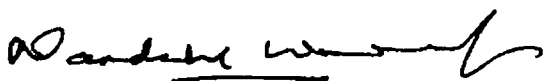
Importantly, as per the provisions of CBA, under the Flexible Inflation Targeting (FIT) framework, the inflation target is determined jointly by the Government and the Central Bank following a thorough assessment, with a high degree of coordination between the authorities. Furthermore, while the CBA places restrictions on direct monetary financing, it provides for limited provisional advances to the Government to manage short-term cash flow requirements at the beginning of the fiscal year. However, with improved fiscal discipline and performance, the Government has not invoked this provision since the enactment of the CBA in 2023. In addition to the

above, provisions exist to enable monetary financing under exceptional circumstances such as global health emergency, subject to the approval of Parliament.

In conclusion, a well-structured and efficiently coordinated fiscal-monetary framework is firmly in place while strong and meaningful coordination between fiscal and monetary authorities has been effective since the enactment of the CBA while respecting each other's scope and independence, enabling the authorities not only to manage adverse shocks but also to maintain macroeconomic stability, enhance the country's overall economic resilience, and foster sustainable and inclusive economic growth.

We hope the matters intended to be discussed at the meeting scheduled for 07 April 2026 on "A policy-level discussion with the officials of the Ministry of Finance, Planning and Economic Development (MoF) and the CBSL to address concerns regarding coordination between fiscal and monetary authorities" are adequately addressed through the provision of above information. Further, matters relating to policy are decided with the approval of the Members of the Cabinet as necessary and once approved such policies are anyway presented to the COPF as per the relevant provisions for applicable deliberations. Accordingly, given several well-functioning mechanisms in already place to ensure effective & timely coordination, we are of the view that there are no such concerns regarding coordination requiring deliberation at this juncture.

Yours sincerely,



**Dr. P Nandalal Weerasinghe**  
Governor and the Chairman of  
the Governing Board  
and the Monetary Policy Board  
Central Bank of Sri Lanka



**Dr. Harshana Suriyapperuma**  
Secretary to the Treasury  
Ministry of Finance, Planning  
and Economic Development

*Cc: Secretary General of Parliament*