பத்தாவது பாராளுமன்றம் - முதலாவது கூட்டத்தொடர்

அவுஸ்திரேலியாவுக்கான 2.5 மில்லியன் அமெரிக்க டொலர் கடனை மீளச் செலுத்துகையில் இணையவழிக் குற்றத்துடன் தொடர்புடைய மோசடி

தொடர்பான

அரசாங்க நிதி பற்றிய குழுவின் அறிக்கை

குழுவின் தவிசாளர் கௌரவ (கலாநிதி) ஹர்ஷ த சில்வா அவர்களால்
2026 ஜூலை 10 ஆம் திகதி வெள்ளிக்கிழமை
பாராளுமன்றத்தில் சமர்ப்பிக்கப்பட்டது.

குழுவின் உறுப்பினர்கள்

கௌரவ (கலாநிதி) ஹர்ஷ த சில்வா, பா.உ., (தவிசாளர்)

கௌரவ சதுரங்க அபேசிங்ஹ, பா.உ.,

கௌரவ (கலாநிதி) (செல்வி) கௌஷல்யா ஆரியரத்ன, பா.உ.,

கௌரவ அர்கம் இல்யாஸ், பா.உ.,

கௌரவ நிசாந்த ஜயவீர, பா.உ.,

கௌரவ சட்டத்தரணி ரஊப் ஹகீம், பா.உ.,

கௌரவ ரவி கருணாநாயக்க, பா.உ.,

கௌரவ ஹர்ஷன ராஜகருணா, பா.உ.,

கௌரவ சாணக்கியன் ராஜபுத்திரன் இராசமாணிக்கம், பா.உ.,

கௌரவ அஜித் அகலகட, பா.உ.,

கௌரவ எம்.கே. எம். அஸ்லம், பா.உ.,

கௌரவ நிமல் பலிஹேன, பா.உ.,

கௌரவ சட்டத்தரணி சித்ரால் பெர்னாந்து, பா.உ.,

கௌரவ விஜேசிரி பஸ்நாயக்க, பா.உ.,

கௌரவ சுனில் றாஜபக்ஷ, பா.உ.,

கௌரவ திலிண சமரகோன், பா.உ.,

கௌரவ சம்பிக ஹெட்டிஆரச்சி, பா.உ.,

கௌரவ (செல்வி) சட்டத்தரணி லக்மாலி ஹேமசந்திர, பா.உ.,

1. நிறைவேற்றுச் சுருக்கம்

சைபர் குற்றத்துடன் தொடர்புடைய ஒரு மோசடி காரணமாக 2025 நவம்பர் முதல் 2026 சனவரி வரையான காலப்பகுதியில் 'எக்ஸ்போர்ட் பைனான்ஸ் அவுஸ்திரேலியா' (Export Finance Australia) நிறுவனத்திற்கு செலுத்த வேண்டிய சில கொடுப்பனவுகளில், திறைசேரிக்கு ஐ.அ.டொ 2.5 மில்லியன் இழப்பு ஏற்பட்டுள்ளது. இது வெளிநாட்டுக் கடன் வழங்குநருக்கு செலுத்த வேண்டிய நிலுவைத் தொகையையும் ஏற்படுத்தியது. நிலையியற் கட்டளை 121 இன் கீழ், பொதுப் படுகடன் சேவை மீதான தனது கண்காணிப்புப் பணிகளுக்கு இணங்க, அரசாங்க நிதி பற்றிய குழு (COPF) இந்த விடயம் தொடர்பாக விசாரித்தது. இந்தச் சம்பவங்களின் தொடர் பற்றி பல அதிகாரிகளுடன் கலந்துரையாடுவதற்கும், சம்பந்தப்பட்ட நிறுவனங்களிடமிருந்து விரிவான அறிக்கைகளைப் பெறுவதற்கும் இக்குழு நான்கு சந்தர்ப்பங்களில் கூடியது. இந்த உரையாடல்கள் மற்றும் ஆவணங்கள் மூலம் குழுவிற்கு வழங்கப்பட்ட தகவல்களின் அடிப்படையில், COPF இனால் கண்டறியப்பட்டவாறு, சைபர் குற்றத்துடன் தொடர்புடைய இந்த மோசடிக்கு பங்களித்த நிகழ்வுகள் மற்றும் காரணிகளை இந்த அறிக்கை முன்வைக்கிறது.

கடன் திருப்பிச் செலுத்தும் செயல்பாட்டில் உள்ள உள்ளகக் கட்டுப்பாடுகளில் காணப்பட்ட முறைமை சார்ந்த குறைபாடுகள் மற்றும் காலாவதியான மின்னஞ்சல் உள்கட்டமைப்பு ஆகியவற்றின் காரணமாகவே சைபர் குற்றத்துடன் தொடர்புடைய மோசடி இடர் நேர்வுகள் அதிகரித்துள்ளதாக குழு முடிவு செய்கிறது. இது ஒரு தனிமைப்படுத்தப்பட்ட குறைபாடு அல்ல, மாறாக பல நிறுவனங்களில் காணப்பட்ட நிர்வாக, நடைமுறை மற்றும் செயல்பாட்டுத் தவறுகைகளின் விளைவாக ஏற்பட்டுள்ளது.

புதிதாக நிறுவப்பட்ட பொதுப் படுகடன் முகாமைத்துவ அலுவலகத்திற்கு (PDMO) கடன் திருப்பிச் செலுத்தும் பணிகளை மாற்றுவதற்கான செயல்முறையை வழிநடாத்துவதற்கான ஒரு நிகழ்வுக்கு முன்னரான விசாரணை நியதிகள் ஆவணத்தின் (ex-ante terms of reference document) இல்லாநிலையானது, நடைமுறை மற்றும் செயல்பாட்டு இடைவெளிகளை மோசமாக்கிய ஒரு முக்கிய நிர்வாகக் குறைபாடாகும். நடைமுறை மட்டத்தில், மூத்த அதிகாரிகளிடம் பயனுள்ள உள்ளகக் கட்டுப்பாடுகள் மற்றும் வலுவான தகவல் தொழில்நுட்ப முறைமைகளின் இல்லாநிலை, அத்துடன் பிரச்சினைகளைத் தீர்ப்பதற்கான போதிய தீவிரப்படுத்துதல் நடைமுறைகள் (escalation procedures) இல்லாமை போன்ற கடமை தவறிய தன்மைகள் அவதானிக்கப்பட்டன. செயல்பாட்டு மட்டத்தில், நடுத்தர நிலை அதிகாரிகள் அலட்சியமாக இருந்ததுடன், சரியான முறையில் முடிவெடுக்கத் தவறியுள்ளனர். வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தும் செயல்முறையில் நடைமுறைக் குறைபாடுகள் வரலாற்று ரீதியாக இருந்துவந்துள்ளதைக் குழு அவதானித்தது.

இந்த முடிவுகளின் அடிப்படையில், பொது நிதி நிர்வாகத்தில் இத்தகைய பாரதூரமான தவறுகைகள் மீண்டும் ஏற்படுவதைத் தடுப்பதற்கான முக்கியமான நடவடிக்கைகளாக குழு பல முக்கிய விதப்புரைகளை வழங்குகிறது. தேசிய கணக்காய்வு அலுவலகத்தால்

ஒட்டுமொத்த வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தும் செயல்முறையின் உடனடி விசேட கணக்காய்வின் தேவை; டிஜிட்டல் பொருளாதார அமைச்சினால் அரச துறை தகவல் தொழில்நுட்ப அமைப்புகளில் இலங்கை கணினி அவசர தயார்நிலை குழுவின் (SL-CERT) விதப்புரைகளை செயல்படுத்துவதை உறுதி செய்வதற்கான அவசர நடவடிக்கை; மற்றும் நிதி அமைச்சினால் அரசாங்க நிதிச் செயல்முறைகளை வழிநடாத்தும் நிதிப் பிரமாணங்களை உடனடியாக மறுசீரமைத்தல் ஆகியவை இவற்றில் அடங்கும்.

இந்த அறிக்கையின் உள்ளடக்கங்கள், அரசாங்க நிதி மீதான கண்காணிப்பின் அடிப்படையில் COPF இன் ஆணை வரம்பிற்கு உட்பட்டதாக உள்ளன. COPF இன் ஆணை குற்றவியல் விசாரணைகளோ அல்லது சட்டப் பொறுப்பு பற்றி தீர்ப்பு வழங்குவதையோ உள்ளடக்காது.

2. அறிமுகம்

இலங்கை பாராளுமன்றத்தின் நிலையியற் கட்டளை 121இன் பிரகாரம், நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு (நிதி அமைச்சு/MoF) மற்றும் ஏனைய சம்பந்தப்பட்ட அரச நிறுவனங்கள், நிறுவப்பட்ட சட்டக் கட்டமைப்புகள் மற்றும் வருடாந்த ஒதுக்கீட்டுச் சட்டம் ஆகியவற்றுக்கிணங்க, தொடர்புடைய சட்ட ஏற்பாடுகள், நிதிப் பிரமாணங்கள் மற்றும் செயல்முறைகளையும் பின்பற்றுகின்றனவா என்பதை உறுதிப்படுத்தி, அரசாங்க நிதியின் எந்தவொரு அம்சத்தையும் ஆராய்வதே அரசாங்க நிதி பற்றிய குழுவின் (COPF) ஆணையாகும். அரசாங்க நிதியின் மீதான கண்காணிப்பின் போது COPF இன் வகிபாகம் கடன் முகாமைத்துவம் மற்றும் கடன் சேவைகள் ஆகியவற்றை உள்ளடக்குகிறது. ஆகவே, காணாமல் போன ஐ.அ.டொ. 2.5 மில்லியன் வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தல் தொடர்பான பிரச்சினை இக்குழுவின் நோக்கெல்லைக்குள் வருகிறது. COPF இன் ஆணை குற்றவியல் விசாரணைகளோ அல்லது சட்டப் பொறுப்பு பற்றி தீர்ப்பு வழங்குவதையோ உள்ளடக்காது.

2026 ஏப்பிறல் 30 ஆம் திகதிய குழுவின் கலந்துரையாடலையும் 2026 மே 8 ஆம் திகதி பாராளுமன்றத்தில் சமர்ப்பிக்கப்பட்ட COPF இன் பூர்வாங்க அறிக்கையையும் தொடர்ந்து,[1] COPF வழங்கிய அறிவுறுத்தல்களுக்கு பதிலிறுத்தும் வகையில், நிதி அமைச்சு (MoF) 2026 ஜூன் தொடக்கத்தில் சைபர் குற்றத்துடன் தொடர்புடைய மோசடி பற்றிய விரிவான அறிக்கை ஒன்றை வழங்கியது.[2] அந்த அறிக்கை, குறித்த மோசடியைக் கண்டறியப்படுவதற்கு இட்டுச் சென்ற நிகழ்வுகளையும், அதுவரை மேற்கொள்ளப்பட்ட

---

[1] *பின்னிணைப்பு 1* – ஐ.அ.டொ. 2.5 *மில்லியன் மோசடியான வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தல் கொடுக்கல் வாங்கல் மீதான 2026 மே: 08 ஆம் திகதிய அரசாங்க நிதி பற்றிய* குழுவின் அறிக்கை

[2] *பின்னிணைப்பு 2* – சுமார் ஐ.அ.டொ. 2.5 மில்லியன் மதிப்புள்ள வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தல் கொடுக்கல் வாங்கல்கள் நிகழ்ந்ததாகக் கூறப்படும் மோசடி மீதான 2026 ஜூன் 01 ஆம் திகதிய நிதி அமைச்சின் அறிக்கை – பின்ணிணைப்புகளைத் தவிர.

நடவடிக்கைகளையும் உள்ளடக்கியிருந்தது. உரிய ஆவணங்கள் மற்றும் மின்னஞ்சல் பரிமாற்றங்களைக் கொண்ட இணைப்புகளும் அதனுடன் இணைக்கப்பட்டிருந்தன.

2026 ஜூன் 8 ஆம் திகதி நிதி அமைச்சின் (MoF) அறிக்கை பற்றி கலந்துரையாடும் போது, இலங்கை மத்திய வங்கியின் (CBSL) ஆளுநர், MoF அறிக்கையில் குறிப்பிடப்பட்டிருந்த சில விடயங்களை எதிர்த்ததுடன், மத்திய வங்கியின் அறிக்கை ஒன்றைச் சமர்ப்பிப்பதற்குகான காலத்தை வழங்குமாறும் வேண்டிக்கொண்டார். குறிப்பாக, *நிதிசார் கொடுக்கல் வாங்கல்களை* அறிக்கையிடல் சட்டத்தின் கீழ் பணத்தூய்தாக்கல் தடுப்பு பற்றிய சர்ச்சைகள் தொடர்பாக கடன் திருப்பிச் செலுத்தும் செயல்முறையின் பொருத்தமான நடைமுறைகள் மற்றும் பொறுப்புகள் தொடர்பாக நிதி அமைச்சிற்கு (MoF) ஆலோசனை வழங்கவில்லை என்று மத்திய வங்கி மீது குற்றம் சாட்டப்பட்டதே இந்த கலந்துரையாடலில் முக்கிய எழுப்பட்ட விடயமாகும். இந்த கலந்துரையாடலின் விளைவாக, பின்வரும் அறிக்கைகள் COPF குழுவிடம் சமர்ப்பிக்கப்பட்டன:

- இரண்டு CBSL அறிக்கைகள்: குறித்த நிகழ்வுகள்[3] தொடர்பாக மத்திய வங்கியின் கண்ணோட்டம் பற்றிய ஓர் அறிக்கையும், மற்றும் நிதி அமைச்சின் அறிக்கைக்குக் குறிப்பான பதில்களை வழங்கும் இன்னுமோர் அறிக்கையும்[4] உரிய ஆவணங்கள் மற்றும் மின்னஞ்சல் பரிமாற்றங்கள் அடங்கிய விரிவான இணைப்புகளுடன் சமர்ப்பிக்கப்பட்டன.
- தற்போதைய தேசிய சைபர் பாதுகாப்பு அடிக்கோடு நிறுவப்பட்ட 2023 ஆம் ஆண்டிலிருந்து, அரச நிறுவனங்களுக்கான தற்போதைய சைபர் பாதுகாப்பு கொள்கை மற்றும் அதன் மதிப்பீடும் மற்றும் நிதி அமைச்சின் தகவல் தொழில்நுட்ப முறைகளின் கணக்காய்வு ஆகியவற்றை விவரிக்கும் இலங்கை கணினி அவசர தயார்நிலை குழுவின் (SL-CERT) பதிலிறுத்தல். [5]
- இலங்கை மத்திய வங்கிக்கான *நிதிசார் கொடுக்கல் வாங்கல்களை* அறிக்கையிடல் சட்டத்தின் பிரயோகம் மற்றும் கடன் முகாமைத்துவம் மீதான அதன் இடைக்காலப் பொறுப்பு தொடர்பாக இலங்கை மத்திய வங்கிச் சட்டத்தின் 132 வது பிரிவின்

---

[3] *பின்னிணைப்பு 3 –* அரசாங்க நிதி பற்றிய குழுவிற்கு இலங்கை மத்திய வங்கி வழங்கிய பூரணமான அறிக்கை - திகதி: 2026 ஜூன் 15 – பின்னிணைப்புகளைத் தவிர.

[4] *பின்னிணைப்பு 4 -* சுமார் ஐ.அ.டொ. 2.5 மில்லியன் மதிப்புள்ள வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தல் கொடுக்கல் வாங்கல்கள் நிகழ்ந்ததாகக் கூறப்படும் மோசடி மீதான நிதி அமைச்சின் அறிக்கைக்குப் பதிலளிக்கும் வகையில் இலங்கை மத்திய வங்கி வழங்கிய அறிக்கை – திகதி: 2026 ஜூன் 15 – பின்னிணைப்புகளைத் தவிர.

[5] *பின்னிணைப்பு 5 -* SL-CERT இலிருந்து அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட 2026 ஜூன் 09 ஆம் திகதிய கடிதம், - சைபர் பாதுகாப்பு அறிக்கைகளைச் சமர்ப்பித்தல் மற்றும் வெளிநாட்டு வளங்கள் திணைக்களத்தின் மின்னஞ்சல் சேவையகத்தின் நிலை பற்றியத விளக்கம் - பின்னிணைப்புகளைத் தவிர.

பிரயோகம் தொடர்பாக சட்டத்துறை தலைமையதிபதி திணைக்களத்தின் பொருள்கோடல்.[6]

சம்பந்தப்பட்ட நிறுவனங்களால் வழங்கப்பட்ட ஆவணங்களை ஒப்பிட்டு மதிப்பீடு செய்து இந்தச் சமர்ப்பிப்புகள் 2026 ஜூன் 23 ஆம் திகதி கலந்துரையாடப்பட்டது. 2025 டிசெம்பர் 31 ஆம் திகதி மத்திய வங்கியின் (CBSL) பொதுப் படுகடன் திணைக்களம் மூடப்படுவதற்கு முன்னரும், 2026 மே 22 ஆம் திகதி வெளியிடப்பட்ட வர்த்தமானி மூலம் பொதுப் படுகடன் நிர்வாகத்தில் மத்திய வங்கியின் வகிபாகம் உத்தியோகபூர்வமாக முடிவுக்குக் கொண்டு வரப்படும் வரையிலும், மத்திய வங்கிச் சட்டத்தின் பிரிவு 132 எவ்வாறு பிரயோகிக்கப்பட்டது என்பது பற்றி சட்டத்துறை தலைமையதிபதியிடமிருந்து மேலதிக விளக்கம் இக்கூட்டத்தின் போது கோரப்பட்டது.[7]

இந்த அறிக்கை மேலே குறிப்பிடப்பட்ட அனைத்து அறிக்கைகளையும், நான்கு நிறுவனங்களின் பதில்களையும் மற்றும் 2026 ஏப்பிறல் 30, ஜூன் 08 மற்றும் ஜூன் 23 ஆகிய திகதிகளில் COPF இல் நடாத்தப்பட்ட கலந்துரையாடல்களையும் உள்ளடக்கியுள்ளது. இந்த அறிக்கை மேலும் ஐந்து பிரிவுகளாகக் கட்டமைக்கப்பட்டுள்ளது: சைபர் குற்றத்துடன் தொடர்புடைய மோசடி நிகழ்ந்த நிறுவனச் சூழமைவு பற்றிய சுருக்கம்; சம்பந்தப்பட்ட நிகழ்வுகள் மற்றும் சைபர் குற்றத்துடன் தொடர்புடைய மோசடி கண்டறியப்பட்டது பற்றிய ஒரு பூரணமான சுருக்கம்; சில அம்சங்கள் மற்றும் நிகழ்வுகள் தொடர்பாக CBSL மற்றும் நிதி அமைச்சிற்கு (MoF) இடையிலான கருத்து வேறுபாடுகள்; அதனைத் தொடர்ந்து குழுவின் முடிவுகள் மற்றும் விதப்புரைகள். இந்த அறிக்கையின் உள்ளடக்கங்களும் முடிவுகளும் குழுவிற்கு வழங்கப்பட்ட தகவல்களுக்கு மட்டுமே மட்டுப்படுத்தப்பட்டவை என்பதை கவனத்தில் கொள்வது அவசியமாகும்.

3. பின்னணி

சைபர் குற்றத்துடன் தொடர்புடைய மோசடி நிகழ்ந்த காலப்பகுதியானது (நவம்பர் 2025 முதல் 2026 மார்ச்சில் அது கண்டறியப்பட்டும் வரை), 2022 ஆம் ஆண்டு ஏப்பிறல் இருதரப்பு மற்றும் வர்த்தகக் கடன் வழங்குநர்களுக்கான கடன் கொடுப்பனவுகள் ஒருதலைப்பட்சமாக இடைநிறுத்தப்பட்டதன் பின்னர், அவர்களுடனான உடன்படிக்கையின் அடிப்படையில் வெளிநாட்டுக் கடன் மறுசீரமைப்பு செயல்முறையின் இறுதி நிலைகளுடனும், பொதுப் படுகடன் முகாமைத்துவ அலுவலகத்திற்கு கடன் முகாமைத்துவப் பொறுப்புகளை மாற்றும் நிறுவன மாற்றத்தின் இறுதிப் பகுதிக்கு இணையாக உள்ளது. கடன் மறுசீரமைப்பு நியதிகள் தொடர்பாக 2024 ஆம் ஆண்டின் நடுப்பகுதியில் இருதரப்புக் கடன் வழங்குநர்களுடன்

---

[6] *பின்னிணைப்பு 7* – சட்டத்துறை தலைமையதிபதி திணைக்களத்திலிருந்து அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம், திகதி: 2026 ஜூன் 15

[7] *பின்னிணைப்பு 8* - சட்டத்துறை தலைமையதிபதி திணைக்களத்திலிருந்து அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம், திகதி: 2026 ஜூன் 25

கையொப்பமிடப்பட்ட புரிந்துணர்வு ஒப்பந்தங்களின் அடிப்படையில், நிதி அமைச்சு 2025 ஆம் ஆண்டின் பிற்பகுதி வரை கூட திருத்தப்பட்ட கடன் ஒப்பந்தங்களை முடிவாக்கும் பணியில் ஈடுபட்டிருந்தது.

2024 ஜூன் மாதத்தில் 2024 ஆம் ஆண்டின் 33 ஆம் இலக்க பொதுக்கடன் முகாமைத்துவச் சட்டம் இயற்றப்பட்டதைத் தொடர்ந்து, பொதுப் படுகடன் நிர்வாகத்தை பொதுப் படுகடன் முகாமைத்துவ அலுவலகத்திற்கு மாற்றும் நிறுவன நிலைமாற்று 2024 நவம்பரில் தொடங்கப்பட்டது. 18 மாத இடைக்கால நிலைமாறு காலத்துடன் இது 2026 மே வரை நீடித்தது. மத்திய வங்கியின் பொதுப் படுகடன் திணைக்களம், நிதி அமைச்சின் வெளிநாட்டு வளங்கள் திணைக்களம் மற்றும் நிதி அமைச்சின் அரச தொழில்முயற்சிகள் திணைக்களம் ஆகியவற்றுக்கு இடையில் பகிர்ந்தளிக்கப்பட்டிருந்த பொறுப்புகளை ஒருமுகப்படுத்துவதை இச் செயற்பாடு உள்ளடக்கியிருந்தது.

ஒட்டுமொத்த நிலைமாற்றச் செயல்முறையானது கடன் முகாமைத்துவத்தின் பல அம்சங்களை உள்ளடக்கியிருந்த போதிலும், வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தல் செயல்முறை நிலைமாற்றத்தின் மீது மாத்திரமே இந்த அறிக்கை கவனம் செலுத்துகிறது. இங்கு பரிசீலிக்கப்படும் சைபர் குற்றத்துடன் தொடர்புடைய மோசடி இந்தச் செயல்முறைக்குள்ளேயே நிகழ்ந்துள்ளது.

3.1. பொதுப் படுகடன் முகாமைத்துவ அலுவலகம் உருவாக்கப்படுவதற்கு முன்னரான வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தும் செயல்முறை

பொதுப் படுகடன் முகாமைத்துவ அலுவலகத்திற்குப் பொறுப்புகள் மாற்றப்படுவதற்கு முன்னர், இருதரப்பு மற்றும் பலதரப்புக் கடன் திருப்பிச் செலுத்தல்களைக் கையாள்வதற்கான செயல்முறை பின்வருமாறு அமைந்திருந்தது:

I. வெளிநாட்டு வளங்கள் திணைக்களம் கடன் வழங்குநர்களிடமிருந்து கடன் மீள் செலுத்தலுக்கான கொடுப்பனவு பட்டியல்களை பெற்றது; அவற்றை அதன் கடன் முகாமைத்துவ பிரிவு செயலாக்கம் செய்து, சரிபார்த்து, அனுமதி அளித்தது.

II. அனுமதிக்கப்பட்ட கொடுப்பனவு பட்டியல்கள் மத்திய வங்கியின் பொதுப் படுகடன் திணைக்களத்திற்கு அனுப்பப்பட்டன. அத்திணைக்களம், கொடுப்பனவு பட்டியலில் உள்ள சரிபார்க்கப்பட்ட கட்டண விவரங்களை 'தரப்படுத்தப்பட்ட கொடுப்பனவு அறிவுறுத்தல்களாக (SSIs)' ஒதுக்க சாரா முகாமைத்துவ' (NRM) முறைமையில் உள்ளிட்டது.

III. ஒவ்வொரு SSI இலும் தேவையான கொடுப்பனவு விவரங்கள் உள்ளனவா என்பதை மத்திய வங்கியின் நிதித் திணைக்களம் சரிபார்த்தது.

IV. சரிபார்க்கப்பட்ட விவரங்களைப் பயன்படுத்தி, மத்திய வங்கியின் கொடுப்பனவு மற்றும் தீர்ப்பனவுத் திணைக்களம் , திறைசேரியின் திரட்டு நிதியின் ஒரு பகுதியாக மத்திய வங்கியில் பராமரிக்கப்படும் திறைசேரி பிரதிச் செயலாளர் கணக்கில் உள்ள வெளிநாட்டு நாணயத்தைப் பயன்படுத்தி, பயனாளி கணக்கிற்கு SWIFT பரிவர்த்தனையை மேற்கொண்டது.

பொதுப் படுகடன் முகாமைத்துவ அலுவலகம் உருவாக்கப்படுவதற்கு முன்னரான வெளிநாட்டுக் கடன் திருப்பிச் செலுத்தும் செயற்பாடு

மூலம் - இருதரப்பு / பலதரப்புக் கடன் வழங்குநர்

கடன் திருப்பிச் செலுத்துவதற்கான கொடுப்பனவு பட்டியலை வழங்குகிறது.

↓

கடன் மீள் செலுத்தல் கொடுப்பனவு பட்டியல்

↓

கட்டம் 1 வெளிநாட்டு வளங்கள் திணைக்களம் - கடன் முகாமைத்துவப் பிரிவு

கடன் மீள் செலுத்தலுக்கான கொடுப்பனவு பட்டியல்களை பெறுகிறது - செயலாக்கம் செய்கிறது - சரிபார்க்கிறது - அனுமதி அளிக்கிறது.

↓

அனுமதிக்கப்பட்ட கடன் கொடுப்பனவு பட்டியல்

படி II இலங்கை மத்திய வங்கி (CBSL) - பொதுப் படுகடன் திணைக்களம் (PDD)
அங்கீகரிக்கப்பட்ட கொடுப்பனவு பட்டியல் விபரங்களைப் பயன்படுத்தி, தரப்படுத்தப்பட்ட தீர்வு வழிமுறைகள் (SSI) ஊடாக NRM முறைமைக்குள் கொடுப்பனவு விபரங்களை உள்ளீடு செய்தல்; NRM, SWIFT-இணக்கமான வழிமுறைகளை உருவாக்குகிறது.

SSI விபரங்களை சரிபார்த்தல் (SII for verification)

படி III இலங்கை மத்திய வங்கி (CBSL) - நிதித் திணைக்களம்
SSI இல் அனைத்துக் கொடுப்பனவுத் தகவல்களும் உள்ளடங்கியுள்ளனவா என்பதைச் சரிபார்க்கிறது.

சரிபார்க்கப்பட்ட கொடுப்பனவு விபரங்கள்

படி IV இலங்கை மத்திய வங்கி (CBSL) - கொடுப்பனவுகள் திணைக்களம்
CBSL இல் உள்ள திறைசேரிப் பிரதிச் செயலாளர் (DST) கணக்கில் உள்ள வெளிநாட்டு நாணயத்தை - திறைசேரியின் திரட்டு நிதியிலிருந்து பயன்படுத்தி - SWIFT கொடுக்கல்வாங்கலை மேற்கொள்ளுதல்

கடன் வழங்குநரின் கணக்கிற்கு SWIFT கொடுப்பனவு

3.2. PDMO இற்கான 18-மாத மாற்றற் காலம்

2024 நவம்பர் முதல் 2026 மே மாதம் வரையிலான 18-மாத **மாற்றற்** காலகட்டத்தில், பல திணைக்களங்களுக்கிடையில் பரவியிருந்த படுகடன் வழங்கல் மற்றும் முகாமைத்துவத் தொழிற்பாடுகளை PDMO ஏற்றுக்கொண்டு மையப்படுத்த வேண்டியிருந்தது.

இருப்பினும், பல நிறுவனங்களை உள்ளடக்கிய இந்த சிக்கலான, பன்முகத்தன்மை வாய்ந்த மாற்ற செயல்முறைக்கு விரிவான வழிகாட்டுதலையோ அல்லது செயல்பாட்டு விதிகளையோ (Terms of references) வழங்கும் எந்த ஆவணத்தையும் குழு பெற்றுக்கொள்ளவில்லை. இந்த மாற்றம் போதுமான முறையில் நிறைவடைந்ததா என்பதை மதிப்பிடுவதற்கு எந்த KPI களும் கிடைக்கவில்லை. PDMO வின் செயல்பாடுகளை

நிர்வகிக்கும் வழிகாட்டுதல்கள் கூட, அந்த அலுவலகம் நிறுவப்பட்டு 10 மாதங்களுக்குப் பிறகு, 2025 செப்டம்பர் 19 திகதி அன்றுதான் வெளியிடப்பட்டன. CBSL மற்றும் PDMO இக்கு இடையேயான ஒத்துழைப்புத் துறைகள் குறித்த புரிந்துணர்வு ஒப்பந்தம் (MoU), உத்தியோகபூர்வ மாற்றற் காலம் முடிவடையும் தருவாயில், 2026 மார்ச் 09 திகதி அன்றுதான் கைச்சாத்திடப்பட்டது.

18 மாத கால மாற்றத்தின் காலவரிசை

2024 நவம்பர் 24		**PDMO இனை நிறுவுதல்** 18 மாத மாற்றற் காலம் தொடங்குதல்
2025 ஜனவரி 1		**ERD கடன் பிரிவை PDMO உடன் இணைத்தல்** வெளிப்புறக் கடன் முகாமைத்துவம் மையப்படுத்துதல்
2025 மார்ச்-டிசம்பர்		**CBSL இனால் PDMO அதிகாரிகள் பயிற்சி அளிக்கப்படல்** அனைத்துப் படுகடன் முகாமைத் தொழிற்பாடுகளுக்குமான திறன் விருத்தி
2025 ஒக்டோபர் 13-15		**உள்ளகத் தொழிற்பாடுகள் PDMO விடம் ஒப்படைக்கப்படுதல்** திறைசேரி ஏலங்கள் (ஒக்டோபர் 13). படுகடன் மீளச்செலுத்தல் (ஒக்டோபர் 15)
2025 அக்டோபர் 13-24		**வெளிப்புறப் படுகடன்: முறைமை அணுகல் வழங்கப்படுதல்** NRM கொடுப்பனவு அறிவுறுத்தல்கள் (ஒக்டோபர் 13) SSI உருவாக்கம் (ஒக்டோபர் 24)
2025 அக்டோபர் 30		**உள்நாட்டு வெளியீட்டுக் கையகப்படுத்தல் டிசம்பர் மாதத்திற்கு ஒத்திவைக்கப்பட்டல்** முதன்மை விநியோகஸ்தர்களுக்கான ஒழுங்குமுறைத் தேவைகள் தாமதமடைதல்
2025 டிசம்பர்		**உள்நாட்டு வெளியீடு PDMO இக்கு மாறுகிறது** நிதி அமைச்சின் கீழ் உள்ள PDD வளாகம் (முதல் வாரம்) PDMO வளாகம் (இரண்டாம் வாரம்)
2025 டிசம்பர் 31		**PDD உத்தியோகபூர்வமாக மூடப்படுகிறது** 2026 ஜனவரி 01 ஆம் திகதி உத்தியோகபூர்வமாக நிறைவு விழா
2026 மார்ச் 9		**PDMO மற்றும் CBSL இடையேயான புரிந்துணர்வு ஒப்பந்தம் (MoU) கைச்சாத்திடப்படுகிறது**

		தொடர்ச்சியானதாக இருக்கும் ஒத்துழைப்புக்கான கட்டமைப்பு
2026 மே 22		**CBSL இன் இடைக்காலப் பதவி முறைப்படி முடிவடைகிறது** 18 மாத கால இடைக்காலம் முடிவடைகிறது. வர்த்தமானி வெளியிடப்படுகிறது.

மாற்றத்தின் தொடக்கத்தில், பொதுநலவாய செயலக படுகடன் பதிவு மற்றும் முகாமைத்துவ முறைமையைக் (CS-DRMS) கையாண்டு வந்த வெளி வளங்கள் திணைக்களத்தின் (ERD) படுகடன் முகாமைத்துவ பிரிவு, அதனுடன் இணைந்த பணியாளர்களுடன் 2024 டிசம்பர் PDMO இற்கு மாற்றப்பட்டது. அவர்கள் 2025 ஜனவரி 01 ஆம் திகதி தங்கள் கடமைகளைப் பொறுப்பேற்றனர்.

இந்த மாற்றத்தின் போது, கடன் ஒப்பந்தங்கள் மற்றும் கொடுப்பனவுகளைச் சரிபார்த்துப் பதிவுசெய்யும் பணியை PDMO பின்தள அலுவலகம் (Back office) மேற்கொண்டது. இதன் பொருள், முன்னர் ERD இன் பொறுப்பாக இருந்த கொடுப்பனவு பட்டியல்களைப் சரிபார்த்தல் மற்றும் கொடுப்பனவுகளுக்கு அங்கீகாரம் அளித்தல் ஆகியவற்றுக்கு இப்போது PDMO பொறுப்பேற்றது என்பதாகும்.

இருப்பினும், வெளிநாட்டுக் கடன் வழங்குநர்களுடன் ஒருங்கிணைப்பதில் தனக்கிருந்த பாரம்பரியப் பங்கின் காரணமாக (legacy role), கடன் வழங்குநர்களிடமிருந்து வரும் கொடுப்பனவு பட்டியல்களில் பெரும் பகுதியை ERD தொடர்ந்து மின்னணுத் தொடர்பு வழியாகவே பெற்று வந்ததுடன் அவை செயலாக்கத்திற்காக PDMO இன் பின்தள அலுவலகத்திற்கு அனுப்பப்பட்டன.
PDD-CBSL ஐ கையாளும் படுகடன் முகாமைத்துவத் தொழிற்பாடுகளை மேற்கொள்வதைப் பொறுத்தவரையில், PDMO பணியாட்டொகுதியினருக்கு 2025 மார்ச் மற்றும் டிசம்பர் மாதங்களுக்கிடையில் மூன்று தொகுதிகளாக PDD பணியாட்டொகுதியினர்களால் பயிற்சி அளிக்கப்பட்டது. வெளிநாட்டுக் படுகடன் திருப்பிச் செலுத்தும் செயல்முறையில் SSI களை உருவாக்குவது உள்ளிட்ட இருப்பு அல்லாத முகாமைத்துவ முறைமையின் (Non -Reserve Management System) செயல்பாடுகளும் இதில் உள்ளடக்கப்பட்டிருந்தன.

2025 செப்டம்பர் 23 ஆம் திகதி நிதி அமைச்சுக்கும் இலங்கை மத்திய வங்கிக்கும் இடையில் நடைபெற்ற ஒருங்கிணைப்புப் பேரவைக் கூட்டத்திலும், 2025 செப்டம்பர் 25 திகதியிடப்பட்ட ST இன் CBSL இக்கு அனுப்பப்பட்ட கடிதத்தின் மூலமாகவும், PDMO இனால் PDD இன் தொழிற்பாடுகளைக் கையகப்படுத்துவதற்கான காலக்கெடு உறுதி

செய்யப்பட்டது. இந்த அறிக்கையில் பரிசீலனையில் உள்ள பிரச்சினை தொடர்பான விடயங்கள் பின்வருமாறு:

i. உள்நாட்டுத் திறைசேரிப் பத்திரங்கள் வெளியீட்டு ஏலங்கள் PDD ஆல் தொடர்ந்து மேற்கொள்ளப்படும், ஆனால் 2025 ஒக்டோபர் 13 ஆம் திகதி முதல் CBSL ஒப்புதல் செயல்முறையின் கீழ் PDMO அதிகாரிகளால் கையாளப்பட்டு வந்தன.

II. உள்நாட்டுக் கடன் சேவை 15 அக்டோபர் 2025 அன்று PDMO-க்கு மாற்றப்படும்.

III. வெளிநாட்டுப் படுகடன் மீளளிப்பு தொடர்பாக, PDMO அதிகாரிகளுக்கு உள்நுழைவுச் சான்றுகள் (login credentials) உருவாக்கப்பட்டன. இதன்மூலம், ஒக்டோபர் 13 ஆம் திகதி முதல் பணம் செலுத்தும் அறிவுறுத்தல்களை வழங்கவும், ஒக்டோபர் 24 ஆம் திகதி முதல் SSI களை உருவாக்கவும் NRM அமைப்பை அணுக அவர்களுக்கு அனுமதி வழங்கப்பட்டது.

இந்த மாற்றத்தின் மூலம், கடன் வழங்குநர்களின் கொடுப்பனவு பட்டியல்கள் மற்றும் பணம் செலுத்தும் விபரங்களைச் சரிபார்த்து அங்கீகரிக்கும் பொறுப்பு PDMO விடம் ஒப்படைக்கப்பட்டது; இதற்கு முன்னர் இப்பணியை ERD செய்து வந்தது. மேலும், NRM அமைப்பில் SSI ஆக பணம் செலுத்தும் அறிவுறுத்தல்களை உள்ளிடும் அமைப்பாகவும் இது மாறியது; இதற்கு முன்னர் இந்தப் பணியை PDD-CBSL செய்து வந்தது. CBSL இன் நிதித் திணைக்களம் SSI இல் தேவையான பணம் செலுத்தும் விபரங்களைத் தொடர்ந்து சரிபார்த்து வந்தது. CBSL இன் கொடுப்பனவுகள் மற்றும் தீர்வுகள் திணைக்களம், கொடுப்பனவுகளைத் தொடர்ந்து செயல்படுத்தி வந்தது.

2025 டிசம்பர் மாதத்தில் இப்பணிகள் PDMO விடம் ஒப்படைக்கப்பட்டதால், PDD-CBSL இடம் வேறு எந்தப் பணிகளும் மீதமிருக்கவில்லை. இதன் விளைவாக, PDD ஆனது 2025 டிசம்பர் 31 ஆம் திகதி முதல் மூடப்பட்டது. மேலும், நிதி அமைச்சின் மூத்த அதிகாரிகள் முன்னிலையில் 2026 ஜனவரி 01 ஆம் திகதி ஒரு முறையான மூடும் விழா நடைபெற்றது.

வன்பொருள் மற்றும் மென்பொருளைப் பொறுத்தவரை, PDD ஆல் முன்பு பயன்படுத்தப்பட்ட முறைமைகள் PDMO ஆலும் தொடர்ந்து பயன்படுத்தப்படுகின்றன. குறிப்பாக, NRM முறைமை மற்றும் அரசாங்கப் பத்திரங்கள் ஏல அமைப்பு (GSAS) ஆகியவை முறையே வெளிநாட்டுப் படுகடன் திருப்பிச் செலுத்துதல் மற்றும் உள்நாட்டுக் படுகடன் வழங்கல் முகாமைத்துவ செயன்முறை ஆகியவற்றின் ஒரு பகுதியாகத் தொடர்ந்து இருந்து வருகின்றன. 2026 மார்ச் 09 திகதியிடப்பட்ட புரிந்துணர்வு ஒப்பந்தம், 2025 டிசம்பர் முதல் 2 ஆண்டுகளுக்கு GSAS அணுகல் வழங்கப்படும் என்றும், அதனுடன் NRM முறைமை மற்றும் படுகடன் முகாமைத்துவத்துக்கு அவசியமான தரவுத்தளங்கள் மற்றும்

கருவிகள் போன்ற பிற அமைப்புகளுக்கான தொடர்ச்சியான அணுகலும் வழங்கப்படும் என்றும் குறிப்பிடுகிறது. GSAS பயன்பாட்டில் இருக்கும் வரை, CBSL இன் பேரிடர் மீட்புத் தளம் மற்றும் வங்கியியல் ஆய்வுகளுக்கான மையம் ஆகியவையும் PDMO அதிகாரிகளுக்குக் கிடைக்கச் செய்யப்பட்டன.

PDMO விற்கு மாறியதைத் தொடர்ந்து வெளிநாட்டுக் படுகடன் திருப்பிச் செலுத்தும் செயல்முறை

மூலம் - இருதரப்பு / பலதரப்பு கடன் வழங்குநர்
படுகடன் திருப்பிச் செலுத்துவதற்கான கொடுப்பனவு பட்டியலை வழங்குகிறது

கொடுப்பனவு பட்டியல்

படி I வெளி வளங்கள் திணைக்களம்
கடன் வழங்குநரிடமிருந்து கொடுப்பனவு பட்டியலை பெற்று, அதை PDMO பின்தள அலுவலகத்திற்கு அனுப்புகிறது.

விலைப்பட்டியல் அனுப்பப்பட்டது

படி II பொதுப் படுகடன் முகாமைத்துவ அலுவலகம் - PDMO பின்தள அலுவலகம்
விலைப்பட்டியலைச் செயலாக்கி, சரிபார்த்து, அங்கீகரிக்கிறது; தரப்படுத்தப்பட்ட தீர்வு வழிமுறைகள் (SSI) வழியாக NRM முறைமையில் SWIFT இணக்கமான அறிவுறுத்தல்களை உருவாக்கி பணம் செலுத்தும் விபரங்களை உள்ளிடுதல்

SSI விபரங்களை சரிபார்த்தல் (SII for verification)

படி III இலங்கை மத்திய வங்கி (CBSL) - நிதித் திணைக்களம்
SSI இல் தேவையான அனைத்துக் கொடுப்பனவுத் தகவல்களும் அடங்கியுள்ளனவா என்பதைச் சரிபார்க்கிறது.

சரிபார்க்கப்பட்ட கொடுப்பனவு விபரங்கள்

அரசாங்க நிதி பற்றிய குழுவின் அறிக்கை

படிநிலை IV: இலங்கை மத்திய வங்கி (சிபீஎஸ்எல்) - கொடுப்பனவுகள் மற்றும் தீர்ப்பனவுத் திணைக்களம்

இலங்கை மத்திய வங்கியில் உள்ள திறைசேரியின் பிரதிச் செயலாளர் கணக்கில் உள்ள வெளிநாட்டு நாணயத்தைப் பயன்படுத்தி சுவிஃப்ட் (SWIFT) பரிவர்த்தனை செயல்படுத்துகிறது — இதற்கான நிதி திறைசேரியின் ஒருங்கிணைந்த நிதியத்திலிருந்து பெறப்படுகிறது.

↓

கடனளிப்பவரின் கணக்கிற்கு சுவிஃப்ட் கொடுப்பனவு

3.3. நிதி அமைச்சின் தகவல் தொழில்நுட்பம் மற்றும் இணையப் பாதுகாப்பு உட்கட்டமைப்பு

நிதி அமைச்சு அர்ப்பணிப்புள்ள தகவல் தொழில்நுட்ப முகாமைத்துவத் திணைக்களம் ஒன்றைக் கொண்டுள்ளதுடன் இந்தத் திணைக்களத்திற்கு அமைச்சின் தகவல் தொழில்நுட்ப முறைமைகள் தொடர்பான முகாமை ஒப்படைக்கப்பட்டுள்ளது. எவ்வாறாயினும், இந்தத் திணைக்களம் treasury.gov.lk என்ற இணைய டொமைனைப் பயன்படுத்தும் 17 திணைக்களங்களின் தகவல் தொழில்நுட்ப முறைமைகளுக்கு மாத்திரமே பொறுப்பாகும். வெளிநாட்டு வளங்கள் திணைக்களம் (ஈஆர்டி), எவ்வாறாயினும், அதன் பணிப்பாளரின் கீழ் பணிபுரியும் அதற்கு உரித்தான தகவல் தொழில்நுட்ப அலுவலர்களுடன் erd.gov.lk என்ற டொமைனுடன், கிட்டத்தட்ட 2000 ஆம் ஆண்டிலிருந்து, தனியான தகவல் தொழில்நுட்ப முறைமையைக் கொண்டுள்ளது. இந்த இரண்டு தகவல் தொழில்நுட்பக் குழுக்களுக்கு இடையே ஒருங்கிணைப்பு இருந்ததாகத் தெரியவில்லை. இது ஆளுகை மற்றும் நடைமுறையில் காணப்படுகின்ற மிகக் கவலைக்குரிய சீர்குலைவு ஒன்றாகும்.

வெளிநாட்டு வளங்கள் திணைக்களத்தின் முறைமைகள் தனியான முறைமை ஒன்றாக பேணப்பட்டுக்கொண்டிருந்த போதிலும், தகவல் தொழில்நுட்ப முகாமைத்துவத் திணைக்களத்தின் பணிப்பாளர் நாயகம் அதன் மீதான மேற்பார்வையை மேற்கொண்டிருப்பார் என எதிர்பார்க்கப்படுகிறது. பொதுப் படுகடன் முகாமைத்துவ அலுவலகத்தின் (பிடிஎம்ஓ) பணிப்பாளர் நாயகத்தின் கூற்றிற்கு அமைவாக, இந்த அலுவலகம் தாபிக்கப்பட்டபோது, திணைக்களத்தின் மின்னஞ்சல்கள் மற்றும் ஏனைய பணிகளுக்கான தேவையான பரிமாறி இடவசதி, வெளிநாட்டு வளங்கள் திணைக்களத்தின் முறைமைகளில் இருந்தே பெறப்பட்டது. பிடிஎம்ஓ இன் முறைமையினைப் பராமரிப்பதற்காக, அதன் தகவல் தொழில்நுட்ப அலுவலர் ஈஆர்டி, இல் இருந்து தற்காலிகமாக இணைக்கப்பட்டார். 2026 ஜூன் 23 ஆம் திகதி வரை, பிடிஎம்ஓ தனக்குச் சொந்தமான பரிமாறிகளைப் பெறுவதற்கு அதற்கான கொள்முதல் செயன்முறை தொடர்ந்தும் இடம்பெற்றுக்கொண்டிருந்தது.

இங்குள்ள மிகப் பாரதூரமான பிரச்சினை என்னவெனில், ஈஆர்டி காலாவதியான மைக்ரோசொஃப்ட் எக்ஸ்சேஞ்ச் பரிமாறி 2016 இனைப் பயன்படுத்தி இருந்தது. இலங்கை கணினி அவசர தயார்நிலைக் குழுவின் கூற்றிற்கு அமைவாக, இந்தப் பரிமாறிக்கான மைக்ரோசொஃப்ட்டின் வழக்கமான முழுமையான தொழில்நுட்ப ஆதரவு 2020 ஒக்டோபரில் நிறைவடைந்தது, ஆயினும்,

2025 ஒக்டோபர் 14 வரை நீடிக்கப்பட்ட ஆதரவின் கீழ் மைக்ரோசொஃப்ட்டிடம் இருந்து சிறிய பாதுகாப்பு இற்றைப்படுத்தல்களை அது தொடர்ந்து பெற்றது. விற்பனையாளரால் வழங்கப்பட்ட தொழில்நுட்ப ஆதரவை நீடிப்பதற்கு நடவடிக்கை எடுக்கப்பட்டிருந்த அதேவேளை, இற்றைப்படுத்தப்பட்ட முறைமை ஒன்று கொள்முதல் செய்யப்படவில்லை. இது ஈஆர்டி மற்றும் பிடிஎம்ஒ ஆகியவற்றின் தகவல் தொழில்நுட்ப முறைமைகள் இணையவழித் தாக்குதல்களுக்கு முழுமையாக உள்ளாகும் அபாயத்திற்கு இட்டுச்சென்றது. அதன்காரணமாக, பிரச்சினைக்குரிய இணையவழி குற்றச்செயற்பாட்டுடன் தொடர்புடைய மோசடி, மைக்ரோசொஃப்ட் பாதுகாப்பு இற்றைப்படுத்தல்கள் பெறுவது நிறுத்தப்பட்டு ஒரு மாதத்திற்கும் குறைவான காலத்திற்குள் 2025 நவம்பர் மாதத்தில் தொடங்கியது.

வெளிநாட்டு வளங்கள் திணைக்களம் உள்ளிட்ட, நிதி அமைச்சிலுள்ள தகவல் தொழில்நுட்ப உட்கட்டமைப்பு மற்றும் இணையப் பாதுகாப்பு நடவடிக்கைகளில் காணப்பட்ட முறைமையான குறைபாடுகளின் தன்மை, 2024 டிசம்பரில் ‘கேபிஎம்ஜீ இனால் இலங்கை கணினி அவசர தயார்நிலைக் குழுவுடன் இணைந்து மேற்கொள்ளப்பட்ட விரிவான கணக்காய்வு ஒன்றின் மூலம் வெளிப்படுத்தப்பட்டது. பல நிலை அடையாளச் சரிபார்ப்புப் (Multifactor authentication) போன்ற சாதாரண பாதுகாப்பு நடவடிக்கைகள் கூட அங்கு நடைமுறையில் இருக்கவில்லை என்பதுடன், பலவீனமான கடவுச்சொற்கள் பயன்படுத்தப்பட்டு வந்தன எனவும் சுட்டிக்காட்டப்பட்டது. ஊழியர்களுக்கு மத்தியில் தெளிவற்ற வகிபாகங்கள் மற்றும் பொறுப்புகள் காரணமாக, வகைபொறுப்புக்கூறலில் இருந்து தவறுதல் செயற்பாட்டுச் செயல்திறன் குறைபாடுகள் ஆகியன அடையாளம் காணப்பட்டன. 2026 ஜனவரி மற்றும் ஏப்ரல் மாதங்களில் இலங்கை கணினி அவசர தயார்நிலைக் குழு மற்றும் தேசிய இணையப் பாதுகாப்பு செயற்பாட்டு நிலையம் ஆகியவற்றினால் மேற்கொள்ளப்பட்ட மீளாய்வுகளிலும், இந்தத் தகவல் தொழில்நுட்ப முறைமைகளில் தொடர்ந்தும் நீடித்துவரும் பாதிப்படையக்கூடிய தன்மைகள் சுட்டிக்காட்டப்பட்டிருந்தன.

துரதிர்ஷ்டவசமாக, இலங்கை கணினி அவசர தயார்நிலைக் குழுவின் எச்சரிக்கைகள் மற்றும் விதப்புரைகளை சம்பந்தப்பட்ட நிறுவனங்கள் கடைப்பிடிப்பதை உறுதி செய்வதற்கான அதிகாரம் அதற்கு இருப்பதாகத் தெரியவில்லை. அவசியமான நடவடிக்கைகளை மேற்கொள்ளும் பொறுப்பு சம்பந்தப்பட்ட நிறுவனங்களின் மீதே உள்ளது.

4. நிகழ்வுகள் தொடர்பான காலவரிசை

இந்தப் பிரிவு பிரதான நிகழ்வுகள் மற்றும் ஆவணங்களின் சாரம்சத்தை வழங்குகிறது. அரசாங்கக் கணக்குகள் பற்றிய குழுவிடம் சமர்ப்பிக்கப்பட்ட ஆவணங்களை அடிப்படையாகக் கொண்டு, இணையக் குற்றத்துடன் தொடர்புடைய மோசடி எவ்வாறு நிகழ்ந்தது என்பதை இது விபரிக்கிறது. இந்தப் பிரிவின் நோக்கம் இந்தத் தொடர் சம்பவங்கள் எவ்வாறு இடம்பெற்றன என்பதை நன்றாகப் புரிந்துகொள்வதற்கு, உள்ளக கட்டுப்பாட்டுச் சூழலை மீளாய்வு செய்வதாகும்.

4.1. இந்தியாவிற்கான மீள்கொடுப்பனவுகள் தொடர்பான பிரச்சினை ஒன்று பற்றிக் கண்டறிதல்

விசாரணையின் கீழ் உள்ள இணையத்தளம்சார் குற்றத்துடன் இணைந்த மோசடி, எக்ஸ்போட்

பினான்ஸ் அவுஸ்திரேலியவக்கான கொடுப்பனவு ஒன்று தொடர்பானது என்றபோதிலும், நிதி அமைச்சு தனது முதலாவது இணையப் பாதுகாப்பு அச்சுறுத்தலை, 2026 ஜனவரியில் இந்தியாவின் ஏற்றுமதி-இறக்குமதி (எக்சிம்) வங்கிக்கு மேற்கொள்ளப்படவிருந்த கடன் மீளச்செலுத்தல் ஒன்றின் போது கண்டறிந்தது.

2026 ஜனவரி 6 ஆம் திகதி, இந்தியாவின் எக்சிம் வங்கிக்கு மேற்கொள்ளப்பட்டிருந்த கொடுப்பனவு ஒன்று செலுத்தப்படவில்லை.[8] இடைத்தரகராக ஜேபிமோகனைக் கொண்டு பிடிஎம்ஓ இனால் வழங்கப்பட்ட கணக்கு விபரங்களுக்கு இலங்கை மத்திய வங்கி அந்தக் கட்டணத்தை செலுத்த முயற்சித்தபோது, ஜேபிமோகனின் உலகளாவிய மோசடித் தடுப்புச் செயற்பாட்டு அணியினால் அந்தக் கொடுப்பனவு நிராகரிக்கப்பட்டது. பிடிஎம்ஓ அதிகாரிகளால் இந்திய எக்சிம் வங்கி அணியுடன் தொடர்பு மேற்கொள்ளப்பட்டது. இதன் மூலம் மோசடியான கட்டண அறிவுறுத்தல்கள் வழங்கப்பட்டிருந்தது என உறுதிப்படுத்துவதற்கு நிதி அமைச்சிற்கு சாத்தியமானது.

பின்னர் இந்தியாவின் எக்சிம் வங்கியுடனான தொடர்பாடல் மூலம் சரிபார்க்கப்பட்டு, சரியான கணக்கிற்கு கட்டணம் செலுத்தப்பட்டது. இந்த சந்தேகத்திற்கிடமான நடவடிக்கை 2026 ஜனவரி 9 ஆம் திகதி குற்றப் புலனாய்வுத் திணைக்களம் மற்றும் இலங்கை கணினி அவசர தயார்நிலைக் குழு ஆகியவற்றுக்கு அறிவிக்கப்பட்டது. சந்தேகிக்கப்படும் மோசடி மின்னஞ்சல் முகவரி eximbenkindia.in என்ற டொமைனைப் பயன்படுத்தியதாக இலங்கை கணினி அவசர தயார்நிலைக் குழுவிற்கு ஈஆர்டி தகவல் தொழில்நுட்ப அலுவலர் வழங்கிய முறைப்பாட்டில் குறிப்பிடப்பட்டிருந்தது (இருப்பினும் சரியான டொமைன் eximbankindia.in எனக் காணப்படுகிறது).

4.2. அவுஸ்திரேலியாவிற்கு மீளச்செலுத்தப்படாமை தொடர்பாக கண்டறியப்படுதல்

இந்திய எக்சிம் வங்கி சம்பந்தப்பட்ட சம்பவத்தைத் தொடர்ந்து, இணையப் பாதுகாப்பு அச்சுறுத்தலின் அபாயம் திறைசேரியின் செயலாளருக்குக் கொண்டு செல்லப்பட்டதுடன், இந்த நிலைமையை விசாரிப்பதற்கு ஈஆர்டி இன் பணிப்பாளர் நாயகத்திடம் ஒப்படைக்கப்பட்டது. நிறுவன மறுசீரமைப்பு செயன்முறைகள் பூர்த்தியடைந்ததன் பின்னர் சமர்ப்பிக்கப்பட்ட கொடுப்பனவு பட்டியல்களை அடிப்படையாகக் கொண்டு, கடந்த காலங்களில் மேற்கொள்ளப்பட்ட கொடுப்பனவுகளை உன்னிப்பாக ஆராய்வதற்கு ஈஆர்டி நடவடிக்கை எடுத்தது. ஐக்கிய இராச்சியம் (1,294,605.99அமெரிக்க டொலர்கள்), ஜெர்மனி (4,059,987.81 யூரோக்கள்) மற்றும் பெல்ஜியம் (60,974.88 யூரோக்கள்) ஆகிய நாடுகளுக்கான கொடுப்பனவுகள் உட்பட, மின்னஞ்சல் மூலம் பெறப்பட்ட பல ஏனைய கொடுப்பனவுகளுக்கான கட்டண அறிவுறுத்தல்கள் மோசடியானவையாக மேலும் அடையாளம் காணப்பட்டன.

சந்தேகத்திற்குரியதாகக் குறியிடப்பட்ட கொடுப்பனவு பட்டியல்களின் செல்லுபடித்தன்மையை உறுதிப்படுத்துவதற்காக, 2026 ஜனவரி முதல் மார்ச் வரை இந்த மூன்று கடன் வழங்குநர்களுடனும் பின்தொடர் நடவடிக்கைகள் மேற்கொள்ளப்பட்டன. இதன் விளைவாக, ஐக்கிய இராச்சியத்திற்கான சம்பந்தபப்பட்ட கொடுப்பனவு உடனடியாக இடைநிறுத்தப்பட்டது. சந்தேகத்திற்கிடமான தரப்பினரால் ஆரம்பிக்கப்பட்ட தொடர்பாடல்கள் அடையாளம் காணப்பட்டதுடன், விசாரணை அதிகாரிகளின் கவனத்திற்கு கொண்டுவரப்பட்டது. பெல்ஜியம் தொடர்பான கொடுப்பனவு சரியான கணக்கிற்கு வைப்புச்செய்யப்பட்டது.

---

8 இக் கொடுப்பனவானது *2025* ஆம் ஆண்டில் மறுசீரமைக்கப்பட்ட கடன்களுக்கான வட்டி செலுத்துவதற்காக மேற்கொள்ளப்பட்டதாகும்.

இந்த சரிபார்ப்புச் செயன்முறையின் போது, முன்னைய மாதங்களில் செலுத்தப்பட வேண்டிய கடன் மீளச்செலுத்தல்கள் கிடைக்கப் பெறவில்லை என எக்ஸ்போர்ட் பினான்ஸ்

அவுஸ்திரேலியாவிடமிருந்து வந்த தொடர்பாடல்கள் குறித்து, 2026 மார்ச் 23 ஆம் திகதி நிதி அமைச்சு அதிகாரிகளின் கவனத்திற்கு கொண்டுவரப்பட்டது.

4.3. இணையத்தளம்சார் குற்றத்துடன் தொடர்புடைய மோசடி சம்பந்தப்பட்ட மின்னஞ்சல் பரிமாற்ற தொடர்களின் சாரம்சம்

ஈஆர்டி அதிகாரிகள் (உண்மையான மற்றும் ஆள்மாறாட்டம் செய்யப்பட்டவர்கள்), எக்ஸ்போர்ட் பினான்ஸ் அவுஸ்திரேலியாவின் அதிகாரிகள் (உண்மையான மற்றும் ஆள்மாறாட்டம் செய்யப்பட்டவர்கள்), மற்றும் இந்தச் செயன்முறையில் சம்பந்தப்பட்ட ஏனைய இலங்கை நிறுவனங்களின் அதிகாரிகளுக்கு இடையேயான மின்னஞ்சல்களின் பரிமாற்ற தொடர்கள், இணையத்தளம்சார் குற்றத்துடன் தொடர்புபட்ட இந்த மோசடியின் செயன்முறை மற்றும் காலவரிசையை புரிந்துகொள்ள முடிவதற்கான மிகத் தெளிவான வழிமுறையாக காணப்படுகிறது. நிதி அமைச்சு மற்றும் இலங்கை மத்திய வங்கி ஆகியவற்றால் அரசாங்க நிதி பற்றிய குழுவிற்கு வழங்கப்பட்ட மின்னஞ்சல் பரிமாற்ற தொடர்களை அடிப்படையாகக் கொண்டு, விளக்கப்பட சாரம்சம் ஒன்று இந்தப் பிரிவில் வழங்கப்படுகிறது. மின்னஞ்சல் முகவரிகளில் இருந்து தனியாட்களின் பெயர்களை நீக்கி, டொமைன்களை மாத்திரம் மாற்றமின்றி வைக்கப்பட்ட வகையில், அநாமதேயமாக்கப்பட்ட மூன்று தனித்தனி மின்னஞ்சல் பரிமாற்ற தொடர்களின் மீது கவனம் செலுத்தப்படுகிறது.

மின்னஞ்சல் பரிமாற்ற தொடர் 1 - 2025 ஒக்டோபர் 28 முதல் 2026 ஜனவரி 15 வரையிலான காலப்பகுதியில், ஈஆர்டி மற்றும் கடன் வழங்குநரின் எனக் கருதப்படும் மின்னஞ்சல் முகவரிகளுக்கு இடையே இடம்பெற்றது.

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

2025 அக்டோபர் 28

ஒப்பமிடப்பட்ட மறுசீரமைக்கப்பட்ட கடன் ஒப்பந்தங்களின் ஸ்கேன் செய்யப்பட்ட பிரதிகள் அனுப்பப்பட்டன

அவுஸ்திரேலியாவுடனான கடன் மறுசீரமைப்பு 2025 ஒக்டோபர் 27 ஆம் திகதி நிறைவடைந்ததுடன், 2025 ஒக்டோபர் 28 ஆம் திகதி பகிரங்கமாகவும் அறிவிக்கப்பட்டது. ஒப்பமிடப்பட்ட மூலப் பிரதிகளின் பிரதிகள் ஈஆர்டி இனால் பிடிடி மற்றும் பிடிஎம்ஒ ஆகியவற்றுக்கு அனுப்பப்பட்டன. எக்ஸ்போர்ட் பினான்ஸ் அவுஸ்திரேலியா மீளச்செலுத்தல்களுக்கான நடைமுறையிலிருக்கும் கணக்கு விபரங்கள் திருத்தப்பட்ட ஒப்பந்தத்தில் மாற்றப்பட்டிருக்கவில்லை என நிதி அமைச்சு அதிகாரிகள் குழுவில் தெரிவித்தனர்.

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

2025 நவம்பர் 13

கொடுப்பனவு செயன்முறைக்காக, அவுஸ்திரேலிய கடன் மறுசீரமைப்பு ஒப்பந்தத்தின் கீழ் ஆறு கொடுப்பனவு பட்டியல்கள் அனுப்பப்பட்டன.

இந்த மின்னஞ்சல், Z@exportfinance.gov.au என்ற முகவரிக்கு அனுப்பப்பட்ட முன்னைய மேலே குறிப்பிடப்பட்ட மின்னஞ்சலிற்கு அனுப்பப்பட்ட பதிலாகும்.

குறிப்பு: இந்த விலைப்பட்டியல்களுக்கான கொடுப்பனவுகள் 2025 நவம்பர் 14 ஆம் திகதி மேற்கொள்ளப்படுகிறது.

அந்த ஆறு கொடுப்பனவு பட்டியல்கள் பின்வருமாறு (மொத்தம் சுமார் 2,180,184 அமெரிக்க டொலர்களுக்காக):

I. 141,739.95 அவுஸ்திரேலிய டொலர்கள்: சட்டக் கட்டணங்கள்

II. 996,221.85 அமெரிக்க டொலர்கள்: அவுட்டோடெக் பரிவர்த்தனை மீதான வட்டி நிலுவை

III. 69,199.59 அமெரிக்க டொலர்கள்: வெல்லார்ட் 1 பரிவர்த்தனை மீதான வட்டி நிலுவை

IV. 340,126.84 அமெரிக்க டொலர்கள்: வெல்லார்ட் 2 பரிவர்த்தனை மீதான வட்டி நிலுவை

V. 304,432.45 அமெரிக்க டொலர்கள்: வெல்லார்ட் 3 பரிவர்த்தனை மீதான வட்டி நிலுவை

VI. 377,660.26 அமெரிக்க டொலர்கள்: ஆர். ஆர். டெய்லர் பரிவர்த்தனை மீதான வட்டி நிலுவை

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

2025 நவம்பர் 25

2025 நவம்பர் 24 ஆம் திகதி மேற்கொள்ளப்பட்ட 1,375,882.11 அமெரிக்க டொலர் (USD) கட்டணம், பயனாளி வங்கியால் (beneficiary bank) தெளிவான காரணம் எதுவும் வழங்கப்படாது, இலங்கை மத்திய வங்கிக்கு (உண்மையில், 1,375,459.74 அமெரிக்க டொலர் மாத்திரமே திருப்பி அனுப்பப்பட்டது) திருப்பி அனுப்பப்பட்டதாக அறிவிக்கப்படுகிறது.

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

2025 நவம்பர் 26

கட்டணம் ஏன் திருப்பி அனுப்பப்பட்டிருக்கக்கூடும் என்பதற்கான விரிவான காரணங்களை விளக்கியதுடன், திருத்தப்பட்டு சரிசெய்யப்பட்ட கொடுப்பனவு பட்டியல்களை அனுப்புவதற்கும் வாக்குறுதியளிக்கப்பட்டது.

இந்தக் கட்டணம் இரண்டு கொடுப்பனவுகளாகப் பிரிக்கப்பட்டதை இலங்கை மத்திய வங்கி அறிக்கை காட்டுகிறது. அதாவது அமெரிக்க வங்கிக் கணக்கிற்கு 377,660.26 அமெரிக்க டொலரும், ஐக்கிய அரபு அமீரக வங்கிக் கணக்கிற்கு 997,799.48 அமெரிக்க டொலரும் செலுத்தப்பட்டன. ஐக்கிய அரபு அமீரக கணக்கிற்கான இந்தக் கட்டணம், மின்னஞ்சல் பரிமாற்ற தொடர் 2 இல் இலங்கை மத்திய வங்கி நிதித் திணைக்கள அதிகாரிகளால் கேள்விக்கு உட்படுத்தப்பட்டது.

2025 நவம்பர் 28 ஆம் திகதி அமெரிக்க வங்கிக் கணக்கிற்கிற்கான திருத்தப்பட்ட கொடுப்பனவு பூரணப்படுத்தப்பட்ட அதேவேளை, 2025 டிசம்பர் 17 ஆம் திகதி ஐக்கிய அரபு அமீரகக் கணக்கிற்கான கொடுப்பனவு இடைநிலை வங்கியால் நிராகரிக்கப்பட்டது. அந்த நிதி 2026 ஜனவரி 13 ஆம் திகதி இலங்கை மத்திய வங்கிக்கு திருப்பி அனுப்பப்பட்டது.

5 A@erd.gov.lk - Z@exportfinanceau.com
2026 ஜனவரி 07
பி.டி.எம்.ஒ வினால் அனுப்பப்பட்ட மின்னஞ்சலுக்கமைவாக இலங்கை மத்திய வங்கிக்கு நிதி திருப்பி அனுப்பப்படவில்லையெனக் குறிப்பிடப்பட்டுள்ளது.

6. Z@exportfinanceau.com - A@erd.gov.lk
2026 ஜனவரி 14
இடைநிலை வங்கியிடமிருந்து திருப்பி அனுப்புமாறு கோரப்பட்ட கொடுப்பனவு பட்டியலுக்கு எதிரான கொடுப்பனவுக் குறித்து தொடர்ந்து நடவடிக்கை மேற்கொள்ளுமாறு கோரப்பட்டது. கொடுப்பனவு மேலும் தாமதிக்கப்பட்டால் மேலதிக வட்டி செயற்படுத்தப்படுவதற்கான சாத்தியம் இருப்பதாக குறிப்பிடப்பட்டுள்ளது.

7. A@erd.gov.lk - Z@exportfinanceau.com
2026 ஜனவரி 14
நிதி திருப்பி அனுப்பப்பட்டிருப்பதனை இலங்கை மத்திய வங்கி உறுதிசெய்திருப்பதாக குறிப்பிடப்பட்டுள்ளது. அது விகொடுப்பனவு பட்டியலை மீள வழங்குமாறு அறிவுறுத்தப்பட்டமைக்கு அமைவாக இருந்தது.

8. Z@exportfinanceau.com - A@erd.gov.lk
2026 ஜனவரி 15
திருத்தப்பட்ட கொடுப்பனவு பட்டியல்கள் அனுப்பப்பட்டன.

முன்னதாக மேற்கொள்ளப்பட்ட இரண்டு கொடுப்பனவு முயற்சிகளிலும் நிறைவேறாத 997,799.48 அமெரிக்க டொலர்கள் 2026 ஜனவரி 20 அன்று அமெரிக்க வங்கி கணக்கிற்கு வெற்றிகரமாகச் செலுத்தப்பட்டது.
இதேவேளை, எக்ஸ்போர்ட் பைனேன்ஸ் அவுஸ்திரேலியாவுக்கு 2026 ஜனவரியில் செலுத்தப்படாமல் இருந்த இரண்டாவது கட்ட மீளச் செலுத்துகை செயற்படுத்தப்பட்டு 2026 ஜனவரி 5 ஆம் திகதியன்று வெற்றிகரமாகச் செலுத்தப்பட்டது.

9. F@erd.gov.lk – Z@exportfinanceau.com
2025 டிசெம்பர் 22
2026 ஜனவரி 5 ஆம் திகதி செலுத்தப்பட வேண்டிய ஐந்து கொடுப்பனவு பட்டியல்கள் கோரப்பட்டன.

10 Z@exportfinanceau.com- F@erd.gov.lk
2025 டிசெம்பர் 23
ஐந்து இருதரப்பு உடன்படிக்கைகளுக்காக 2026 ஜனவரி 5 அன்று செலுத்தப்பட வேண்டிய வட்டிக் கொடுப்பனவுக்கான ஐந்து விலைப்பட்டியல்கள் அனுப்பப்பட்டன.

எக்ஸ்போர்ட் பைனேன்ஸ் அவுஸ்திரேலியாவுக்கு அனுப்பப்பட வேண்டிய பணம் திரும்ப அனுப்பப்பட்டதை தொடர்ந்து 2025 நவம்பர் 26 அன்று பி.டி.எம்.ஒ மற்றும் இலங்கை மத்திய வங்கி அதிகாரிகளுக்கிடையே இடம்பெற்ற மின்னஞ்சல் பரிமாற்றத் தொடர் 2.

1. **D@cbsl.lk** – நிதி திணைக்களத்தைச் சேர்ந்த ஊழியர் ஒருவரது மின்னஞ்சல் முகவரி (இலங்கை மத்திய வங்கி)

   2025 நவம்பர் 26

   ஐக்கிய அரசு இராச்சியத்திலுள்ள புதிய பயனாளிக்கான கொடுப்பனவு உள்ளிட்ட திருத்தப்பட்ட கடன் மீளச் செலுத்தல் அறிவுறுத்தல்கள் கடன் கொடுத்தவரிடமிருந்து கிடைக்கப்பெற்றிருப்பதாக குறிப்பிட்டு பி.டி.எம்.ஓ விடமிருந்து கிடைத்த மின்னஞ்சல் இலங்கை மத்திய வங்கியின் நிதி திணைக்களத்துக்கு அனுப்பி வைக்கப்பட்டது. இக்கொடுப்பனவைச் செலுத்த முடியுமா மற்றும் இடைநிலை வங்கித் தேவையா என்பது தொடர்பிலான அனுமதி மற்றும் அறிவுறுத்தலும் கோரப்பட்டிருந்தன.

2. நிதி திணைக்களத்தைச் சேர்ந்த ஊழியர் ஒருவரது மின்னஞ்சல் முகவரி (இலங்கை மத்திய வங்கி) - D@cbsl.lk

   2025 நவம்பர் 26

   பயன்பெறுநரின் முகவரியானது எக்ஸ்போர்ட் பைனேன்ஸ் அவுஸ்திரேலியாவின் முகவரியல்ல என்றும் இதனால் பயன்பெறுநரின் வங்கியினால் பண மோசடி தடுப்பு தொடர்பான சிக்கல்கள் உள்ளிட்ட மேலுமொரு நிராகரிப்பை இது ஏற்படுத்தக்கூடுமென்றும் குறிப்பிட்டு இலங்கை மத்திய வங்கியின் நிதி திணைக்களமானது மேற்படி மின்னஞ்சலுக்கு பதில் அனுப்பியது. மீளச் செலுத்துவதற்காக கணக்கு விவரங்களை மீள்உறுதி செய்வதற்கென கடன் வழங்குனருடன் தொடர்பை ஏற்படுத்துவதற்கான அறிவுறுத்தல்களை அவர்கள் வழங்கியிருந்தனர்.

3. **D@cbsl.lk** - **G@pdmo.gov.lk**

   2025 நவம்பர் 26

   ஐக்கிய அரசு இராச்சியத்தின் கணக்கிற்கு செலுத்தப்பட வேண்டிய கொடுப்பனவு பட்டியல் தொடர்பாக இலங்கை மத்திய வங்கியின் நிதி திணைக்களம் தமது அக்கறையை எழுப்பியிருப்பதாக இலங்கை மத்திய வங்கியின் பி.டி.டி பிரிவுக்குப் பொறுப்பான அதிகாரி பி.டி.எம்.ஓ விற்கு அறிவித்ததுடன் அது தொடர்பில் அவசியமான செயற்பாடுகளை முன்னெடுக்குமாறும் பி.டி.எம்.ஓ விற்கு அறிவித்தது.

2025 நவம்பர் 25 முதல் 2026 மார்ச் 23 வரையிலான காலப்பகுதியில் ஈ.ஆர்.டி மற்றும் கடன் கொடுத்தோரின் எனக் கருதப்படும் மின்னஞ்சல் முகவரிகளுக்கும் இடையில் இடம்பெற்ற மின்னஞ்சல் பரிமாற்றத் தொடர் 3

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

   2025 நவம்பர் 25

   தவறான பயனாளி காரணமாகவே நிதி திருப்பி அனுப்பப்பட்டது என விளக்கமளிக்கப்பட்டதுடன் புதுப்பிக்கப்பட்ட கொடுப்பனவு பட்டியல்களை ஈ.ஆர்.டியின் சம்பந்தப்பட்ட அதிகாரிக்கு அனுப்புமாறும் கேட்டுக்கொள்ளப்பட்டது.

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

   2025 நவம்பர் 26

   திருத்தப்பட்ட வங்கி விவரங்களுடன் திருத்தப்பட்ட கொடுப்பனவு பட்டியல்கள் அனுப்பப்பட்டன.

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

   2025 நவம்பர் 27

   வங்கி விவரங்கள் சரியாக பெற்றுக்கொள்ளப்பட்டன என்பது உறுதிசெய்யப்பட்டது.

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

   2025 டிசெம்பர் 3-16

   கொடுப்பனவு மேற்கொள்ளப்படும் என எதிர்பார்க்கப்படும் திகதியை கடன் கொடுத்தவர் கேட்டிருந்தார்.

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

   2025 டிசம்பர் 19

   அதற்கு பதிலளிக்கும் முகமாக கொடுப்பனவு ஜனவரி முதல் வாரமளவில் அனுப்பப்படுமென எதிர்பார்க்கப்படுவதாக ஈ.ஆர்.டி அலுவலகர் குறிப்பிட்டார். டிட்வா சூறாவளியின் விளைவாக ஏற்பட்ட பணியாளர் பற்றாக்குறையே (resource consultant) தாமதத்திற்கான காரணமென குறிப்பிடப்பட்டதுடன் இதற்கிடையே அனுப்பப்பட வேண்டிய இருதரப்பு உடன்படிக்கைகளுக்கு கீழான 2026 ஜனவரி 5 ஆம் திகதிக்குள் செலுத்தப்பட வேண்டிய அனைத்து கொடுப்பனவு பட்டியல்களும் கோரப்பட்டன.

6. Z@exportfinance.gov.au - B@erd.gov.lk

2025 டிசெம்பர் 23

2026 ஜனவரி 5 ஆம் திகதிக்குள் செலுத்தப்பட வேண்டிய ஐந்து கொடுப்பனவு பட்டியல்கள் அனுப்பப்பட்டன.

7. Z@exportfinance.gov.au - B@erd.gov.lk

2026 ஜனவரி 12-20

நிலுவையிலுள்ள கொடுப்பனவு பட்டியல்களின் கொடுப்பனவுகள் பற்றிய விவரங்களை, உரிய தினத்தில் செலுத்தப்படாது நிலுவையிலுள்ள கொடுப்பனவுகள் தொடர்பில் பணிப்பாளர்கள் சபையின் அதிக கவனத்துக்கு கொண்டு வர வேண்டியதன் அவசியத்தை வலியுறுத்தி ஜனவரி 20 ஆம் திகதி வழங்கப்பட்ட எச்சரிக்கையுடன் இணைந்த ஒரு தரவேற்றத்தை இக்காலப்பகுதிக்குரிய மின்னஞ்சல் கோரியிருந்தது.

8. B@erd.gov.lk – Z@exportfinance.gov.au

2026 ஜனவரி 20

எக்ஸ்போர்ட் பைனேன்ஸ் அவுஸ்திரேலியாவின் தாமதிக்கப்பட்ட கொடுப்பனவு தொடர்பில் அதனை எவ்வாறு செயற்படுத்துவது என்பது குறித்து பி.டி.எம்.ஒவும் அமைச்சரவையும் ஒரு தீர்மானத்தை எட்டுமென இதற்கு பதிலளிக்கும் வகையில் ஈ.ஆர்.டி அலுவலகர் உறுதிசெய்தார்.

9. A@erd.gov.lk – Z@exportfinance.gov.au

2026 பெப்ரவரி 02

உரிய தினத்தில் செலுத்தப்படாது நிலுவையிலுள்ள கொடுப்பனவுகளைச் செலுத்தி தீர்ப்பதற்காக அமைச்சரவையினால் அங்கீகரிக்கப்பட்டதாகக் கூறப்படும் காலவரையறையை வழங்கும் விபரமான மின்னஞ்சல். 2025 நவம்பர் 15 அன்று செலுத்தப்பட வேண்டிய 5 கொடுப்பனவு பட்டியல்கள் 2026 மார்ச் 16 அன்று செலுத்தப்பட வேண்டும். 2026 ஜனவரி 05 அன்று செலுத்தப்பட வேண்டிய 5 கொடுப்பனவு பட்டியல்கள் 2026 ஏப்ரல் 6 அன்று செலுத்தப்பட வேண்டும்.

10. Z@exportfinance.gov.au - A@erd.gov.lk

2026 பெப்ரவரி 16

மேற்படி கொடுப்பனவு அட்டவணை ஏற்றுக்கொள்ளப்பட்டது.

11. Z@exportfinance.gov.au -A@erd.gov.lk
2026 பெப்ரவரி 19
கொடுப்பனவுக்காக மீள் அட்டவணைப்படுத்தப்பட்ட மொத்த பெறுமதி உறுதி செய்யப்பட்டது.
2026 மார்ச் 16 அன்று செலுத்தப்பட வேண்டியது 2,089,640.99 அமெரிக்க டொலர்கள்.
2026 ஏப்ரல் 6 செலுத்தப்பட வேண்டியது 420,211.96 அமெரிக்க டொலர்கள்

12. B@erd.gov.lk - Z@exportfinance.gov.au
2026 மார்ச் 14 முதல் 16 வரை
நிதி வழங்கல் தொடர்பான விரிவான தகவலை வழங்க மார்ச் 20 ஆம் திகதி வெள்ளிக்கிழமை வரை அவகாசம் கேட்கப்பட்டிருப்பதுடன் கொடுப்பனவு நடவடிக்கைகள் செயற்படுத்தப்பட்டு வருவதாகவும் குறிப்பிடப்பட்டுள்ளது.

13. B@erd.gov.lk - Z@exportfinance.gov.au

15-16 மார்ச்
கொடுப்பனவு பற்றிய தகவல்கள் குறித்து கடன் கொடுநர் கோரிக்கைகளை தொடர்ந்தார்.

14. Z@exportfinance.gov.au -B@erd.gov.lk + A@erd.gov.lk
2026 மார்ச் 21
புதிய அட்டவணையின்படி மீளச் செலுத்தப்பட வேண்டிய தொகை கிடைக்காமை குறித்து குற்றச்சாட்டுக்கள் முன்வைக்கப்பட்டன.

15. A@erd.gov.lk – வேறுபட்ட ஈ.ஆர்.டி அலுவலகர்கள்
2026 மார்ச் 23
ஒரே தொடர்பு நபர் தொடர்பாக (same contact point) கடன் வழங்குனரின் தொடர்பு நபருடன் தொடர்புடைய மூன்று வெவ்வேறு மின்னஞ்சல் முகவரிகளில் இருந்து மின்னஞ்சல்கள் பெறப்பட்டுள்ளது அவதானிக்கப்பட்டது

இந்த இறுதி மின்னஞ்சலானது, அவுஸ்திரேலிய ஏற்றுமதி நிதியத்திற்கான கடன் மீளச் செலுத்துகைகளில் ஒரு பிரச்சினை உள்ளது என்பதை வெளிநாட்டு வளங்கள் திணைக்கள அதிகாரிகள் உணர்ந்துகொண்ட தருணமாகத் தோன்றுவதுடன், இதுவே அடுத்தடுத்த நடவடிக்கைகளுக்கும் விசாரணைகளுக்கும் வழிவகுத்துள்ளது.

2026 ஜனவரி 9 மற்றும் 2026 மார்ச் 7 ஆம் திகதிகளில் சந்தேகிக்கப்படும் இணையவழி குற்றங்கள் தொடர்பில் எழுதப்பட்ட முன்னைய கடிதங்களைக் குறிப்பிட்டு, காணாமல் போன கொடுப்பனவுகள் குறித்து மார்ச் 24 ஆம் திகதியன்று வெளிநாட்டு வளங்கள்

திணைக்களத்தின் பணிப்பாளர் நாயகம், இலங்கை கணினி அவசர தயார்நிலைக் குழுவிற்குக் கடிதம் எழுதினார். அத்துடன், நிதியியல் கொடுக்கல்வாங்கல் அறிக்கையிடல் சட்டத்தின் கீழ் இவ்விடயம் தொடர்பில் தகவல்களைக் கோரிய நிதியியல் உளவறிதல் பிரிவின் கோரிக்கைக்குப் பதிலளிக்கும் வகையில், 2026 ஏப்ரல் 3 ஆம் திகதி வெளிநாட்டு வளங்கள் திணைக்களத்தின் பணிப்பாளர் நாயகம் குறித்த பிரிவிற்கும் விவரங்களுடன் கடிதம் எழுதினார்.

2026 மார்ச் 24 ஆம் திகதி, "மின்னஞ்சல் ஊடாகப் பெறப்பட்ட மோசடியான கொடுப்பனவு அறிவுறுத்தல்களின் அபாயம் மற்றும் அவுஸ்திரேலியாவிற்குச் செய்யப்பட்ட காணாமற்போன கொடுப்பனவு" குறித்து விசாரணை செய்வதற்காக ஒரு தொழில்நுட்ப விசாரணைக் குழு நியமிக்கப்பட்டது. இக்குழுவில் திறைசேரியின் பிரதிச் செயலாளர் ஏ.என். ஹப்புகல, திறைசேரியின் பிரதிச் செயலாளர் எஸ்.எஸ். முதலிகே, தேசிய திட்டமிடல் திணைக்களத்தின் பணிப்பாளர் நாயகம் கே.ரி.ஐ. பிரேமரத்ன, சட்ட அலுவல்களுக்கான மேலதிக பணிப்பாளர் நாயகம் ஏ.கே.டீ.டீ.டீ. அரந்தர மற்றும் தகவல் தொழில்நுட்ப முகாமைத்துவத் திணைக்களத்தின் உதவிப் பணிப்பாளர் ஈ.டீ. சிரந்த ஆகியோர் உள்ளடங்கியிருந்தனர். அவர்கள் தமது அறிக்கையை 2026 ஏப்ரல் 10 ஆம் திகதி சமர்ப்பித்தனர். இந்த அறிக்கையின் கண்டறிதல்களின் அடிப்படையில், 2026 ஏப்ரல் 17 ஆம் திகதி நான்கு ஊழியர்கள் பணி இடைநிறுத்தம் செய்யப்பட்டனர்.

கவனத்திற் கொள்ள வேண்டிய ஒரு முக்கியமான விடயம் யாதெனில், தற்போதுள்ள 135 ஆம் இலக்க நிதி ஒழுங்குவிதிகளின் பிரகாரம், கடன் மீளச் செலுத்துகைகளின் பொறுப்புகள் தொடர்பில் நிதி அமைச்சினுள் முறையான அதிகாரப் பகிர்வு காணப்படவில்லை என அரசாங்க நிதிப் பற்றிய குழு கண்டறிந்துள்ளமையாகும்.

2026 ஏப்ரல் 30 ஆம் திகதி நடைபெற்ற கலந்துரையாடலினைத் தொடர்ந்து, இது தொடர்பாக அரசாங்க நிதி பற்றிய குழுவின் விசாரணைக்குப் பதிலளிக்கும் வகையில், திறைசேரியின் செயலாளர் 2026 ஜூன் 23 ஆம் திகதியிட்ட கடிதமொன்றில், கடன் மீளச் செலுத்தும் செயன்முறையானது ஒரு தற்றுணிபான செலவின விடயம் அல்ல என்பதால், வரலாற்று ரீதியாக அது தற்போதுள்ள நிதி ஒழுங்குவிதிகளுக்குள் அடங்கவில்லை எனப் பதிலளித்திருந்தார்.[9] நிதி அமைச்சினுள் இறுதி கொடுப்பனவுக்கான அங்கீகாரமானது, முன்னர் வெளிநாட்டு வளங்கள் திணைக்களத்திலும் தற்போது பொதுக் கடன் முகாமைத்துவ அலுவலகத்திலும் சிரேஷ்ட அதிகாரிகளின் எந்தவொரு சரிபார்த்தல் செயன்முறையும் இன்றி, கடன் சேவைச் செயற்பாட்டின் மீது அதிகாரம் கொண்ட பணிப்பாளரால் வரலாற்று ரீதியாக மேற்கொள்ளப்பட்டு வந்துள்ளமையானது, அங்குள்ள பலவீனமான உள்ளகக் கட்டுப்பாடுகளை எடுத்துக்காட்டுகிறது.

[9] *இணைப்பு 9 - 2026 யூன் 23 ஆந் திகதிய கடன் மறுசெலுத்துகைச் செயல்பாடுகளுக்கான அதிகாரப் பகிர்வு (delegation of authority)*

5. தொடர்ச்சியான சம்பவங்களைத் தொடர்ந்து செயன்முறைகளை மேம்படுத்துவதற்காக நிதி அமைச்சினால் எடுக்கப்பட்ட நடவடிக்கைகள்

நிதி அமைச்சின் அறிக்கையின்படி, இவ்வாறான சம்பவங்கள் மீண்டும் நிகழும் அபாயத்தைக் குறைப்பதற்கும் வெளிநாட்டுக் கடன் மீளச் செலுத்தும் செயன்முறையை மேம்படுத்துவதற்கும் தொடர்ச்சியான சம்பவங்களைத் தொடர்ந்து அமைச்சினால் பல நடவடிக்கைகள் எடுக்கப்பட்டன.[10] எடுக்கப்பட்ட முக்கிய நடவடிக்கைகளின் சுருக்கம் பின்வருமாறு:

- வெளிநாட்டு வளங்கள் திணைக்களத்திடமிருந்து கடன் சேவையளிப்புத் தொடர்பான வழங்குநர்களுடனான ஒருங்கிணைப்புச் செயற்பாட்டை பொதுக் கடன் முகாமைத்துவ அலுவலகம் முழுமையாகப் பொறுப்பேற்றல்.
- கடன் வழங்குநர்களால் சமர்ப்பிக்கப்படும் தகவல்கள் ஆகக்குறைந்தது இரண்டு வழிமுறைகளினூடாகப் பயனுறுதிமிக்க வகையில் சரிபார்க்கப்படுவதை உறுதிப்படுத்துவதற்காக, இராஜதந்திரத் தொடர்பாடல் வழிகள் உள்ளடங்கலாக, சம்பந்தப்பட்ட கடன் வழங்குநர்களுடன் முறையான தொடர்பாடல் வழிமுறைகளை ஏற்படுத்துதல்.
- முதலாவது கொடுப்பனவு மேற்கொள்ளப்படுவதற்கு ஆகக்குறைந்தது 10 நாட்களுக்கு முன்னர், மாதாந்தக் கடன் சேவை முன்னறிவிப்பானது கொடுப்பனவு அனுமதிக்காக திறைசேரியின் செயலாளருக்கு சமர்ப்பிக்கப்படுகின்றது.
- திறைசேரி தொழிற்பாடுகள் திணைக்களம் சரிபார்த்தல் செயன்முறைக்குள் முறையாகக் கொண்டுவரப்பட்டுள்ளதுடன், சரிபார்த்தல் செயன்முறையில் சரியான விவரங்கள் தெளிவாக உறுதிப்படுத்தப்பட்டால் மாத்திரமே அத்திணைக்களம் முகாமை செய்யும் திரட்டிய நிதிக் கணக்குகளிலிருந்து மாதாந்தக் கடன் மீளச் செலுத்துகைகளுக்கான ஒதுக்கீட்டினை அது அங்கீகாரம் வழங்குகின்றது.
- உரிய அங்கீகாரமும் சரிபார்ப்பும் இன்றி, நிறுவன வள திட்டமிடல் முறைமையில் ஏற்கெனவே பதிவுசெய்யப்பட்டுள்ள வங்கி விபரங்களை மாற்றிப் பதிவுசெய்வதற்குக் கட்டுப்பாடுகள் விதிக்கப்பட்டுள்ளன.
- நிதி அமைச்சின் ஒட்டுமொத்த இணையப் பாதுகாப்பினை வலுப்படுத்துவதற்கும், வெளிநாட்டு வளங்கள் திணைக்களத்தின் தகவல் தொழில்நுட்ப முறைமைகளில் அடையாளம் காணப்பட்ட குறைபாடுகளை நிவர்த்தி செய்வதற்கும் இலங்கை கணினி அவசரகால ஆயத்தக் குழு மற்றும் தேசிய சைபர் பாதுகாப்பு செயல்பாட்டு மையம் உள்ளிட்ட டிஜிட்டல் பொருளாதார அமைச்சின் உதவி பயன்படுத்தப்படுகின்றது.

---

[10] *அமைச்சினால் மேற்கொள்ளப்பட்ட நடவடிக்கைகளின் விரிவான விபரங்கள் இணைப்பு 2ல் வழங்கப்பட்டுள்ளன*

இந்நடவடிக்கைகள், நிதி அமைச்சினுள் உள்ளகக் கட்டுப்பாடுகளை ஏற்படுத்தி வலுப்படுத்துவதற்கும் அடிப்படை இணையவெளிப் பாதுகாப்பை உறுதிசெய்தல் ஆகியவற்றுடன் தொடர்புடையவையாகும்.

அவை ஓர் அடிப்படையாக ஏற்கனவே நடைமுறையில் இருந்திருக்க வேண்டும். இன்றியமையாத இவ்வடிப்படை நடவடிக்கைகளை நடைமுறைப்படுத்த வேண்டியதன் அத்தியாவசியத்தன்மையை அண்மைய சம்பவம் தெளிவாகப் புலப்படுத்தியுள்ளது.

6.வெளிநாட்டுக் கடன் மீளச் செலுத்தும் செயன்முறையினுள் இலங்கை மத்திய வங்கியின் பொறுப்புகள் தொடர்பில் இலங்கை மத்திய வங்கி மற்றும் நிதி அமைச்சின் வேறுபட்ட கருத்துகள்

வெளிநாட்டுக் கடன் மீளச் செலுத்தும் செயன்முறை மற்றும் பொதுக் கடன் முகாமைத்துவ அலுவலகத்தின் நிலைமாற்றம் ஆகியவற்றில் இலங்கை மத்திய வங்கியின் பொறுப்புத் தொடர்பில் 2026 ஜூன் 8 ஆம் திகதி நடைபெற்ற கலந்துரையாடல்களின் போது எழுந்த வேறுபட்ட கருத்துகளைத் தொடர்ந்து, நிதி அமைச்சின் ஆரம்ப அறிக்கைக்குப் பதிலளிக்கும் வகையில் இலங்கை மத்திய வங்கி இரண்டு அறிக்கைகளை வழங்கியது. இலங்கை மத்திய வங்கியின் பொறுப்புகள் தொடர்பான குறிப்பிட்ட விடயங்கள் குறித்து சட்டமா அதிபரிடம் குழு மேலதிகத் தெளிவுபடுத்தலைக் கோரியது.

நிதிசார் கொடுக்கல்வாங்கல்களை அறிக்கையிடல் சட்டத்தின் கீழ் பணத்தூய்தாக்கல் எதிர்ப்பு தொடர்பான கரிசனைகள் தொடர்பில் இலங்கை மத்திய வங்கி மேலும் அவதானமாக இருந்திருக்க வேண்டும் எனவும் முனைப்பான நடவடிக்கைகளை எடுத்திருக்க வேண்டும் எனவும் நிதி அமைச்சு கருதியது. அரசாங்கத்தின் வங்கியாளர் என்ற ரீதியிலான அதன் வகிபாகத்திற்கு நிதிப் பரிமாற்றங்கள் அறிக்கைப்படுத்தல் சட்டத்தின் கீழ் எவ்வித சட்டப் பொறுப்பும் இல்லை என இலங்கை மத்திய வங்கி கருதியது. குழு இந்த வாதத்தை ஆழமாக ஆராய்ந்ததுடன், சட்டமா அதிபர் திணைக்களத்தின் ஆலோசனையையும் கோரியது. தற்போதைய நிலைமை மீதான சட்டமா அதிபரின் சட்டரீதியான விளக்கமானது, பெரும்பாலும் இலங்கை மத்திய வங்கியின் கருத்துடன் ஒத்திருக்கின்றது. ஆயினும், எதிர்காலப் பொறுப்பினை ஏற்படுத்துவதற்காக கொள்கை ரீதியான தீர்மானங்களை எடுக்க முடியும் என்பதை அது ஏற்றுக்கொள்கிறது.

2025 நவம்பரில் மோசடியான கொடுப்பனவு ப்பட்டியல்களின் மீதான மீளச் செலுத்துகைகளுக்காக பொதுக் கடன் முகாமைத்துவ அலுவலக அதிகாரிகள் நிலையான தீர்ப்பனவு அறிவுறுத்தல்களை உருவாக்கிய காலப்பகுதியில், இலங்கை மத்திய வங்கியின் பொதுப்படுகடன் திணைக்கள அதிகாரிகள் தொடர்ந்தும் அச்செயன்முறையை மேற்பார்வை செய்தனர் என நிதி அமைச்சு கருதியது. தமது அரச கடன் திணைக்களமானது ஒதுக்கு அல்லாத முகாமைத்துவ முறைமையின் நிலைமாற்றம் மற்றும் நிலையான தீர்ப்பனவு அறிவுறுத்தல்களை உருவாக்குதல் ஆகியவற்றை 2025 ஒக்டோபர் 24 ஆம்

திகதியளவில் கடன் முகாமைத்துவ அலுவலக அதிகாரிகளிடம் வழங்கி முழுமையாக நிறைவுசெய்துவிட்டதாகவும், இதன் காரணமாக 2025 நவம்பரில் மோசடியான கொடுக்கல்வாங்கல்கள் இடம்பெற்ற போது இலங்கை மத்திய வங்கிக்கு எவ்விதப் பொறுப்புகளும் இருக்கவில்லை எனவும் இலங்கை மத்திய வங்கி கருதியது.

சர்வதேச நிதிப் பரிமாற்றச் செயன்முறைகள் மற்றும் பணத்தூய்தாக்கல் எதிர்ப்பு தொடர்பான கரிசனைகள் குறித்து பொதுக் கடன் முகாமைத்துவ அலுவலக உத்தியோகத்தர்கள் முறையான புரிந்துணர்வைக் கொண்டிருக்கவில்லை எனவும், இத்தகைய விடயங்கள் தொடர்பில் இலங்கை மத்திய வங்கி உத்தியோகத்தர்களால் வழங்கப்பட்ட மட்டுப்படுத்தப்பட்ட தகவல்களின் அடிப்படையில் நடவடிக்கை மேற்கொள்வதற்கான அவர்களது இயலுமை இதனால் மட்டுப்படுத்தப்பட்டது என்றும் நிதி அமைச்சு விளக்கமளித்தது. கொடுப்பனவுச் சரிபார்த்தலுக்கான நிதி அமைச்சின் உள்ளகக் கட்டுப்பாடுகள் தொழிற்படாத போது, இலங்கை மத்திய வங்கியினால் தனது கொடுப்பனவுச் செயன்முறையினூடாக சரிபார்த்தலை உறுதிப்படுத்த முடியாது என இலங்கை மத்திய வங்கியின் விளக்கம் அமைந்திருந்ததுடன், இவ்வாறானதொரு சூழ்நிலையில் இணையக் குற்றத்துடன் தொடர்புடைய ஒரு மோசடியைத் தடுப்பதற்கு இலங்கை மத்திய வங்கியின் பொதுப் படுகடன் திணைக்களம்கூட தவறியிருக்கும் என்பதையும் அது ஏற்றுக்கொண்டது.

2026 ஜூன் 25 ஆம் திகதியிட்ட கடிதத்தில் வழங்கப்பட்ட சட்டமா அதிபரின் கருத்தானது, இலங்கை மத்திய வங்கியின் பொதுப் படுகடன் திணைக்களத்திலிருந்து, பொதுக் கடன் முகாமைத்துவ அலுவலகத்திற்கு ஒரு செயற்பாடு முறையாகக் கையளிக்கப்பட்ட பின்னர், அச்செயற்பாட்டின் மீதான பொறுப்பானது அதன்பின்னர் பொதுக் கடன் முகாமைத்துவ அலுவலகத்தினுடையதாகவே இருக்கும் என்பதைச் சுட்டிக்காட்டியது.

7. முடிவுகள்

I. இணையக் குற்றத்துடன் தொடர்புடைய ஒரு மோசடி தெளிவாக இடம்பெற்றுள்ளது. 2.5 மில்லியன் அமெரிக்க டொலர் பொது நிதி திருடப்பட்டுள்ளது. இணையக் குற்றத்துடன் தொடர்புடைய இந்த மோசடியைப் புரிவதில் சம்பந்தப்பட்ட நிறுவனங்களுக்குள் ஏதேனும் உள்ளகக் கூட்டுச்சதி இருந்ததா என்பதை, குற்றவியல் விசாரணை உள்ளிட்ட சட்ட அமுலாக்கச் செயன்முறை தீர்மானிக்க வேண்டும். சம்பந்தப்பட்ட அதிகாரிகள் தமது நடவடிக்கைகளில் வெறுமனே அறியாமையுடனும், திறமையற்ற வகையிலும் மற்றும் கவனக்குறைவாகவும் மாத்திரமே இருந்தார்களா என்பதை இது உறுதிப்படுத்தும்.

II. இணையக் குற்றத்துடன் தொடர்புடைய மோசடி பற்றிய விசாரணையை அதன் மேற்பார்வைச் செயற்பாட்டின் கண்ணோட்டத்தில் கருத்தில் கொள்வதும்; ஆளுகை, நடைமுறை மற்றும் செயற்பாட்டு அம்சங்கள் ரீதியாக எவ்வாறான அரச நிதி முகாமைத்துவக் குறைபாடுகள் அபாயங்களைத் தீவிரப்படுத்தின என்பதைத் தீர்மானிப்பதுமே அரசாங்க நிதி பற்றிய குழுவின் ஆணையாகும்.

அ. ஒட்டுமொத்த ஆளுகை மட்டத்தில், திறைசேரியின் செயலாளர் மற்றும் மத்திய வங்கியின் ஆளுநர் மட்டத்திலான சிரேஷ்ட அதிகாரிகள் பல குறைபாடுகளுக்குப் பொறுப்பாவார்கள்.

i. புதிதாக ஸ்தாபிக்கப்பட்ட பொதுக் கடன் முகாமைத்துவ அலுவலகத்திற்கான 18 மாத கால நிலைமாற்றத்திற்கு வழிகாட்டுவதற்கான நியதிச்சட்டங்களை வழங்கும் வகையிலான ஒரு புரிந்துணர்வு ஒப்பந்தம் முன்னதாகவே இருந்திருந்தால், திறைசேரியின் செயலாளர் மற்றும் இலங்கை மத்திய வங்கியின் ஆளுநர் ஆகியோர் பயனுள்ள நிலைமாற்றத்திற்கான பொறுப்பு தொடர்பான கருத்து வேறுபாடுகளைத் தவிர்த்திருக்க முடியும். போதுமான பயிற்சி பெறப்பட்டதா என்பதை உறுதிப்படுத்துவதற்கான பிரதான செயற்றிறன் குறிகாட்டிகளையும் பின்பற்றப்பட வேண்டிய சரியான காலக்கெடுவினையும் அது உள்ளடக்கியிருக்கும். புரிந்துணர்வு ஒப்பந்தம் இல்லாமைக்கும் இச்சம்பவம் நிகழ்ந்தமைக்கும் இடையில் நேரடித் தொடர்பொன்றைக் குழுவினால் நிறுவ முடியாவிடினும், அத்தகையதொரு ஒப்பந்தத்தை முறைப்படுத்துவதன் மூலம் அக்காலப்பகுதியில் சம்பந்தப்பட்ட அனைத்து அதிகாரிகளின் பொறுப்புகளும் தெளிவுபடுத்தப்பட்டிருக்கும் எனவும், அது இச்சம்பவம் நிகழ்வதைத் தடுத்திருக்கக் கூடும் எனவும் அது நம்புகின்றது.

ii. 2026 ஆம் ஆண்டின் முற்பகுதியில், இணையக் குற்றத்துடன் தொடர்புடைய மோசடி பற்றி அறிவதற்கு முன்னதாகவே, மற்றவற்றுடன் வெளிநாட்டுக் கடனை மீளச் செலுத்துவதில் நிதி அமைச்சு மற்றும் இலங்கை மத்திய வங்கி ஆகியவற்றுக்கு இடையிலான ஒருங்கிணைப்புப் பொறிமுறைகள் குறித்து கலந்துரையாடலொன்றை நடத்துமாறு அரசாங்க நிதிப் பற்றிய குழு கோரியிருந்தது. இக்கோரிக்கைக்கு பதிலளிக்கும் வகையில், 2026 ஏப்ரல் 4 ஆம் திகதியிட்ட, அரசாங்க நிதிப் பற்றிய குழுவிற்கு இணைக்கையொப்பமிட்டு அனுப்பப்பட்ட கடிதத்தில், ஒருங்கிணைப்பிற்கான தற்போதைய பொறிமுறைகள் போதுமானவையாக உள்ளன என திறைசேரியின் செயலாளர் மற்றும் இலங்கை மத்திய வங்கியின் ஆளுநர் ஆகிய இருவரும் உறுதியளித்திருந்தனர்.[11] எவ்வாறாயினும், பின்னோக்கிப் பார்க்கையில், கடன் மீளச்செலுத்தலுக்கான மாற்றுச் செயன்முறை உட்பட, ஒருங்கிணைப்பில் கணிசமான மேம்பாடுகள் மேற்கொள்ளப்பட வேண்டியிருந்தமை தெளிவாகின்றது.

[11] இணைப்பு 10 - 2026 ஏப்ரல் 04 ஆந் திகதிய திறைசேரி மற்றும் இலங்கை மத்திய வங்கிக்கு இடையிலான ஒருங்கிணைப்பு பொறிமுறைகளின் (Treasury-CBSL coordination mechanisms) போதியதன்மை குறித்து திறைசேரியின் செயலாளர் மற்றும் இலங்கை மத்திய வங்கியின் ஆளுநர் ஆகியோரால் கூட்டாக கையொப்பமிடப்பட்டு அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம்.

iii. நிதி அமைச்சினுள் கடன் மீளச் செலுத்தும் செயன்முறை தொடர்பான பணிகளை முறையாகக் கையளிக்கும் நடைமுறை காணப்படவில்லை எனவும், இது ஒரு தற்றுணிபிலான செலவீனக் கூறு அல்ல என்பதனால் தற்போது இது நிதி ஒழுங்குவிதிகளின் கீழ் உள்ளடக்கப்படவில்லை எனவும், 2026 ஜூன் 23 ஆம் திகதியிடப்பட்ட கடிதத்தின் மூலம் திறைசேரியின் செயலாளர் அரசாங்க நிதி பற்றிய குழுவிற்குச் சமர்ப்பித்துள்ளார். பொது நிதி நிர்வாகத்தை நிர்வகிக்கும் நிதி ஒழுங்குமுறைகளை மீளாய்வு செய்வதன் மற்றும் புதுப்பிப்பதன் அவசியத்தை இது அடிக்கோடிட்டுக் காட்டுகிறது. பொது நிதி செயல்முறைகளை நிர்வகிக்கும் நிதி ஒழுங்குமுறைகளை உடனடியாக மீளாய்வு செய்வதற்கும் புதுப்பிப்பதற்கும் மற்றும் கடன் மறுசெலுத்துகைச் செயல்முறை குறித்து ஆழமாகப் பரிசீலிப்பதற்கும் உள்ள தேவையை இது தெளிவாக எடுத்துக் காட்டுகிறது.

ஆ. நடைமுறை மட்டத்தில், வெளிநாட்டு வளங்கள் திணைக்களம் மற்றும் பொதுக் கடன் முகாமைத்துவ அலுவலகம் ஆகியவற்றின் பணிப்பாளர் தலைமை அதிபதிகள் பல விடயங்களில் தங்களது கடமைகளில் இருந்து முற்றிலும் தவறியுள்ளனர்.

I. கடன் ஒப்பந்தங்களுக்கு எதிராகக் கடன் வழங்குநர்களின் பற்றுச்சீட்டுகளை சரிபார்ப்பதில் போதுமான உள்ளக கட்டுப்பாட்டு நடைமுறையொன்றை நிறுவுவதற்கும், சரிபார்க்கப்பட்ட தகவல் தொடர்பு முறைமைகளை உறுதிப்படுத்துவதற்கும் அவர்கள் தவறியுள்ளனர். இந்த எளிய பணிகள் சரியாகச் செய்யப்பட்டிருந்தால், சைபர் குற்றத்துடன் தொடர்புடைய இந்த மோசடியைத் நிச்சயமாகத் தவிர்த்திருக்க முடியும்.

II. தகவல் தொழில்நுட்ப அமைப்புகள் போதுமான அளவில் புதுப்பிக்கப்பட்டு, சரியாகச் செயல்படுவதை உறுதி செய்ய அவர்கள் தவறியுள்ளனர்.

இ. செயல்பாட்டு மட்டத்தில், வெளிநாட்டு வளங்கள் திணைக்களம், பொதுக் கடன் முகாமைத்துவ அலுவலகம் மற்றும் பொதுக் கடன் திணைக்களம் ஆகியவற்றின் நடுத்தர மட்ட ஊழியர்கள் அலட்சியமாகச் செயல்பட்டதுடன், தங்களது கடமைகளில் சரியான பகுத்தறிவைப் பயன்படுத்துவதை உறுதி செய்யத் தவறியுள்ளனர். இதில் பின்வருவன அடங்கும்:

I. தாம் மின்னஞ்சல் மூலம் தொடர்புகொண்ட முகவரிகளின் டொமைன்களில் சீரான தன்மை பேணப்படுவதை வெளிநாட்டு வளங்கள் திணைக்கள அதிகாரிகள் உறுதிப்படுத்தவில்லை.

II. பரிமாற்றம் நடந்து கொண்டிருந்த போது, கடன் வழங்குநர்களுடனான மின்னஞ்சல் தொடர்புகளின் போது, பொதுக் கடன் முகாமைத்துவ அலுவலகத்தின் இணை அதிகாரிகளை பிரதியாக (CCed) இணைப்பதற்கு

வெளிநாட்டு வளங்கள் திணைக்கள அதிகாரிகள் நடவடிக்கை எடுக்கவில்லை.

III. வெளிநாட்டு வளங்கள் திணைக்களத்தின் தகவல் தொழில்நுட்ப அதிகாரிகள் தங்களது தகவல் தொழில்நுட்ப அமைப்புகளின் உறுதித்தன்மையை உறுதிப்படுத்தவில்லை.

IV. அதிகாரப் பரிமாற்றத்திற்கு உட்பட்டுக்கொண்டிருந்த மற்றும் பொதுக் கடன் முகாமைத்துவ அலுவலக குழுவின் அனுபவமின்மை குறித்து நன்கு அறிந்திருந்தபோதிலும், இலங்கை மத்திய வங்கியின் பொதுக் கடன் திணைக்கள (CBSL-PDD) அதிகாரிகள், அதன் நிதித் திணைக்களத்தினால் எழுப்பப்பட்ட சாத்தியமான பணத் தூய்தாக்கல் தடுப்பு தொடர்பான பொறுப்புகளை, 2025 நவம்பரில் அதன் வெளிநாட்டு தொடர்பு வங்கியினால் மீண்டும் மீண்டும் சுட்டிக்காட்டப்பட்ட போதிலும், பொதுக் கடன் முகாமைத்துவ அலுவலகத்தின் சிரேஷ்ட அதிகாரிகளின் கவனத்திற்கு கொண்டு செல்ல தவறியுள்ளனர்.

III. இந்த அறிக்கையானது கடன் மறுசெலுத்துகைச் செயல்முறையில் கட்டமைப்பு ரீதியான தோல்விகள் காணப்படுவதைக் கண்டறிந்துள்ளதுடன், இதன் விளைவாக பரிமாற்றக் காலப்பகுதியில் நீண்ட காலமாகக் தொடர்ச்சியான மோசடிப் பரிவர்த்தனைகள் இடம்பெற்றுள்ளன. எவ்வாறாயினும், இணையக் குற்றத்துடன் தொடர்புடைய இந்த மோசடி சார்ந்த செயல்பாட்டுக் குறைபாடுகள் காரணமாக நிதி அமைச்சின் நடுத்தர மட்ட ஊழியர்கள் நால்வர் மாத்திரமே பணியிடை நீக்கம் செய்யப்பட்டுள்ளதாக இக்குழுவிற்கு அறிவிக்கப்பட்டுள்ளது. இந்த நான்கு ஊழியர்களில் ஒருவரது திடீர் மரணம் உண்மையிலேயே மிகவும் துரதிர்ஷ்டவசமானது. தனிப்பட்ட பொறுப்புகள் கணக்கில் கொள்ளப்பட வேண்டுமாயின், இந்த அறிக்கையின் கண்டுபிடிப்புகளைக் கருத்திற் கொண்டு, தற்போது நடைபெற்று வரும் குற்றவியல் விசாரணைகளின் முடிவுகளுக்கு அமைவாகவே அது செய்யப்பட வேண்டும்.

IV. இணையக் குற்றத்துடன் (cybercrime) தொடர்புடைய இந்த மோசடியைத் தொடர்ந்து, அது மீண்டும் நிகழாமல் தடுப்பதற்கும் எதிர்கால இடர்களைக் குறைப்பதற்கும் நிதி அமைச்சினால் எடுக்கப்பட்ட நிறுவன ரீதியான நடவடிக்கைகள், உண்மையில் வெளிநாட்டுக் கடன் மறுசெலுத்துகைச் செயல்முறைக்காக ஆரம்பத்திலிருந்தே நடைமுறையில் இருந்திருக்க வேண்டிய உள்ளக கட்டுப்பாடு மற்றும் இணையப் பாதுகாப்பு ஆகியவற்றின் அடிப்படை நடவடிக்கைகளாகும். இது நிர்வாக, நடைமுறை மற்றும் செயல்பாட்டு அம்சங்கள் முழுவதும் காணப்பட்ட குறைபாடுகளை மீண்டும் ஒருமுறை அடிக்கோடிட்டுக் காட்டுகிறது.

V. இந்த தொடர்ச்சியான சம்பவங்கள் காரணமாக, எக்ஸ்போர்ட் பைனான்ஸ் அவுஸ்திரேலியா நிறுவனத்திற்கு செலுத்த வேண்டிய தொகையில் நிலுவைத் தொகைகளும் ஏற்பட்டுள்ளன. இதனால் அரசாங்கம் உரிய கொடுப்பனவுகளை அவசரமாகச் செலுத்த வேண்டிய தேவை ஏற்பட்டுள்ளது.

8. விதப்புரைகள்

இந்த அறிக்கையில் கண்டறியப்பட்ட விடயங்களின் அடிப்படையில், அரசாங்க நிதி பற்றிய குழுவானது பாராளுமன்றத்தில் சமர்ப்பிப்பதற்காக பின்வரும் விதப்புரைகளை முன்மொழிகிறது:

1. கௌரவ சபாநாயகர் அவர்களும் மற்றும் நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சும், இந்த அறிக்கையின் முடிவுகளின் அடிப்படையில் பொருத்தமான விசாரணை நடவடிக்கைகளுக்கான அவசியமான மற்றும் போதுமான நடவடிக்கைகளை மேற்கொள்வதற்கு.

2. ஒட்டுமொத்த வெளிநாட்டுக் கடன் மறுசெலுத்துகைச் செயல்முறை குறித்தும் ஒரு விசேட கணக்காய்வை மேற்கொள்ளுமாறு தேசிய கணக்காய்வு அலுவலகத்திற்கு கௌரவ சபாநாயகர் அவர்கள் பணிப்புரை விடுப்பதற்கு.

3. விசாரணைகள் நிறைவடைந்ததைத் தொடர்ந்து ஏதேனும் அதிகாரிகள் பொறுப்புக் கூற வேண்டியவர்கள் எனக் கண்டறியப்பட்டால், நிதிப்பிரமாணம் (FR) 105 இன் கீழ், இழப்புகளில் ஒரு பகுதியையேனும் மீட்டெடுப்பதற்கான சாத்தியக்கூறுகளை நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு ஆராய்வதற்கு.

4. பொது நிதி முகாமைத்துவ ச் சட்டத்தின் (PFM Act) கீழ் கடன் முகாமைத்துவச் செயல்முறைகளுக்குப் பொருந்தக்கூடியவை உள்ளடங்கலாக, திருத்தப்பட்ட நிதிப்பிரமாணங்களை அறிமுகப்படுத்துவதை நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு விரைவுபடுத்துவதற்கு. இந்த திருத்தப்பட்ட நிதிப்பிரமாணங்கள் மூன்று மாதங்களுக்குள் நடைமுறைப்படுத்தப்பட வேண்டும். உள்ளக கட்டுப்பாடுகளை, குறிப்பாக கடன் ஒப்பந்தங்களுக்கு எதிராகக் கடன் வழங்குநர்களின் கொடுப்பனவு பட்டியல்களைச் சரிபார்ப்பது மற்றும் அங்கீகரிக்கப்பட்ட தகவல் தொடர்பு வழிகள் தொடர்பானவற்றை நிரந்தரமாக வலுப்படுத்த வேண்டிய தேவை உள்ளது. எதிர்காலத்தில் இதுபோன்ற சம்பவங்களைத் தவிர்ப்பதற்கு இந்த நிலையான சரிபார்ப்புகளை நடைமுறைப்படுத்துவது இன்றியமையாததாகும்.

5. தற்போதுள்ள பொதுக் கடன் முகாமைத்துவ மற்றும் கடன் மறுசெலுத்துகைச் செயல்முறைகள் குறித்த விரிவான மதிப்பீடொன்றை வழங்குவதற்கு தகுதியான, ஒரு சுயாதீனமான, வெளித்தரப்பொன்றின் சேவைகளை நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு பெற்றுக்கொள்வதற்கு.

6. டிஜிட்டல் பொருளாதார அமைச்சுடன் இணைந்து, கடன் வழங்குநர்களின் தகவல்களுக்கான பாதுகாப்பான தரவுத்தளமொன்றை நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு அமைப்பதற்கு.

7. எக்ஸ்போர்ட் பைனான்ஸ் அவுஸ்திரேலியா (Export Finance Australia) நிறுவனத்துடனான நிலுவைப்பணக் கொடுப்பனவுகள் குறித்த கலந்துரையாடல்களில் உடனடியாகக் கவனம் செலுத்துவதற்கு நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு நடவடிக்கை எடுப்பதற்கு.

8. நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு, அதன் கீழ் உள்ள அனைத்து திணைக்களங்களினதும் தகவல் தொழில்நுட்ப அமைப்புகள், அமைச்சின் தகவல் தொழில்நுட்ப முகாமைத்துவ திணைக்களத்தினால் மேற்பார்வை செய்யப்படுவதை உறுதிப்படுத்துவது குறித்து பரிசீலிப்பதற்கு.

9. டிஜிட்டல் பொருளாதார அமைச்சு, அரச நிறுவனங்களின் தகவல் தொழில்நுட்ப மற்றும் இணையப் பாதுகாப்பு அமைப்புகள் தொடர்பாக இலங்கை கணினி அவசர தயார்நிலைக்குழு குழுவின் (SL-CERT) விதப்புரைகள் நடைமுறைப்படுத்தப்படுவதை உறுதி செய்வதற்கான பொறுப்பை ஏற்பதற்கும், முக்கியமான தகவல் தொழில்நுட்ப அமைப்புகள் போதுமான அளவில் புதுப்பிக்கப்பட்டு, செயல்பாட்டு ரீதியாக இருப்பதை நோக்கி கூடுதல் அவதானம் செலுத்தப்படுவதை உறுதிசெய்வதற்கும்.

10. அரசாங்கத்திற்கான வங்கியாளர் என்ற ரீதியில் இலங்கை மத்திய வங்கி தனது பொறுப்புகளை நிறைவேற்றுவது தொடர்பான ஏற்பாடுகளின் அடிப்படையில், நிதியியல் கொடுக்கல் வாங்கல்கள் பற்றிய அறிக்கைப்படுத்தல் சட்டத்தில் அவசியமான திருத்தங்களை மேற்கொள்வது குறித்து அரசாங்கம் பரிசீலிப்பதற்கு.

11. இணையக் குற்றத்துடன் தொடர்புடைய இந்த மோசடி குறித்த குறிப்பிட்ட பரிந்துரைகளுக்கு அப்பால், பொதுத்துறைக்கான ஒரு விரிவான முறைகேடுகளை வெளிப்படுத்துபவர்களைப் பாதுகாக்கும் கொள்கையை அரசாங்கம் அறிமுகப்படுத்த வேண்டும்.

இணைப்புகள்

இணைப்பு 1 -: 2026 மே 08 ஆந் திகதிய 2.5 மில்லியன் அமெரிக்க டாலர் பெறுமதியான வெளிநாட்டுக் கடன் மறுசெலுத்துகை மோசடிப் பரிவர்த்தனை தொடர்பாக அரசாங்க நிதி பற்றிய குழுவிற்கு சமர்ப்பிக்கப்பட்ட அரசாங்க நிதி பற்றிய குழுவின் அறிக்கை

இணைப்பு 2 - 2026 யூன் 01 ஆந் திகதிய 2.5 மில்லியன் அமெரிக்க டாலர் பெறுமதியான வெளிநாட்டுக் கடன் மறுசெலுத்துகை மோசடிப் பரிவர்த்தனை தொடர்பாக அரசாங்க நிதி பற்றிய குழுவிற்கு சமர்ப்பிக்கப்பட்ட நிதி அமைச்சின் அறிக்கை - இணைப்புகள் நீங்கலாக.

இணைப்பு 3 - 2026 யூன் 15 ஆந் திகதிய அரசாங்க நிதி பற்றிய குழுவிற்கு சமர்ப்பிக்கப்பட்ட இலங்கை மத்திய வங்கியின் விரிவான அறிக்கை - இணைப்புகள் நீங்கலாக.

இணைப்பு 4 - 2026 யூன் 15 ஆந் திகதிய ஏறத்தாழ 2.5 மில்லியன் அமெரிக்க டாலர் பெறுமதியான வெளிநாட்டுக் கடன் மறுசெலுத்துகை மோசடிப் பரிவர்த்தனை தொடர்பான நிதி அமைச்சின் அறிக்கைக்கான பதிலீடாக அரசாங்க நிதி பற்றிய குழுவிற்கு சமர்ப்பிக்கப்பட்ட இலங்கை மத்திய வங்கியின் அறிக்கை - இணைப்புகள் நீங்கலாக.

இணைப்பு 5 – 2026 யூன் 09 ஆந் திகதிய இலங்கை கணினி அவசர தயார்நிலைக்குழுவினால் (SL-CERT) அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம் - வெளிநாட்டு வளங்கள் திணைக்களத்தின் மின்னஞ்சல் சேவையகத்தின் (email server) நிலைமை குறித்த இணையப் பாதுகாப்பு அறிக்கைகள் மற்றும் விளக்கங்களைச் சமர்ப்பித்தல் - இணைப்புகள் நீங்கலாக.

இணைப்பு 6 - இலங்கை கணினி அவசர தயார்நிலைக்குழுவினால் (SL-CERT) சமர்ப்பிக்கப்பட்ட அரச நிறுவனங்களுக்கான தகவல் மற்றும் இணையப் பாதுகாப்புக் கொள்கை.

இணைப்பு 7 - 2026 யூன் 15 ஆந் திகதிய சட்டமா அதிபர் திணைக்களத்திலிருந்து அனுப்பப்பட்ட கடிதம்

இணைப்பு 8 - 2026 யூன் 25 ஆந் திகதிய சட்டமா அதிபர் திணைக்களத்திலிருந்து அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம்.

இணைப்பு 9 - 2026 யூன் 23 ஆந் திகதிய கடன் மறுசெலுத்துகைச் செயல்பாடுகளுக்கான அதிகாரப் பகிர்வு (delegation of authority) தொடர்பாக திறைசேரியின் செயலாளரால் அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம்.

இணைப்பு 10 - 2026 ஏப்ரல் 04 ஆந் திகதிய திறைசேரி மற்றும் இலங்கை மத்திய வங்கிக்கு இடையிலான ஒருங்கிணைப்பு பொறிமுறைகளின் (Treasury-CBSL coordination mechanisms) போதியதன்மை குறித்து திறைசேரியின் செயலாளர் மற்றும் இலங்கை மத்திய வங்கியின் ஆளுநர் ஆகியோரால் கூட்டாக கையொப்பமிடப்பட்டு அரசாங்க நிதி பற்றிய குழுவிற்கு அனுப்பப்பட்ட கடிதம்.

அறிக்கை மற்றும் இணைப்புகளைப் பார்வையிட தயவுசெய்து கீழே உள்ள QR குறியீட்டைப் பயன்படுத்தவும்:

Annexure 1

பத்தாவது பாராளுமன்றம் - முதலாவது கூட்டத்தொடர்

2.5 மில்லியன் ஐ.அ.டொலர் பெறுமதியான வெளிநாட்டுக் கடன் மீளச் செலுத்தலில் இடம்பெற்ற மோசடியான பரிவர்த்தனை

தொடர்பிலான

அரசாங்க நிதி பற்றிய குழுவின் அறிக்கை

குழுவின் அங்கத்துவ உறுப்பினர்

கௌரவ ரவி கருணாநாயக்க, பா.உ., அவர்களினால்

2026 மே மாதம் 08 ஆம் திகதி வெள்ளிக்கிழமை

பாராளுமன்றத்திற்குச் சமர்ப்பிக்கப்பட்டது

குழுவின் உறுப்பினர்கள்

கௌரவ (கலாநிதி) ஹர்ஷ த சில்வா, பா.உ. (தலைவர்)

கௌரவ சதுரங்க அபேசிங்ஹ, பா.உ.

கௌரவ (கலாநிதி) (செல்வி) கௌஷல்யா ஆரியரத்ன, பா.உ.

கௌரவ அர்கம் இல்யாஸ், பா.உ.

கௌரவ நிசாந்த ஜயவீர, பா.உ.

கௌரவ சட்டத்தரணி ரஊப் ஹகீம், பா.உ.

கௌரவ ரவி கருணாநாயக்க, பா.உ.

கௌரவ ஹர்ஷன ராஜகருணா, பா.உ.

கௌரவ சாணக்கியன் ராஜபுத்திரன் இராசமாணிக்கம், பா.உ.

கௌரவ அஜித் அகலகட, பா.உ.

கௌரவ எம்.கே. எம். அஸ்லம், பா.உ

கௌரவ நிமல் பலிஹேன, பா.உ.

கௌரவ சட்டத்தரணி சித்ரால் பெர்னாந்து, பா.உ.

கௌரவ விஜேசிரி பஸ்நாயக்க, பா.உ.

கௌரவ சுனில் றாஜபக்ஷ, பா.உ.

கௌரவ திலிண சமரகோன், பா.உ.

கௌரவ சம்பிக ஹெட்டிஆரச்சி, பா.உ.

கௌரவ (செல்வி) சட்டத்தரணி லக்மாலி ஹேமசந்திர, பா.உ.

<u>2.5 மில்லியன் ஐ.அ.டொலர் பெறுமதியான வெளிநாட்டுக் கடன் மீளச் செலுத்தலில் இடம்பெற்ற மோசடியான பரிவர்த்தனை தொடர்பிலான அரசாங்க நிதி பற்றிய குழுவின் அறிக்கை</u>

2026 ஏப்ரல் 30 அன்று அரசாங்க நிதி பற்றிய குழுவில் நடத்தப்பட்ட ஊடகங்கள் இன்றிய ஆலோசனைக் கூட்டத்தில் (Close-door discussion), சுமார் 2.5 மில்லியன் அமெரிக்க டொலர்கள் மதிப்புடைய பத்துக் கொடுப்பனவுகளைப் பாதித்து மோசடியான பரிவர்த்தனை ஒன்று நடைபெற்றுள்ளது என்பதை நிதி, திட்டமிடல், பொருளாதார அபிவிருத்தி அமைச்சு ஏற்றுக்கொண்டது.

<u>சமுகமளித்த உறுப்பினர்கள்</u>

கௌரவ (கலாநிதி) ஹர்ஷ த சில்வா, பா.உ., (தவிசாளர்)

கௌரவ சதுரங்க அபேசிங்ஹ, பா.உ.,

கௌரவ (கலாநிதி) (செல்வி) கௌஷல்யா ஆரியரத்ன, பா.உ.,

கௌரவ அர்கம் இல்யாஸ், பா.உ.,

கௌரவ சட்டத்தரணி ரஊப் ஹகீம், பா.உ.,

கௌரவ ரவி கருணாநாயக்க, பா.உ.,

கௌரவ ஹர்ஷன ராஜகருணா, பா.உ.,

கௌரவ சாணக்கியன் ராஜபுத்திரன் இராசமாணிக்கம், பா.உ., (ஒன்லைன்)

கௌரவ எம்.கே. எம். அஸ்லம், பா.உ.,

கௌரவ நிமல் பலிஹேன, பா.உ.,

கௌரவ சட்டத்தரணி சித்ரால் பெர்னாந்து, பா.உ.,

கௌரவ விஜேசிரி பஸ்நாயக்க, பா.உ.,

கௌரவ சுனில் றாஜபக்ஷ, பா.உ.,

கௌரவ திலிண சமரகோன், பா.உ.,

கௌரவ சம்பிக்க ஹெட்டிஆராச்சி, பா.உ.,

கௌரவ (செல்வி) சட்டத்தரணி லக்மாலி ஹேமசந்திர, பா.உ.,

<u>சமுகமளித்த உத்தியோகத்தர்கள்</u>

<u>நிதி, திட்டமிடல் மற்றும் பொருளாதார அபிவிருத்தி அமைச்சு</u>

டாக்டர். ஹர்சன சூரியப்பெரும, திறைசேரிச் செயலாளர்

திரு. ஏ. கே. செனவிரத்ன, திறைசேரிப் பிரதிச் செயலாளர்

திரு. எஸ். எஸ். முதலிகே, திறைசேரிப் பிரதிச் செயலாளர்

<u>வெளி வளங்கள் திணைக்களம்</u>

திரு. ஆர்.எம்.எஸ்.பி.எஸ். பண்டார, பணிப்பாளர் நாயகம்

திரு. வசந்த தர்மசேன, மேலதிக பணிப்பாளர் நாயகம்

<u>அரச படுகடன் முகாமைத்துவத் திணைக்களம்</u>

திருமதி. உதேனி உடுகஹாபட்டுவ, பணிப்பாளர் நாயகம்

<u>இலங்கை மத்திய வங்கி</u>

திருமதி. கே.எம்.ஏ.என் தவுலகல, சிரேஷ்ட பிரதி ஆளுநர்/பிரதம நிறைவேற்று அதிகாரி

திரு. கே.ஜி.பி. சிறிகுமர, பிரதி ஆளுநர்

திரு.கே.வி.கே. அல்விஸ், பணிப்பாளர், கொடுப்பனவுகள் மற்றும் தீர்ப்பனவுகள் திணைக்களம்

திருமதி. டி.எஸ்.எல்.சிறிமனே, பிரதம கணக்காளர்

திரு. என்.டி.வை.சி. வீரசிங்ஹ, நாணயக் கண்காணிப்பாளர்

பின்புலம்

- 2024 ஆம் ஆண்டின் 33 ஆம் இலக்க அரச படுகடன் முகாமைத்துவச் சட்டம் இயற்றப்பட்டதைத் தொடர்ந்து, அரச படுகடன் திணைக்களத்தினை அரச படுகடன் முகாமைத்துவ அலுவலகமாக நிறுவன ரீதியாக நிலைமாற்றுதல் 2024 ஆம் ஆண்டின் பிற்பகுதியில் இருந்து நடைபெற்று வருகின்றது. இது, இலங்கை மத்திய வங்கியின் அரச படுகடன் திணைக்களத்திற்கும், நிதி, திட்டமிடல் மற்றும் பொருளாதார அமைச்சின் வெளி வளங்கள் திணைக்களத்திற்கும் நிதி அமைச்சின் அரச தொழில் முயற்சிகள் திணைக்களத்திற்கும் இருக்கின்ற பொறுப்புக்களை மத்தியமயப்படுத்துவதைச் சம்பந்தப்படுத்துகின்றது.

- அரச படுகடன் திணைக்களத்தின் செயற்பாடுகளை அரச படுகடன் முகாமைத்துவ அலுவலகத்திற்கு நிலைமாற்றும் செயன்முறை 2025 ஆம் ஆண்டின் பிற்பகுதியில் பூர்த்திசெய்யப்பட்டதுடன் இது 2026 ஜனவரியில் அரச படுகடன் திணைக்களம் மூடப்படுவதற்கு இட்டுச்சென்றது. வெளி வளங்கள் திணைக்களத்தின் அதிகமான செயற்பாடுகள் அரச படுகடன் முகாமைத்துவ அலுவலகத்திற்கு மாற்றப்பட்ட அதேவேளை, வெளி வளங்கள் திணைக்களம், அரச படுகடன் முகாமைத்துவ அலுவலகத்துடன் சேர்ந்து இரு தரப்பு மற்றும் பல் தரப்புக் கடன் பெறல்களைப் பற்றிப் பேச்சுவார்த்தை நடத்துவதிலும் அவற்றினை நிறைவேற்றுவதிலும் தொடர்ந்தும் ஈடுபட்டு வருகின்றது.
- அரச படுகடன் முகாமைத்துவ அலுவலகமானது, முன் அலுவலகம், நடு அலுவலகம், மற்றும் பின் அலுவலகம் எனக் கட்டமைக்கப்பட்டுள்ளது. பின் அலுவலகம் கடன்களைத் திருப்பிச் செலுத்தும் செயற்பாடுகளைக் கையாளுகின்றது.

அரச படுகடன் முகாமைத்துவ அலுவலகத்தின் அதிகாரங்களும் செயற்பாடுகளும் கீழே சுருக்கமாக வழங்கப்பட்டுள்ளன:

அரச படுகடன் முகாமைத்துவ அலுவலகம்

முன் அலுவலகம்

- அரச கடன் பெறல்
- உத்தரவாதங்களும் மறு கடன் வழங்குதலும்
- விநியோகத்தர் கடன்களும் நிதிக் குத்தகைகளும்

நடு அலுவலகம்

- நடுத்தவணைக் கடன் முகாமைத்துவ உபாயமார்க்கம் மற்றும் வருடாந்தக் கடன் பெறல் திட்டம்
- கடன் அபாயநேர்வு மதிப்பீடு மற்றும் கண்காணிப்பு
- அபாயநேர்வுக் கட்டுப்பாடு மற்றும் இயைபுறல்
- கடன்களை மீளச் செலுத்துதல் பற்றிய எதிர்வுகூறல்

பின் அலுவலகம்

- கடன் பதிவிடல்
- கடன்களை மீளச் செலுத்துதல்
- அறிக்கையிடல் மற்றும் வெளியீடுகள்

அவதானிப்புக்கள்

கண்டுபிடிப்பின் காலச்சட்டகம்

1. 2026 ஜனவரி இந்தியாவுக்கானதாக இருக்கலாம் என மறைமுகமாகக் குறிப்பிடப்படுகின்ற,ஓர் இரு தரப்புக் கடன் வழங்குனர் சம்பந்தப்படும் வெளிநாட்டுக் கடன் மீள்கொடுப்பனவுச் செயன்முறை தொடர்பாக சந்தேகத்துக்கிடமான சைபர் செயற்பாடு பற்றி நிதி அமைச்சுக்கு எச்சரிக்கை வழங்கப்பட்டது. இதனை அடிப்படையாகக் கொண்டு இலங்கை கணிணி அவசரநிலைத் தயார்நிலை அணி மற்றும் இலங்கை பொலிசின் சைபர் பாதுகாப்புப் பிரிவு ஆகியவற்றுக்கு அறிவிப்பது உள்ளடங்கலாக நிதி அமைச்சு நடவடிக்கைகளை எடுத்தது.

2. 2026 ஆம் ஆண்டு மார்ச் மாதம்; நிதி அமைச்சும் பின்வருவனவற்றை வினவியது; 2025 ஆம் ஆண்டின் மூன்றாம் காலாண்டில் செலுத்த வேண்டிய கடன் திருப்பிச் செலுத்தல்கள் கிடைக்கவில்லை என அவுஸ்திரேலிய அதிகாரிகள் "எக்ஸ்போட் பினான்ஸ் ஆஸ்ரேலியாவிற்கு (Export Finance Australia)" அறிக்கையிட்டனர்[1]. நிதிக் கட்டளைகள் மற்றும் 2006 ஆம் ஆண்டின் 6 ஆம் இலக்க நிதிசார் கொடுக்கல் வாங்கல்களை அறிக்கையிடல் சட்டத்தின் பிரகாரம் குறித்துரைக்கப்பட்ட காலப் பகுதிக்குள் பொலிஸ் குற்றப் புலனாய்வுத் திணைக்களம் மற்றும் இலங்கை மத்திய வங்கியின் நிதியியல் உளவறிதல் பிரிவு ஆகியவற்றில் முறைப்பாடுகள் செய்வதற்கு இந்தக் கண்டறிதல் இட்டுச் சென்றது.
3. 2025 செப்டெம்பர் முதல் 2026 சனவரி வரையிலான காலப்பகுதியில் மேற்கொள்ளப்பட்ட சுமார் 2.5 மில்லியன் ஐஅ.டொ. பெறுமதியான 10 கொடுக்கல் வாங்கல்கள் தொடர்பான விசாரணைகள் தற்போது மேற்கொள்ளப்பட்டு வருகின்றன. இந்த விசாரணை இலங்கை மற்றும் அவுஸ்திரேலியா மட்டுமல்லாது, பல்வேறு நாடுகளையும் உள்ளடக்கியுள்ளது.
4. குழுவின் கேள்விக்கு பதிலளித்த திறைசேரிச் செயலாளர், நிதிக் கட்டளை 104 இன் கீழ் உள்ளக விசாரணைக்கான தேவையான நடவடிக்கைகள் மேற்கொள்ளப்பட்டு, முடிவில் நான்கு அதிகாரிகள் தற்காலிகமாக பணித்தடைக்கு உள்ளாக்கப்பட்டுள்ளதாவும் குறிப்பிட்டார். நிதிக் கட்டளை 104

[1] நிலுவையிலுள்ள சுமார் ஐ.அ.டொ. 39 மில்லியனுக்கான அவுஸ்திரேலியா மற்றும் இலங்கைக்கு இடையிலான இருதரப்பு கடன் மறுசீரமைப்புக்காக 2025 ஒக்டோபர் 27 ஆம் திகதி உத்தியோகபூர்வமாக கைச்சாத்திடப்பட்டது; 2025 இறுதியில் PDMO இன் 4ஆம் காலாண்டு செய்தி மடலிற்கிணங்க எக்ஸ்போட் பினான்ஸ் அன்ட் இன்சூரன்ஸ் காப்பரேசன் ஒப் அவுஸ்ரேலியாவிற்கு ஐ.அ.டொ. 20.4 மில்லியனும் ANZ இன்வெஸ்ட்மன்ட் பேங்க் அவுஸ்ரேலியாவிற்கு ஐ.அ.டொ. 18.7 மில்லியனும் நிலுவையாக இருந்தன.

இன் பிரகாரம், மோசடி கண்டறியப்பட்டு 7 நாட்களுக்குள் ஒரு பூர்வாங்க அறிக்கையும், மூன்று மாதங்களுக்குள் இறுதி அறிக்கையும் சமர்ப்பிக்கப்பட வேண்டும். இதே போன்ற விசாரணைகள், 2006 ஆம் ஆண்டின் 6ஆம் இலக்க நிதிசார் கொடுக்கல் வாங்கல்களை அறிக்கையிடல் சட்டத்தின் பிரகாரம் இலங்கை மத்திய வங்கியின் நிதியியல் உளவறிதல் பிரிவில் முறைப்பாடு செய்யப்பட்ட விடயமும் வினவலின் போது உறுதி செய்யப்பட்டது.

5. நிலையியற் கட்டளை 121(2) இன் கீழ் அரச படுகடன் மற்றும் கடன் சேவை தொடர்பாக ஆராய்வதற்கான குறிப்பான ஆணையைக் கொண்டுள்ள ஒரேயொரு மேற்பார்வைக் குழுவாக முதன்மைப் பணியைக் கொண்டிருக்கும் அரசாங்க நிதி பற்றிய குழுவின் ஊடாக பாராளுமன்றத்திற்குள்ள வகிபாகத்தை குழு வலியுறுத்தியது.

நிறுவன ரீதியான செயல்முறைகள்:

6. 2026 சனவரி மாதத்தில் மத்திய வங்கியின் அரச படுகடன் திணைக்களம் மூடப்படுவதற்கு முன்னர், 2025 செப்டெம்பர் முதல் 2026 சனவரி வரையிலான காலப்பகுதியும், மத்திய வங்கியின் அரச படுகடன் திணைக்களத்திலிருந்து (PDD) அரச படுகடன் முகாமைத்துவ அலுவலகத்திற்கு (PDMO) கடன் முகாமைத்துவச் செயல்முறைகள் நிலைமாற்றத்தின் இறுதிக் கட்டமும் ஒன்றாக உள்ளது. 2024 ஆம் ஆண்டின் 33 ஆம் இலக்க பொதுத் தனிசு முகாமைத்துவச் சட்டம் மற்றும் 2023 ஆம் ஆண்டின் 16 ஆம் இலக்க இலங்கை மத்திய வங்கிச் சட்டத்தின் எதிர்பார்ப்புகளின் பிரகாரம் மத்திய வங்கியை அரசிறைத் தொழிற்பாடுகளிலிருந்து நீக்குவதற்காக இந்த விடயம் மேற்கொள்ளப்பட்டது.
7. குறிப்பிட்ட காலப்பகுதியில், முழுமையற்ற தகவல்களைக் கொண்ட இரண்டு கொடுக்கல் வாங்கல்களுக்கான கொடுப்பனவுகள் மத்திய வங்கியின் முறைமைகளிலிருந்து நிராகரிக்கப்பட்டதாக மத்திய வங்கி அதிகாரிகள் குறிப்பிட்டனர். மத்திய வங்கியின் நிதித் திணைக்களம் குறைந்தது ஒரு கொடுக்கல் வாங்கல் தகவல் பற்றியாவது மீண்டும் உறுதிப்படுத்துவதற்காக PDMO மற்றும் PDD இன் கவனத்திற்குக் கொண்டுவந்துள்ளது.
8. அரச படுகடன் முகாமைத்துவ அலுவலகம் (PDMO) நிறுவப்படுவதற்கு முன்னர், இருதரப்பு மற்றும் பல்தரப்புக் கடன் முகாமைத்துவம் தொடர்பான அனைத்து தொழிற்பாடுகளையும் வெளி வளங்கள் திணைக்களம் மேற்கொண்டது. கடன் வழங்குநர்களிடமிருந்து கடன் திருப்பிச் செலுத்துவதற்கான கொடுப்பனவு பட்டியல்களை வெளி வளங்கள் திணைக்களம் பெற்று, கொடுப்பனவு அறிவுறுத்தல்களை அதன் பின் அலுவலம் ஊடாகச் செயற்படுத்தி அவற்றை இலங்கை மத்திய வங்கியின் அரச படுகடன் திணைக்களத்திற்கு அனுப்பியது. அரச படுகடன் திணைக்களம் கொடுப்பனவு அறிவுறுத்தல்களை உறுதிப்படுத்தி அவற்றை இலங்கை மத்திய வங்கியின் கொடுப்பனவுகள் திணைக்களத்தின்

மூலமான SWIFT நிதிக் கைமாற்றங்களை உறுதிசெய்வதற்காக இலங்கை மத்திய வங்கியின் நிதித் திணைக்களத்திற்கு அனுப்பியது.

9. அரச படுகடன் முகாமைத்துவ அலுவலகம் (PDMO) நிறுவப்பட்டதுடன், வெளி வளங்கள் திணைக்களத்தின் (ERD) பின் அலுவலகத் தொழிற்பாடுகள் PDMO இன் பின் அலுவலகத்தினால் பொறுப்பேற்கப்பட்டன. ஆனாலும், ERD தொடர்ந்து கடன் வழங்குநர்களிடமிருந்து பெரும்பாலான கொடுப்பனவு பட்டியல்களைப் பெற்று, செயன்முறைக்காக அவற்றைச் PDMO இன் பின் அலுவலகத்திற்கு அனுப்பியது. கொடுப்பனவுத் தகவல் உறுதிப்படுத்தல் செயன்முறைக்காக மத்திய வங்கியின் PDD பயன்படுத்திய அதே செயன்முறைகளையும் மென்பொருள் முறைமைகளையும் PDMO இன் பின் அலுவலகக் கடன் சேவைப் பிரிவு பின்பற்றி உறுதிப்படுத்தப்பட்ட அறிவுறுத்தல்களை மத்திய வங்கியின் நிதித் திணைக்களத்திற்கு அனுப்பப்பட்டதாக குழுவிற்கு PDMO அறிவித்தது. இந்தச் செயன்முறைகளைத் தாபிப்பதற்கு ஆதரவாக மத்திய வங்கியின் PDD, 2025 டிசெம்பர் வரைக்கும் PDMO உடன் இணைந்து செயற்பட்டதாகத் தெரிகிறது.

10. கடன் சேவைக் கொடுப்பனவு செயன்முறையானது நிதி அமைச்சின் உரிய அதிகாரிகளுக்கு அதிகாரம் வழங்கப்பட்டு, காகித ஆவணங்கள் மற்றும் கையொப்பங்களின்றி, முழுமையான டிஜிட்டல் செயன்முறை மூலம் மேற்கொள்ளப்படுகிறது. இந்தச் செயன்முறையின் கீழ், திரட்டு நிதியிலிருந்து அனைத்து வெளிநாட்டுக் கடன் சேவைக் கொடுப்பனவுகளையும் அங்கீகரிக்கும் அதிகாரம் PDMO இன் பின் அலுவலகப் பணிப்பாளருக்கு வழங்கப்பட்டுள்ளதாகத் தெரிகிறது.

11. கடன் சேவை கொடுப்பனவு உறுதிப்படுத்தல் தொடர்பான பிரதி திரட்டு நிதியிலிருந்தான காசுப் பாய்ச்சலுக்கு தொழிற்பாட்டு ரீதியாகப் பொறுப்பான திறைசேரி தொழிற்பாடுகள் திணைக்களத்திற்கு அனுப்பப்படும். ஆனாலும் கொடுப்பனவை உறுதிப்படுத்தவோ அல்லது இறுதி அங்கீகாரம் வழங்கவோ அது தேவைப்படுத்தப்படவில்லை.

12. ITMIS போன்ற பொதுவான முறைமைகளுக்கு அப்பால், நிதி அமைச்சின் பல்வேறுபட்ட திணைக்களங்கள் அவற்றின் குறிப்பான தொழிற்பாடுகளுடன் தொடர்புடைய வித்தியாசமான தகவல் தொழில்நுட்ப முறைமைககளையும் சேவை வழங்குநர்களையும் கொண்டுள்ளன.

13. மேலே விவரிக்கப்பட்ட டிஜிட்டல் கொடுப்பனவு செயன்முறைகளை இயலச்செய்வதற்காக, நிதிக் கட்டுப்பாட்டுக்கான தொழிற்பாடுகளை ஒப்படைப்பதன் மீதான 135 ஆம் நிதிக் கட்டளையின் பிரகாரம் ஆண்டுதோறும் திறைசேரிச் செயலாளரிடமிருந்து உரிய அதிகாரிகளுக்கு அதிகாரம் ஒப்படைக்கப்படுகிறதா என்று குழு வினவியது. இது தொடர்பான தேவையான விபரங்களை குழுவிடம் சமர்ப்பிப்பதாக திறைசேரிச் செயலாளர் உறுதியளித்தார்.

14. நிறுவன ரீதியான செயன்முறைகளில் காணப்படுகின்ற பல அம்சங்கள் தொடர்பாகக் குழு பின்வருவனவற்றை வலியுறுத்தியது:

அ. 2024 மே மாதம் அரச படுகடன் முகாமைத்துவச் சட்டத்தை ஆரம்பாக அங்கீகரித்ததிலிருந்து, கடன் முகாமைத்துவத் தொழிற்பாடுகளை பயனுறுதியுடன் மையப்படுத்துவதற்குத் தேவையான நிபுணத்துவம் கொண்ட அலுவலர்களின் ஆட்சேர்ப்பை PDMO உறுதிசெய்ய வேண்டும் என்ற அரசாங்க நிதி பற்றிய குழுவின் தொடர்ச்சியான கோரிக்கையை மீண்டும் வலியுறுத்தியது.

ஆ. மிக மூத்த அதிகாரிகள் அல்லது மற்றொரு திணைக்களத்தின் அதிகாரிகளின் ஊர்ஜிதப்படுத்தலின்றி, பெரிய அளவிலான கடன் திருப்பிச் செலுத்துதல்களுக்கு இறுதி கொடுப்பனவு அங்கீகாரத்தை PDMO இன் பின் அலுவலகப் பணிப்பாளர் ஒருவருக்கு வழங்கும் ஆற்றல்.

இ. வெளிநாட்டுக் கடன் நிலுவைகள் மற்றும் கொடுப்பனவுகளை உறுதிப்படுத்துவதில் சம்பந்தப்பட்ட நிறுவனங்களுக்கும் அதிகாரிகளுக்கும் இடையே இணக்கமின்மை காணப்பட்டது. கடன் சேவையாற்றல் மற்றும் அறிக்கையிடும் பணிகளை முழுமையாகப் அரச படுகடன் முகாமைத்துவ அலுவலகத்திற்கு மாற்றுவதற்குப் பொதுத் தனிசு முகாமைத்துவச் சட்டம் கட்டளையிட்டிருந்தபோதிலும், வெளிநாட்டு வளங்கள் திணைக்களம் தொடர்ந்து இப்பணியில் கணிசமான பங்கினை வகித்து வருகின்றமை தெரிகிறது.

ஈ. இவ்விடயம் தொடர்பான எந்தவொரு பொறுப்பிலிருந்தும் இலங்கை மத்திய வங்கியின் அதிகாரிகள் தங்களை விடுவித்துக்கொள்ள முடியாது. 2026 ஜனவரி மாதம் வரை, மத்திய வங்கியின் அரச படுகடன் திணைக்களம், அரச படுகடன் முகாமைத்துவ அலுவலகத்தின் பணிகளுக்கு ஆதரவளிப்பதில் ஈடுபட்டிருந்ததுடன், நாட்டின் வெளிநாட்டு ஒதுக்குகளின் முகாமையாளர் என்ற வகையில், மத்திய வங்கியில் பேணப்படும் திறைசேரியின் அந்நியச் செலாவணிக் கணக்குகள் எவ்வாறு பயன்படுத்தப்படுகின்றன என்பது குறித்து அவர்கள் விழிப்புடன் இருந்திருக்க வேண்டும்.

<u>பொது நிதி முகாமைத்துவம் தொடர்பான பிரச்சனைகள்:</u>

15. திட்டமிடப்பட்ட கடன் கொடுப்பனவுகளைச் செலுத்தத் தவறியதன் காரணமாக, இந்த மோசடியான கொடுக்கல் வாங்கலானது இலங்கையை அவுஸ்திரேலியாவுக்கு தொழில்நுட்ப ரீதியான கடன் தவறுநராக மாற்றியுள்ளதா என்பது குறித்து குழு கேள்வி எழுப்பியது. விருப்பம், திறன் மற்றும் குறித்த

நேரத்தில் கொடுப்பனவை மேற்கொண்டமை (அக்கொடுப்பனவு கடனளிப்பவரால் பெறப்படவில்லை என்றபோதிலும்) ஆகியவற்றை வெளிப்படுத்தியுள்ளதால், இவ்விடயத்தின் விளைவாக இலங்கை அவுஸ்திரேலியாவுக்குக் கடன் தவறுநராக அமைந்துள்ளதாகத் தான் நம்பவில்லை எனத் திறைசேரியின் செயலாளர் தெரிவித்தார். இது தொடர்பாகக் கடன் மறுசீரமைப்புச் செயல்முறைக்கு ஆதரவளித்த சர்வதேச ஆலோசகர்களின் கருத்துக்கள் பெறப்பட்டுள்ளன.

16. இத்தகையதொரு பிரச்சினை மீண்டும் ஏற்படாதிருப்பதை உறுதி செய்வதற்கு எத்தகைய நடவடிக்கைகள் எடுக்கப்பட்டுள்ளன என்பது குறித்து குழு வினவியது. இலங்கை மத்திய வங்கியின் ஆதரவுடன் கடன் செலுத்தல் செயன்முறையை குறிப்பாக சரிபார்த்தல் மற்றும் அங்கீகரித்தல் அம்சங்களை வலுப்படுத்துவதற்கு நடவடிக்கைகள் எடுக்கப்பட்டுள்ளதாகத் திறைசேரியின் செயலாளர் தெரிவித்தார்.
17. 1992 ஆம் ஆண்டின் பின்னர் நிதி ஒழுங்குவிதிகள் ஒருங்கமைக்கப்படவோ அல்லது விரிவான முறையில் புதுப்பிக்கப்படவோ இல்லை என்பதை குழு சுட்டிக்காட்டியது. இதன் விளைவாக, அரசின் நவீன நிதிச் செயல்முறைகள் மற்றும் அண்மைய ஆண்டுகளில் இயற்றப்பட்ட புதிய சட்ட ஏற்பாடுகளுக்கு மத்தியில் அவை போதுமானதாக இல்லை. புதுப்பிக்கப்பட்ட நிதி ஒழுங்குவிதிகள் தொகுக்கப்பட்டு வருவதாகவும், இன்னும் சில மாதங்களில் அவை இறுதி செய்யப்படும் என எதிர்பார்க்கப்படுவதாகவும் திறைசேரியின் செயலாளர் தெரிவித்தார்.

<u>பரிந்துரைகள்:</u>

1. நிதி அமைச்சு, நிகழ்வுகளின் விரிவான காலவரிசை மற்றும் இதுவரை எடுக்கப்பட்ட நடவடிக்கைகள், இந்த மோசடியான கொடுக்கல் வாங்கல் எவ்வாறு மற்றும் ஏன் இடம்பெற்றது, கடன் முகாமைத்துவத்தில் ஈடுபட்டுள்ள நிறுவனங்களின் பணியாளர்கள் மற்றும் தொழில்நுட்பத் திறன் உள்ளிட்ட கண்டறியப்பட்ட நிறுவன ரீதியான பிரச்சினைகள் மற்றும் இது மீண்டும் ஏற்படாதிருப்பதற்கான நடவடிக்கைகள் ஆகியவற்றை உள்ளடக்கிய விரிவான அறிக்கையொன்றை நான்கு வாரங்களுக்குள், அதாவது 2026 மே மாத இறுதிக்கு முன்னதாகச் சமர்ப்பிக்க வேண்டும்.
2. நிதி அமைச்சு, அனைத்து வெளிநாட்டுக் கடன் மீளச் செலுத்துதல்களுக்குமான நடைமுறையிலுள்ள கொடுப்பனவுச் செயல்முறைகளின் அடிப்படையாக அமைந்துள்ள நிதிக் கட்டுப்பாட்டு அதிகாரப் பகிர்ந்தளிப்பை உறுதிப்படுத்தும் ஆவணங்களை அதன் விரிவான அறிக்கையுடன் சமர்ப்பிக்க வேண்டும்.
3. பொதுத் தனிசு முகாமைத்துவச் சட்டத்தில் குறிப்பிடப்பட்டுள்ளவாறு, அரச படுகடன் முகாமைத்துவப் பணிகள் முழுமையாக அரச படுகடன் முகாமைத்துவ அலுவலகத்திற்கு மாற்றப்படுவதை நிதி அமைச்சு உறுதி செய்ய வேண்டும்.

4. சைபர் பாதுகாப்பை ஒரு நிதிசார் இடராகக் கருத்திற்கொண்டு, அண்மைய ஆண்டுகளில் அரச நிறுவனங்களில் தொடர்ச்சியாக இடம்பெற்று வரும் கொடுப்பனவு சிக்கல்கள் மற்றும் தரவு மீறல்கள் மீண்டும் ஏற்படுவதைத் தடுப்பதற்கு நிதி அமைச்சு விரிவான நடவடிக்கைகளை எடுக்க வேண்டும்.
5. பகிரங்க நிதிசார் முகாமைத்துவச் சட்டம் மற்றும் பொதுத் தனிசு முகாமைத்துவச் சட்டம் ஆகியவற்றிற்கு அமைவாகத் தொகுக்கப்பட்டு வரும் புதுப்பிக்கப்பட்ட நிதி ஒழுங்குவிதிகள் இறுதி செய்யப்பட்டு, கூடிய விரைவில் பாராளுமன்றத்தின் மீளாய்விற்காகச் சமர்ப்பிக்கப்பட வேண்டும்

Annex 2

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

<u>Background Information of the Incident</u>

- 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.

- 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 01st January 2026.

<u>Brief of the Events Occurred</u>

- 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 06th January 2026 (Annex I- A). Then the payment was done to the correct account and informed the activity to the Criminal Investigation Division on 09th 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

2

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 24th 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 14th 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 14th 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 24th 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 26th 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 05th January 2026 had been paid to the beneficiary account in TD bank on 05th 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 20th 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 15th 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."*

5 B

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 – 09th 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 – 23rd March 2026 (Annex VI- B)

- Appointed an internal Technical fact finding committee for initial internal investigation – 23rd March 2026 (Annex VI- C)

- Made a written complaint to the Criminal Investigation Department – 24th March 2026 (Complaint number C51/26/CR) (Annex VI- D)

- Reported to the Financial Intelligence Unit (FIU) of CBSL by ERD– 01st April 2026 (Annex VI- E)

- Submitted the Committee Report to the Secretary to the Treasury – 10th April 2026 (Annex VI- F)

- Interdicted Two Officials in ERD and Two Officials in PDMO on 17th 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 – 06th May 2026 (Annex VI- H)

b

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 20th 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)

- 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 30th 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 being 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 to expected to complete shortly.

- A Process has being 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 allocates 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.

11

- 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.

Annex 3

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,

[signature]

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

P.O. Box 590 Colombo | TEL.: +94 11 2477477, +94 11 2477577 | FAX: +94 11 2477677 | E-MAIL: governor@cbsl.lk

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 apprises 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 Authorised by	Status
1	LR900	2025.11.14	AUD 141,739.95	Commonwealth Bank of Australia Sydney CTBAAU2SXXX	Mish Global LLC in care of Export Finance and Insurance Corporation	[redacted]	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.	[redacted]	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	[redacted]	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	[redacted]	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	[redacted]	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	[redacted]	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 NRTHUS33XXX	Mish Global LLC in care of Export Finance and Insurance Corporation	[redacted]	Payment Advice authorized by- PDMO (Annex 31.6a) Invoice authorized by- PDMO (Annex 31.6b)	Completed

Note 1:

After processing the payment (LR902) by Federal Reserve Bank, the Beneficiary Bank (US 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.

Annex 4

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."*[1] 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

[1] 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.[2]

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.

[2] 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 emphasis 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.

Annex 5

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය
இலங்கை கணினி அவசர தயார்நிலை அணி
Sri Lanka Computer Emergency Readiness Team

SRI LANKA CERT|CC

කාමර අංක. 4-112, බී.එම්.අයි.සී.එච්, බෞද්ධාලෝක මාවත, කොළඹ 07.
அறை இல. 4-112, பி.எம்.ஐ.சி.எச், பௌத்தாலோக மாவத்தை, கொழும்பு 07.
Room No. 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07.

Consultants, CoPF
I'm sending herewith 13 annextures received from CERT for your perusal and due analysis pls.
10/06/2026

09th June 2026

Our Ref: CERT/106/ADMIN/MoDE/003

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

Through

Secretary
Ministry of Digital Economy 09/06/2026

COMMITTEE OFFICE
09 JUN 2026
PARLIAMENT OF SRI LANKA

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	Annextures
1	Cabinet Decsion on Information and Cyber Security Policy (Policy) for Government Organizations	Cabinet Decsion 22/1173/630/001, Date 2022 August 31	Annexture 1

දුරකථන / தொலைபேசி / Telephone 11-269 1692, 101 (Hot Line)
ෆැක්ස් / தொலைநகல் / Fax 11-269 1064
ඊ-තැපැල / மின்னஞ்சல் / E-mail info@cert.gov.lk
වෙබ් / இணையத்தளம் / Web www.cert.gov.lk
https://lk.linkedin.com/company/sri-lanka-cert-cc https://www.facebook.com/CERT.lk/

No.1225

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) *	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 03-10-2025 21-01-2026 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	Annextures
	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 o Department of Development Finance (DFD): LMS Senior Citizen SystemDepartment o Treasury Operations Department (TOD): TFMS, GFLSMS o Department of State Accounts (SAD): CIGAS, E-Payroll, ITMIS	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)	19th February 2026	Reports submitted to ERD
Forensic Investigation Report on the Email Impersonation Incident (Australia)	30th March 2026	
ERD Report - France Communication	.10th 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

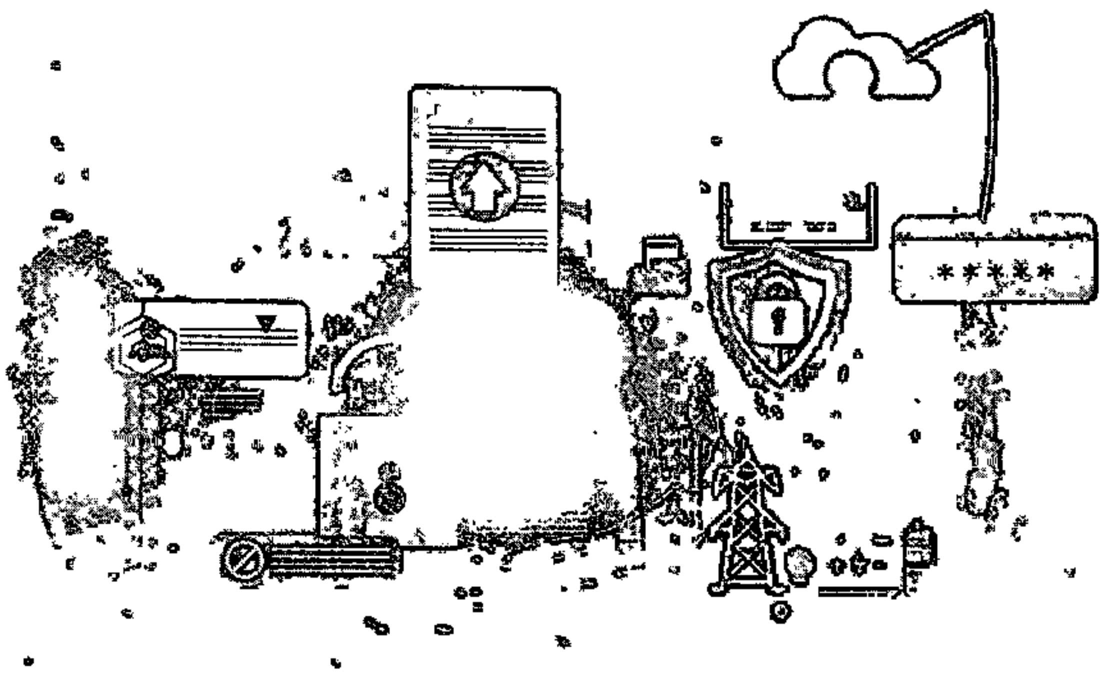
NCKKarunasena

Dr. Kanishka Karunasena
Chief Executive Officer (Actg.)

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

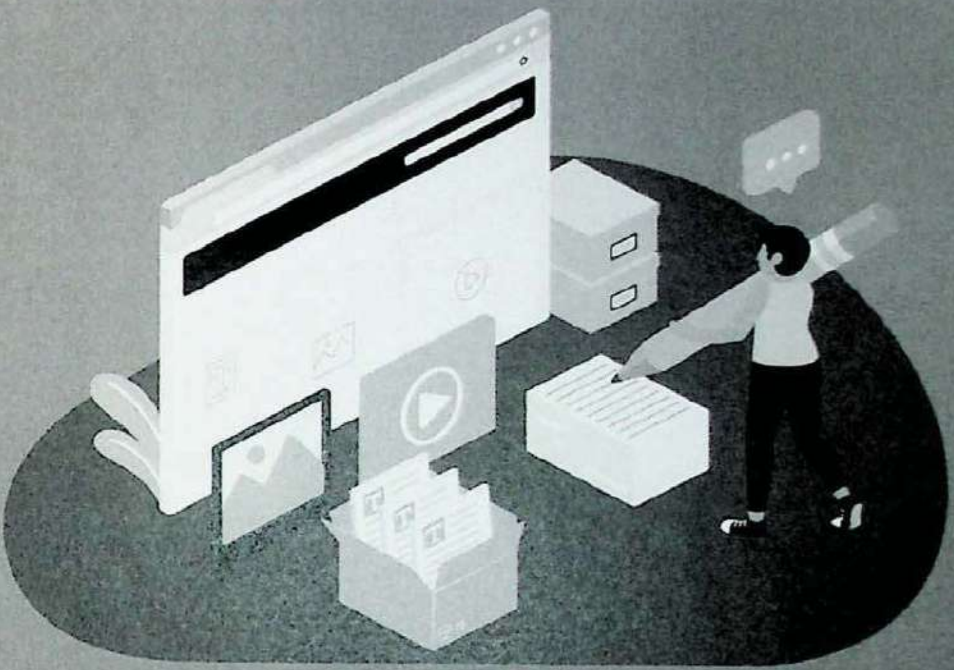
Annex 6

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT)



INFORMATION AND CYBER SECURITY POLICY FOR GOVERNMENT ORGANIZATIONS

அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கை

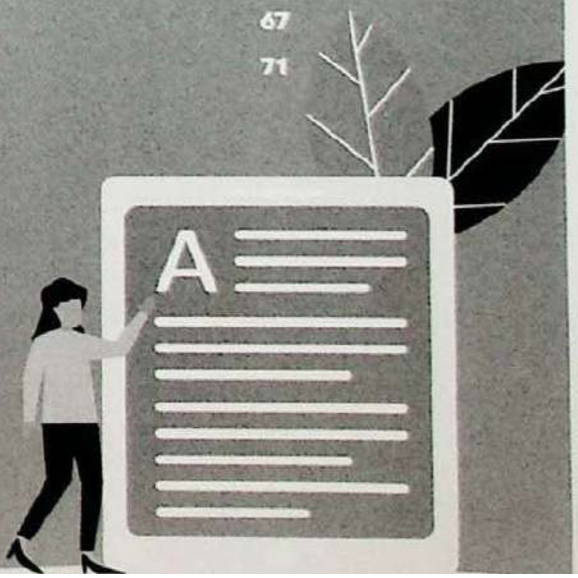


Contents

1.	Introduction		7
2.	Information and Cyber Security Policy Framework		9
3.	Information and Cyber Security Policy		12
	3.1.	Objectives	12
	3.2.	Scope of the Policy	13
4.	Policy Statements		18
	4.1.	Information and Cyber Security Governance	18
	4.1.1.	Leadership	19
	4.1.2.	Security Organization Structure	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.	Information Security Committee (ISC)	21
	4.1.4.	Risk Management Committee (RMC)	21
	4.1.5.	Responsibilities of End Users	21
	4.1.6.	Capacity Building	22
	4.1.7.	Security Clearance of Staff	22

	4.1.8.	Strategic Alignment	23
	4.1.9.	Action Plans and Resource	23
	4.1.10.	Compliance	23
4.2.	**Identify Assets, Owners, Users and Risks**		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.	**Protect Assets**		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

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

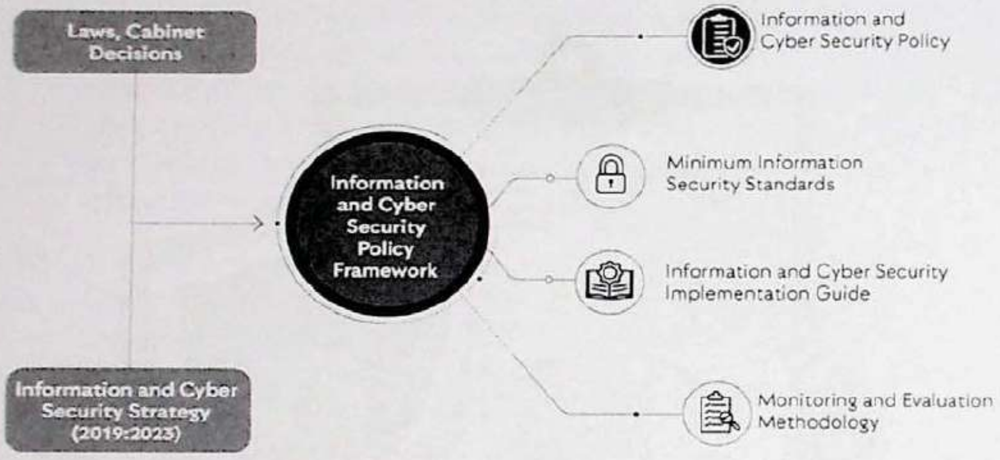


Figure 1: Information and Cyber Security Policy Framework

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 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 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.

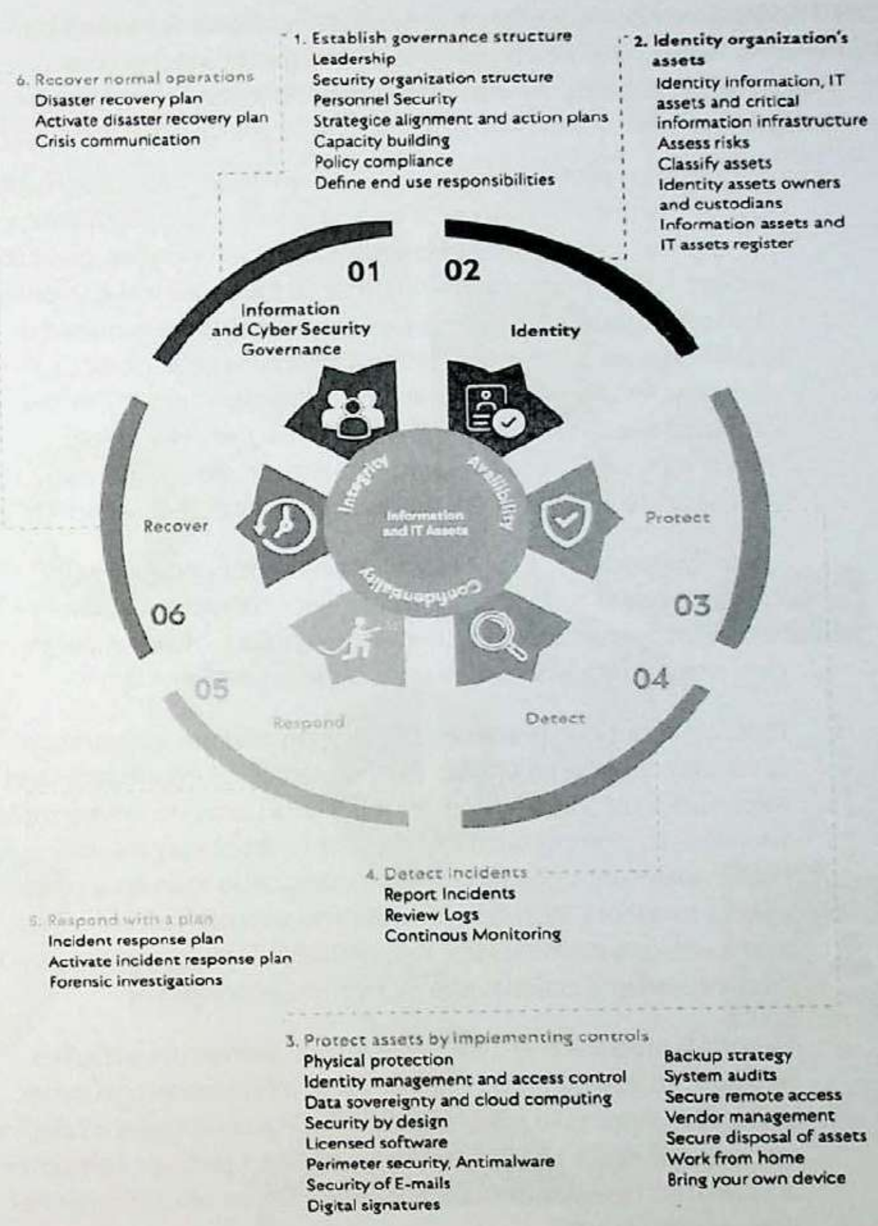


Figure 2: Steps to Information and Cyber Security.

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).

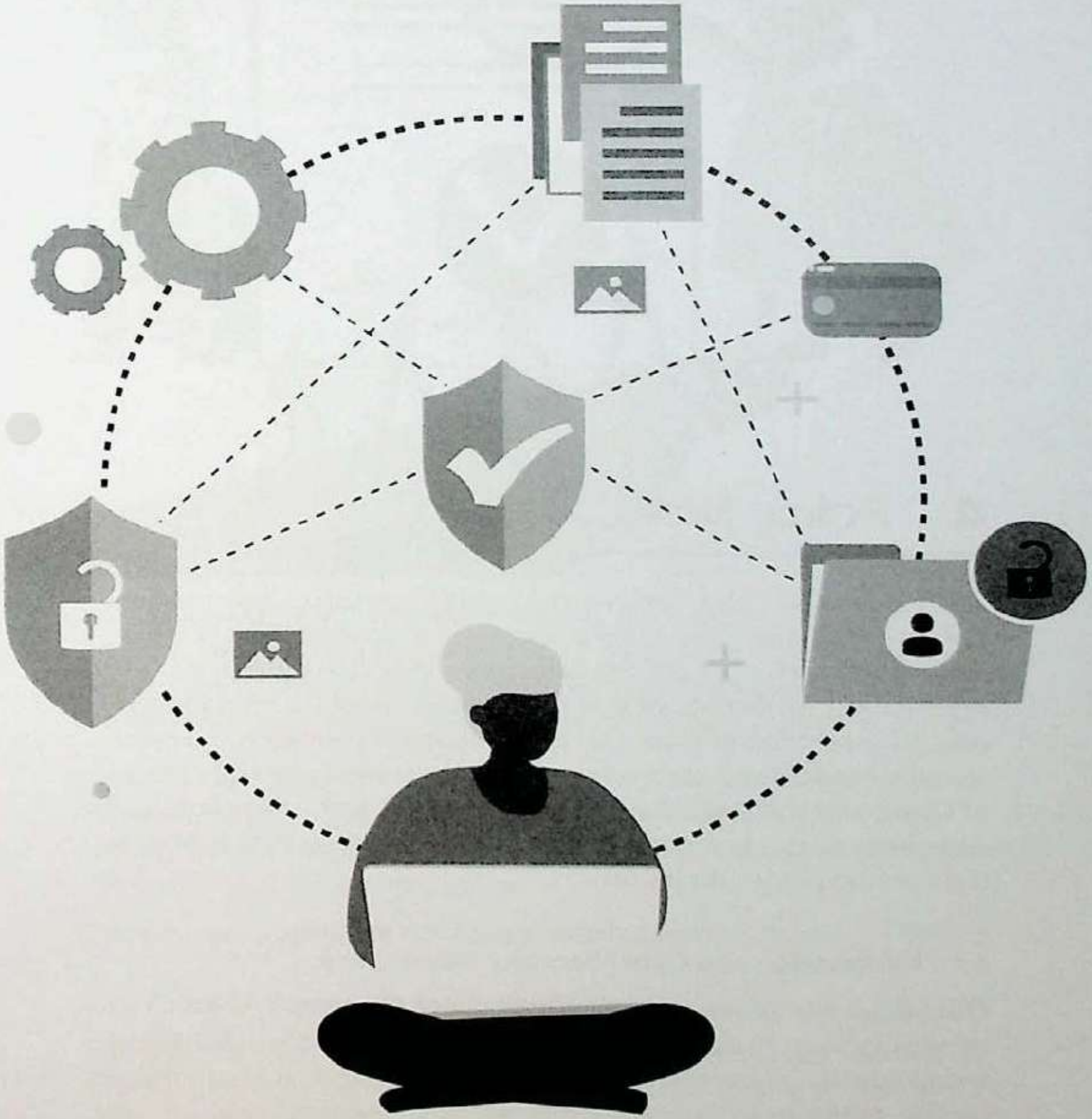
b. Identify Function: It facilitates government organizations to identify assets such as data, information, computers, systems, and digital infrastructure and, to identify and effectively manage the risks associated with those assets (Refer Section 4.2).

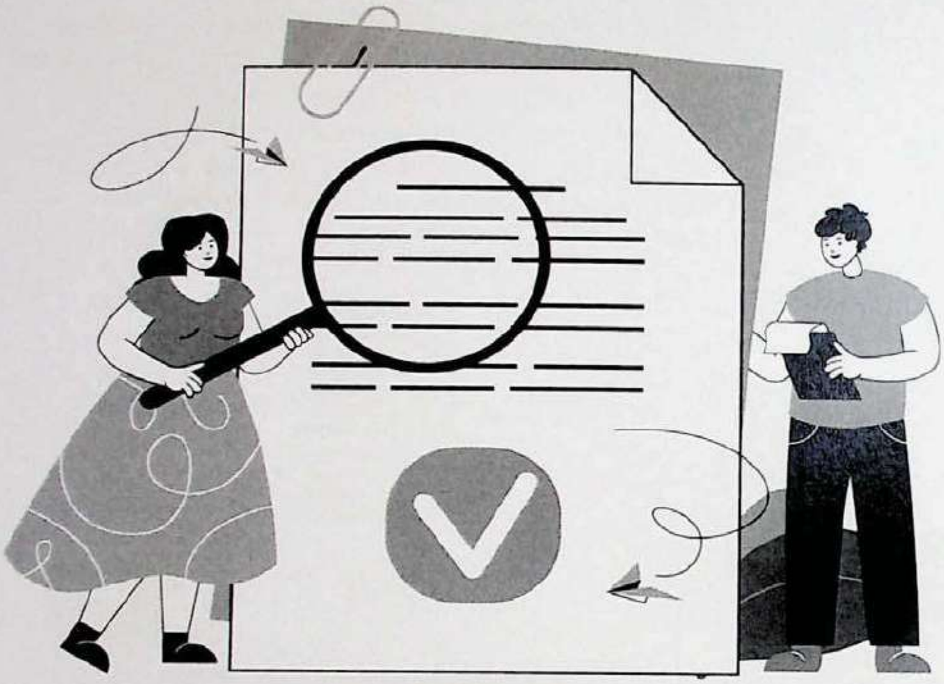
c. Protect Function: The Protect Function outlines appropriate controls required to ensure the protection of information and information technology assets in order to provide uninterrupted services. To comply with the Protect function, organizations shall implement appropriate controls such as managing 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.

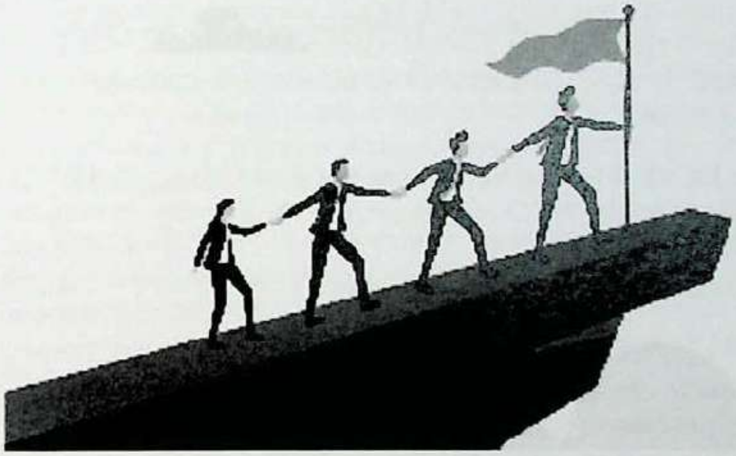
4.1 Information and Cyber Security Governance

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

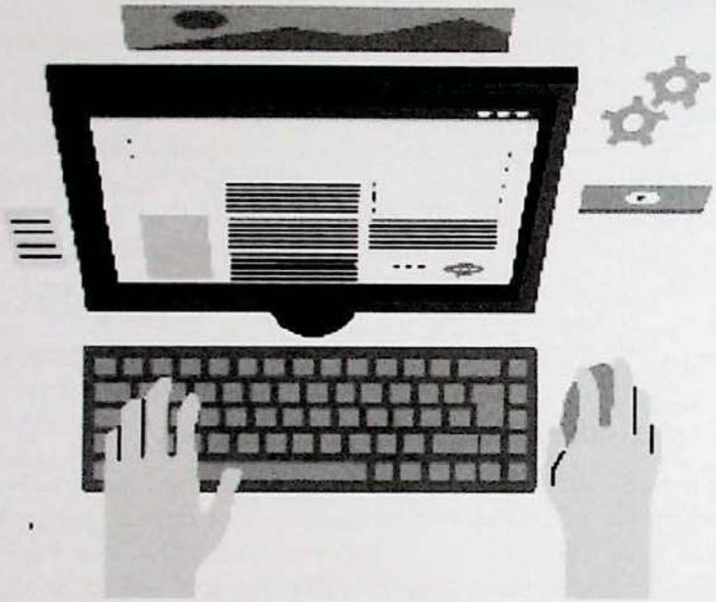
4.1.5 Policy on Responsibilities of End Users

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

4.1.8 Policy on Strategic Alignment

The organization must align its information and cyber security activities with its corporate vision, mission and objectives. All information and cyber security strategies, programs, projects and activities implemented within the organization should be designed in a way that is in line with the vision, mission and objectives of the organization.

Compliance: Applicable to all government organizations

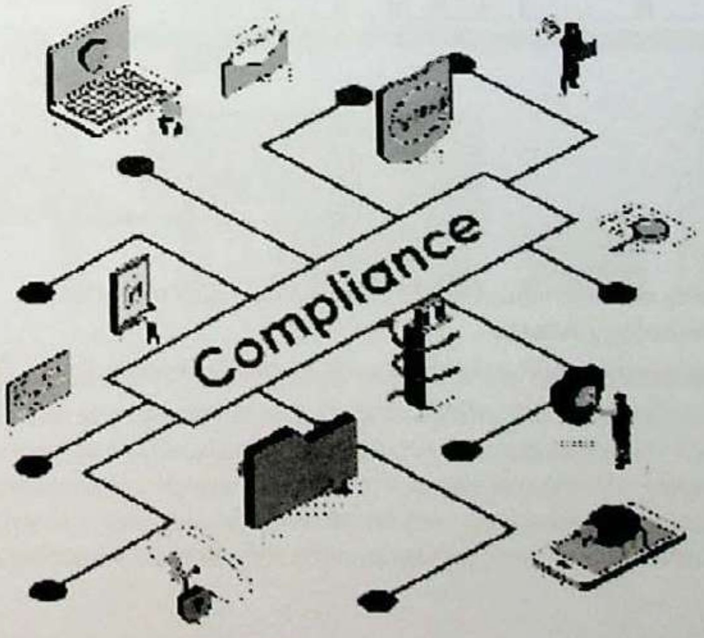
4.1.9 Policy on Action Plans and Resource

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.

Compliance: Applicable to all government organizations

4.1.10 Policy on Compliance

The organization shall comply with the Information and Cyber Security Policy. As noted in Sections 4.1.1 and 4.1.2 (a), the HOO and ISO shall hold the ultimate responsibility of ensuring that the organization complies with this Policy.



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.

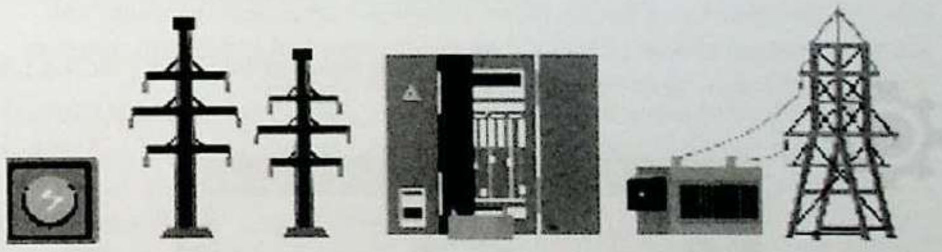
Compliance: Applicable to all government organizations

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 CNIIs to conduct Risk assessments.

Compliance: Applicable to CNII 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.

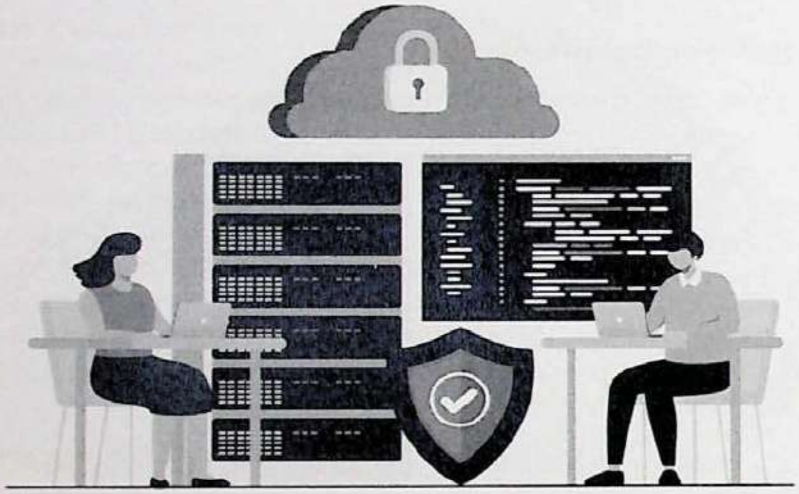
Classification of information assets shall be performed based on accepted guidelines. The classification levels for information assets shall be "Secret", "Confidential", "Limited Sharing", "Public" and "Unclassified".

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.

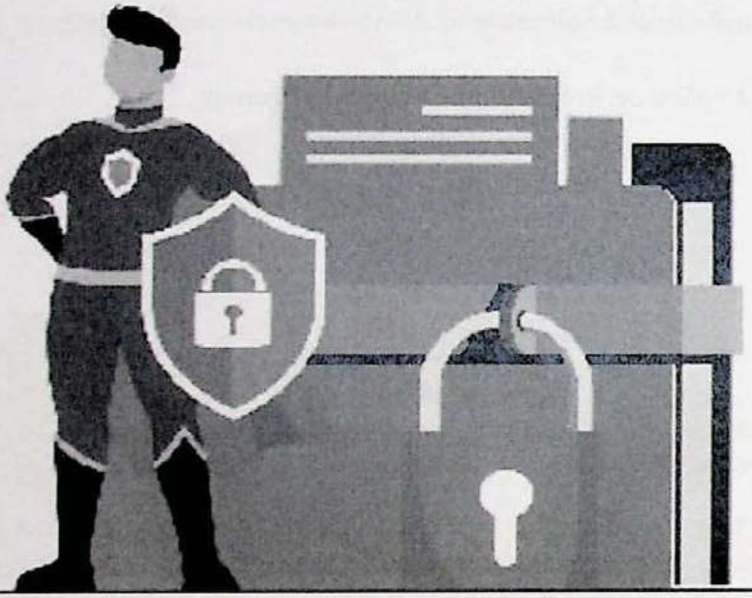
Based on the protection requirements of assets, each organization shall define secure areas to store or process assets which are important to the organization. Information assets classified as "Secret" and "Confidential" are to be stored and processed in the stated secure areas.

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

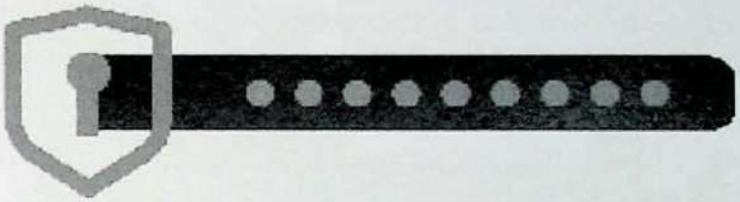
4.3.4 Policy on Identity Management and Access Control

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.



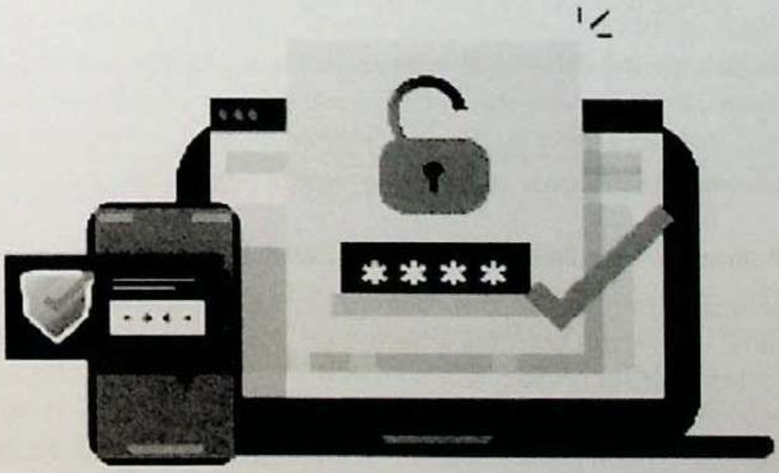
The organization shall ensure that the Identity Management and Access Control Process implemented by the organization is adequate and up-to-date. Further, all employees and all third-party service providers should adhere to the Identity Management and Access control process implemented by the government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

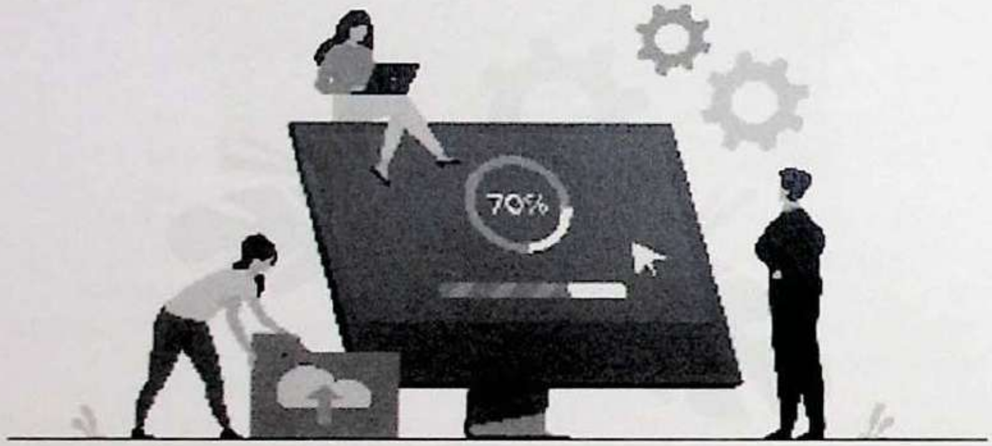
LGC is a government-owned private cloud service operated by the Information and Communication Technology Agency (ICTA), which was designed to fulfill the cloud service requirements of the government. It is, however, strictly recommended to the organizations to perform a proper risk assessment prior to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

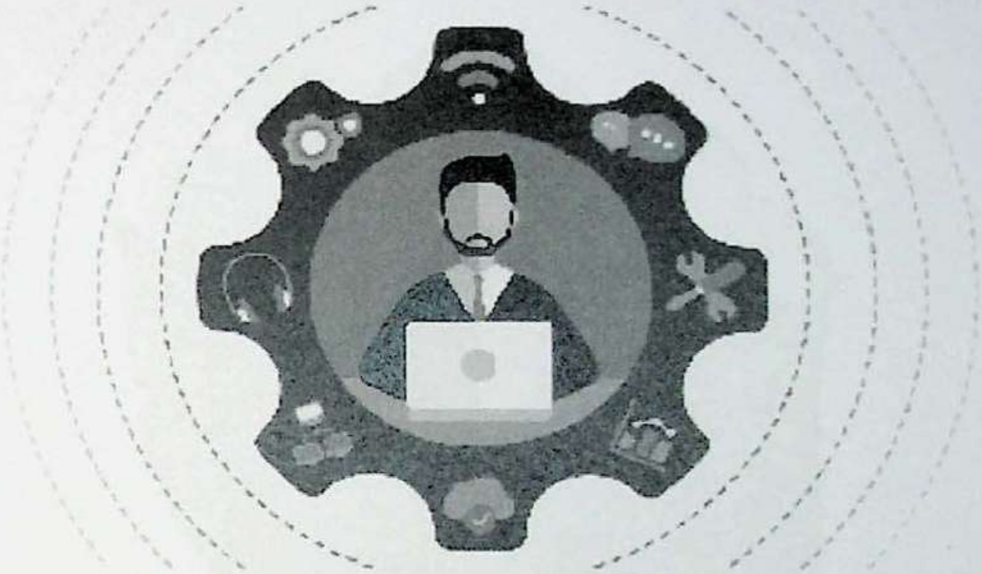
Compliance: Applicable to all government organizations

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

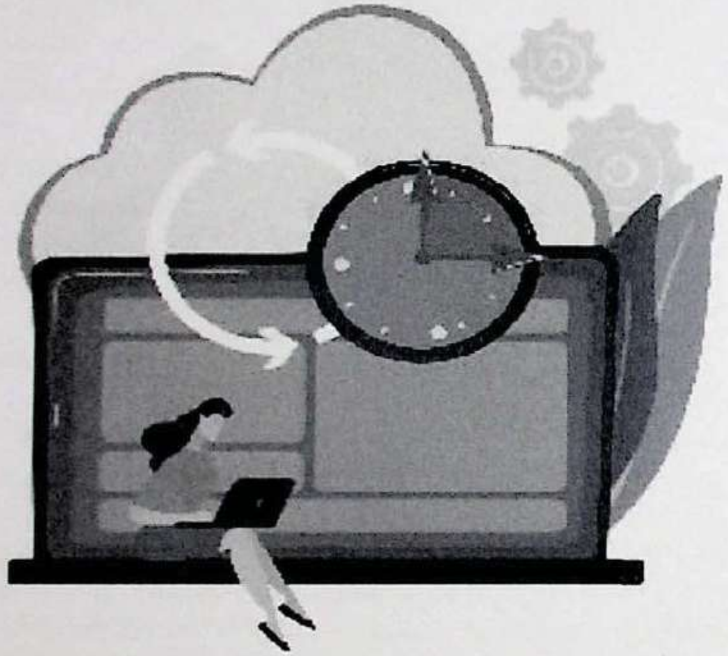
The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

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.

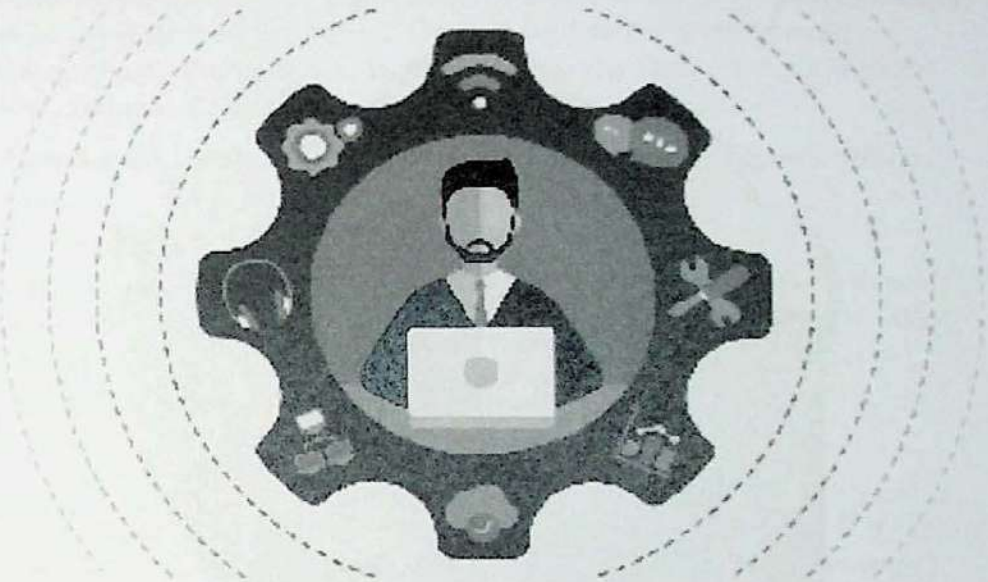
Backups containing information assets labeled as "Secret" and "Confidential" shall be stored as per the security requirements specified in the Assets Register.

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

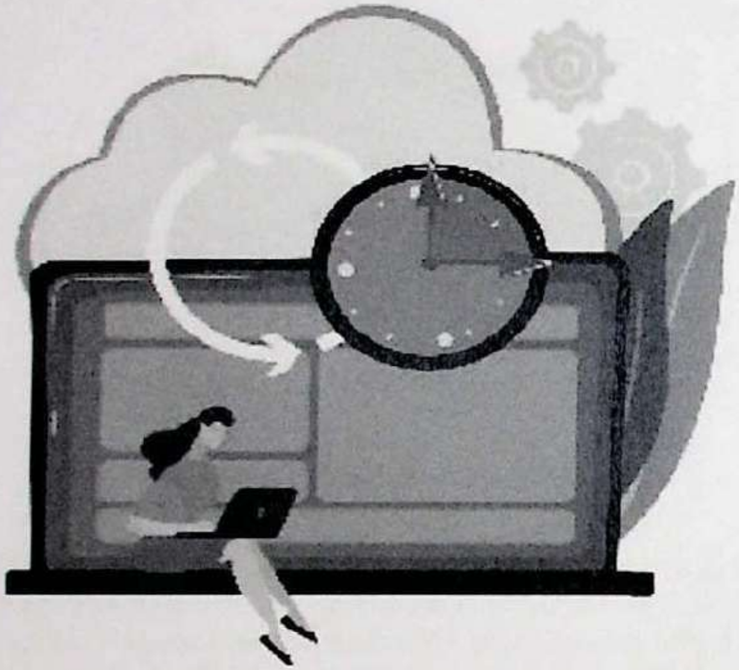
The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

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

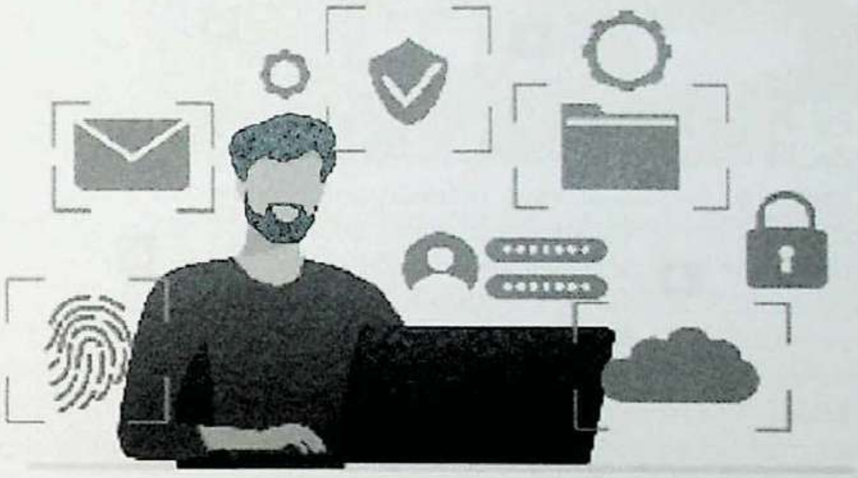
With the transition to working from home (or work from distant locations), there is an increase in information security threats. Therefore, employees shall adhere to "Information Security Guidelines for Working from Home" issued by Sri Lanka CERT which outline a set of security best practices when working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

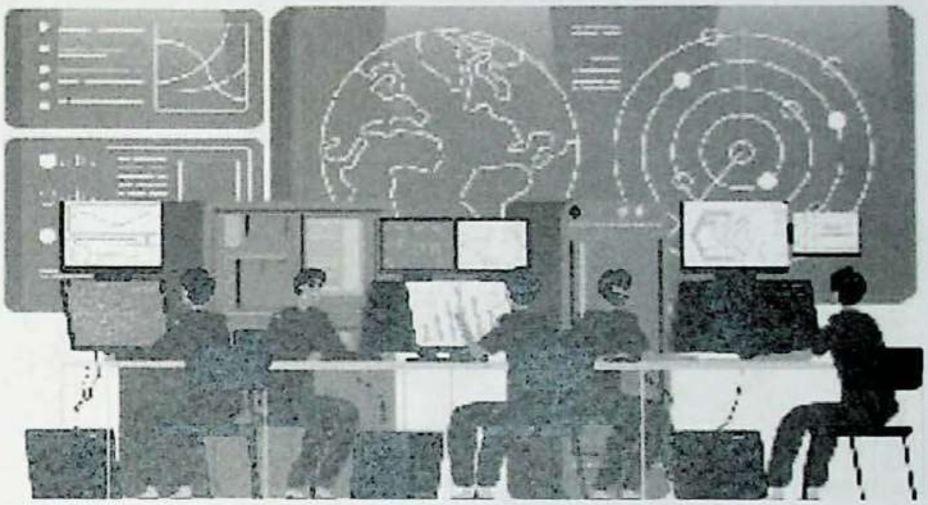
4.3.25 Policy on Change Management

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.

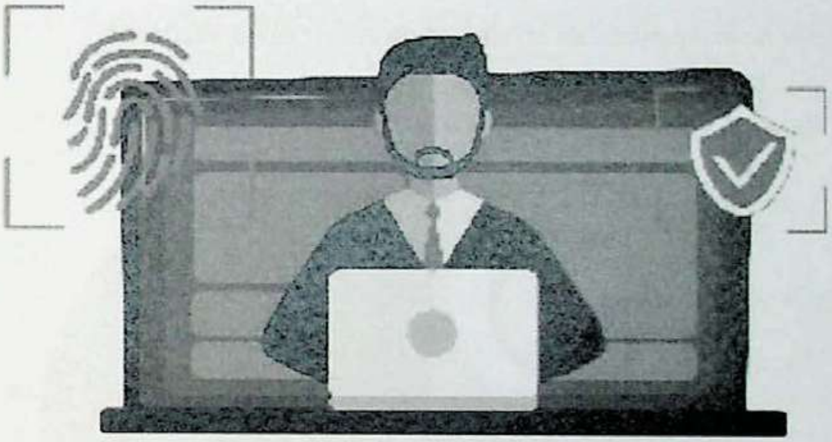
The organization shall maintain an Incident Register to record information related to the incidents. Incident Register shall contain the following information at a minimum: date and time of the incident, name and designation of the employee who reported the incident, description of the incident, nature 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
Information and Cyber Security Governance	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.	✓	✓
Identify Assets, Asset Owners and Risks	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.	✓	✓
Protect Assets	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
Detect Incidents	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.	✓	✓
Respond to Incidents	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.	✓	✓
Recover Normal Operations	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 Yes	Compliance No	Remarks
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			
Protect Assets					
Encryption	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			
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			

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 Yes	Compliance No	Remarks
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 Yes	Compliance No	Remarks
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? - 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 Yes	Compliance No	Remarks
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 Yes	Compliance No	Remarks
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

Antimalware	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).
Assets Classification	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.
Assets Custodian	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.
Assets Owner	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.
Availability of Information	Availability ensures timely and reliable access to and use of information.
Confidentiality of Information	Confidentiality refers to the assurance that information is not disclosed to unauthorized people and organizations.
Sensitive Information Assets	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.

Critical IT Assets	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.
Critical National Information Infrastructure (CNII)	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.
Digital Signature	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).
Encryption	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.
Government Organizations	The government organizations are the public authorities defined in the Right to Information Act No. 12 of 2016.
Information Security Controls	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.
Information Security Officer (ISO)	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.
Information Security Committee (ISC)	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

Private Cloud	Services offered over the Internet or over a private internal network to only select users. E.g. Lanka Government Cloud
Public Cloud	Cloud service available to anyone who wants to purchase them
Recovery Point Objective (RPO)	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.
Recovery Time Objective (RTO)	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.
Systems Hardening	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.
Virtual Private Network (VPN)	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.

2. Minimum Information Security Guidelines. Published by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through 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/NCSStrategy.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. } E/252/2026

ඔබේ අංකය
உமது இல.
Your No. } PS/LEG/CO/10/1/CoPF

දුරකථන අංක
தொலைபேசி இல.
Telephone No. } 2147888 2433967 2320800 2327919 2149001(2)

ඉලෙක්ට්‍රොනික් තැපැල
மின்னஞ்சல்
E-mail } administration@attorneygeneral.gov.lk

ෆැක්ස්
தொலைநகல்
Fax } 2436421

නීතිපති දෙපාර්තමේන්තුව
சட்டமா அதிபர் திணைக்களம்
ATTORNEY - GENERAL'S DEPARTMENT

P. O. Box No. } 502

කොළඹ 12.
கொழும்பு 12.
Colombo 12.

Annex 7

COMMITTEE 23 JUN 2026 PARLIAMENT OF SRI LANKA

15 June 2026

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

'TS OFFICE 8267 27 JUN 2026 CoPF PARLIAMENT

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.

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

4

Annex 8

මගේ අංකය
எனது இல.
My No. E/252/2026

ඔබේ අංකය
உமது இல.
Your No. PS/LEG/CO/10/1/CoPF

දුරකථන අංක
தொலைபேசி இல.
Telephone No. 2147888 2433967 2320800 2327919 2149001(2)

ඉලෙක්ට්‍රොනික් තැපැල
மின்னஞ்சல்
E-mail administration@attorneygeneral.gov.lk

ෆැක්ස්
தொலைநகல்
Fax 2436421

නීතිපති දෙපාර්තමේන්තුව
சட்டமா அதிபர் திணைக்களம்
ATTORNEY - GENERAL'S DEPARTMENT

තැ. පෙ. අංකය
அஞ்சல் பெட்டி
P. O. Box No. 502

කොළඹ 12.
கொழும்பு 12.
Colombo 12.

25 June 2026

ESTABLISHMENT OFFICE
01 JUL 2026
CO1
PARLIAMENT

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 15th 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 15th 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 15th 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.

Sgd./Nirmalan Wigneswaran
Deputy Solicitor General
for Attorney General

Oswald Perera
State Counsel

Annex 9

මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධ

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 / அலுவலகம் / Office: 011-2484500, 011-2484600, 011-2484700

ෆැක්ස් / தொலை நகல் / Fax: 011-2449823

වෙබ් අඩවිය / இணைய தளம் / Website: www.treasury.gov.lk

මගේ අංකය / எனது இல / My No: MF5/PA/04/2026

ඔබේ අංකය / உமது இல / Your No: PS/LEG/CO/10/1/CoPF

දිනය / திகதி / Date: 23.06.2026

Secretary,
Committee on Public Finance,
Parliament of Sri Lanka,
Sri Jayewardenepura, Kotte.

COMMITTEE OFFICE
23 JUN 2026
PARLIAMENT OF SRI LANKA

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.

Annex 10

මුදල්, ක්‍රමසම්පාදන සහ ආර්ථික සංවර්ධ

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 / அலுவலகம் / Office: 011 - 2484500, 011 - 2484600, 011 - 2484700
ෆැක්ස් / தொலைநகல் / Fax: 011 - 2449823
වෙබ් අඩවිය / இணையத்தளம் / Website: www.treasury.gov.lk

මගේ අංකය / எனது இல. / My No.: MF5/PA/04/2026
ඔබේ අංකය / உமது இல. / Your No.:
දිනය / திகதி / Date: 04April 2026

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 (FCMC)
   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 (FCMC) 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 Ditwah 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