அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் சைபர் பாதுகாப்பு கொள்கை

இலங்கை கணினி அவசர தயார்நிலை அணி
(இலங்கை சேர்ட்)
தொழில்நுட்ப அமைச்சு

அரசாங்க முகவராண்மைக்கான தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை – தமிழ் பதிப்பு

முதலாவது வெளியீடு

வெளியீட்டு திகதி: < >

அமைச்சரவையானது < > ஆம் திகதியிலிருந்து பயனுறுதியாகும் வகையில் இந்தக் கொள்கையினை அமுல்படுத்துவதற்கும் வலுவூட்டுவதற்குமான அதிகாரத்தினை வழங்கியுள்ளது.

ஆவண வகையீடு: பொது

வெளியீடு:

ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்ட பிரிவு
இலங்கை சேர்ட்
அறை 4-112, பண்டாரநாயக்க ஞாபகார்த்த சர்வதேச மாநாட்டு மண்டபம்,
பௌத்தலோக மாவத்தை, கொழும்பு 7
இலங்கை

தொலைபேசி: +94 11 269 1692, Fax: +94 11 269 1064
மின்னஞ்சல்: cert@cert.gov.lk
இணையதளம்: www.cert.gov.lk, www.onlinesafety.lk

© இலங்கை சேர்ட் 2022. அனைத்து உரிமைகளும் பாதுகாக்கப்பட்டவை.

பொருளடக்கம்

1 அறிமுகம்

1.1. இலங்கையில் உள்ள பல அரசாங்க நிறுவனங்கள் தற்போது டிஜிற்றல் முறைமைகள் மற்றும் உட்கட்டமைப்புகளின் நம்பகமான செயற்பாடுகளில் தங்கியுள்ளன. எவ்வாறாயினும், தீங்கிழைக்கும் நபர்கள் இத்தகைய டிஜிற்றல் அமைப்புகளைப் பயன்படுத்தி முக்கியமான தகவல் திருட்டு நடவடிக்கைகளிலும், நாளாந்த செயற்பாடுகளில் இடையூறு விளைவிப்பதிலும் ஈடுபட்டு வருவதுடன், நிறுவனங்களின் நற்பெயருக்கும் களங்கம் விளைவிக்கின்றனர். இது பொதுமக்களின் நம்பிக்கையையும் அரசாங்க நிறுவனங்களின் மீதான நம்பிக்கையையும் இழக்க வழிவகுப்பதுடன் தேசத்தின் பாதுகாப்பு, பொருளாதாரம், உள்ளக பாதுகாப்பு மற்றும் பொது மக்களின் நல்வாழ்விலும் ஆபத்தினை ஏற்படுத்துகின்றன.

1.2. இந்தத் தகவல் மற்றும் சைபர் பாதுகாப்பு அபாயங்களைத் திறம்பட நிவர்த்தி செய்வதற்கும், பல்வேறு அச்சுறுத்தல்களிலிருந்து அரசாங்க நிறுவனங்களின் தகவல், டிஜிற்றல் அமைப்புகள் மற்றும் உட்கட்டமைப்பு (இனி, தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள்) ஆகியவற்றைப் பாதுகாப்பதற்கும், இலங்கை கணினி அவசரநிலைத் தயார்நிலை அணியானது (Sri Lanka Computer Emergency Readiness Team) இலங்கை சேர்ட் நிறுவனம் (Sri Lanka CERT) என்றும் அழைக்கப்படுகிறது, இலங்கையின் இணையவெளியைப் பாதுகாப்பதற்கான ஆணையைக் கொண்டுள்ளதுடன், அரசாங்க நிறுவனங்களின் பயன்பாட்டிற்காக தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையை உருவாக்கியுள்ளது. நிறுவன மட்டத்தில் தகவல் மற்றும் சைபர் பாதுகாப்புத் திட்டத்தைச் செயற்படுத்துவதற்கான ஆபத்து அடிப்படையிலான அணுகுமுறையை இந்தக் கொள்கை வழங்குகிறது. சொத்துக்களைக் கண்டறிந்து பாதுகாப்பதற்கும், தகவல் பாதுகாப்பு சம்பவங்களை சரியான நேரத்தில் கண்டறிவதற்கும், சம்பவங்களுக்கு பதிலளிப்பதற்கும், திறமையான மற்றும் பயனுள்ள முறையில் சைபர் தாக்குதல்களில் இருந்து மீள்வதற்கும் நிறுவனங்கள் செயல்படுத்த வேண்டிய செயல்களின் தொகுப்பையும் இது வழங்குகிறது.

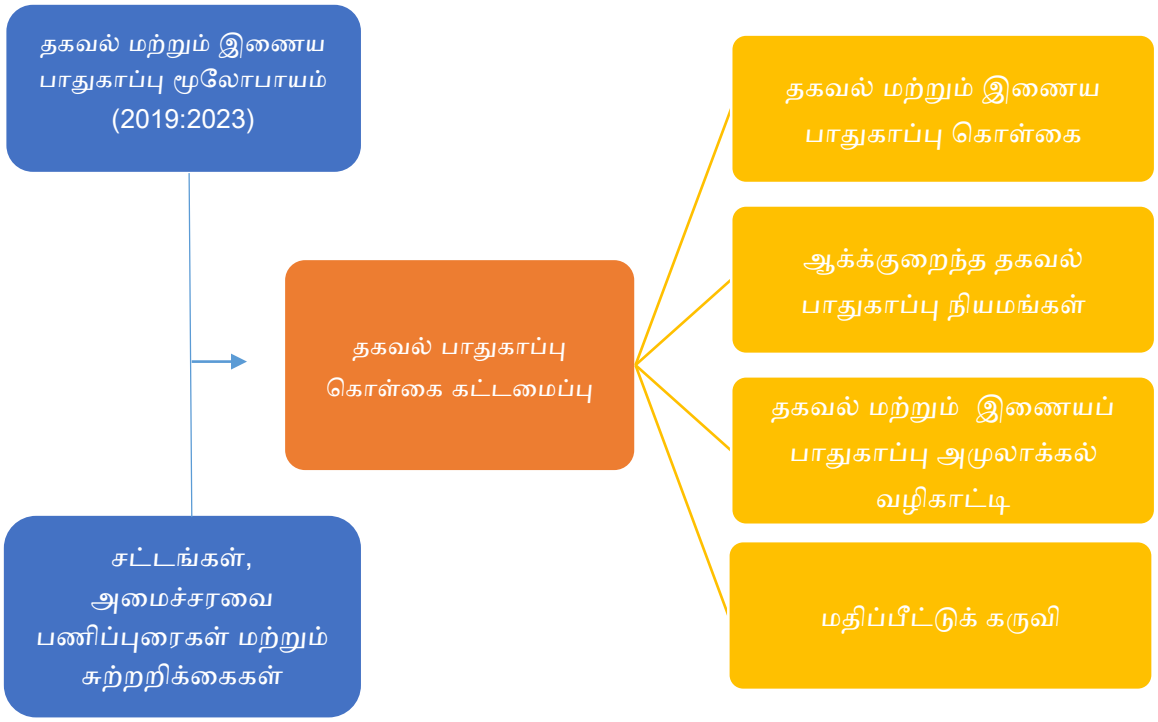
1.3. அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையானது இலங்கையின் தகவல் மற்றும் சைபர் பாதுகாப்பு மூலோபாயத்தின் (2019: 2023) நடைமுறைக்கு இணங்க உருவாக்கப்பட்டுள்ளது. இது சர்வதேச தரநிலைகள் மற்றும் தரநிலைப்படுத்தலுக்கான சர்வதேச அமைப்பு (International Organization for Standardization) மற்றும் அமெரிக்காவின் தேசிய தரநிலைகள் மற்றும் தொழில்நுட்ப நிறுவனம் (National Institute of Standards and

Technology) போன்ற சிறந்த நடைமுறைகளின் அடிப்படையில் உருவாக்கப்பட்டது, மேலும் அரசாங்கத்தின் தகவல் பாதுகாப்பு நிபுணர்கள் மற்றும் மூத்த அதிகாரிகளால் விரிவாக மீளாய்வு செய்யப்பட்டது.

1.4. 2016 ஆம் ஆண்டின் 12 ஆம் இலக்க தகவலுக்கான உரிமைச் சட்டத்தில் 'பகிரங்க அதிகாரசபை' என வரையறுக்கப்பட்டுள்ள அனைத்து அரசு நிறுவனங்களும் இந்தக் கொள்கைக்கு இணங்குதல் வேண்டும். அரசாங்க நிறுவனங்களின் தலைவர்கள் தங்கள் நிறுவனங்களுக்குள் பாதுகாப்பான மற்றும் திறமையான சேவையை வழங்குவதை உறுதி செய்வதற்கான கொள்கையை செயற்படுத்துவதற்கு பொறுப்பாகவும் இருக்க வேண்டும். இலங்கை சேர்ட் நிறுவனம் கொள்கையை நடைமுறைப்படுத்துவதில் அனைத்து அரசாங்க நிறுவனங்களுக்கும் சிபாரிசுகளை எளிதாக வழங்குவதுடன், வருடாந்த அடிப்படையில் கொள்கையை நடைமுறைப்படுத்துவதில் நிறுவனங்களின் செயல்திறனை மதிப்பீடு செய்யும்.

2. தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை கட்டமைப்பு

2.1. தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கைக் கட்டமைப்பானது, தகவல் மற்றும் சைபர் பாதுகாப்புத் திட்டங்களைத் திறமையான மற்றும் பயனுள்ள முறையில் செயற்படுத்துவதற்கு அரசாங்க நிறுவனங்களுக்குத் தேவையான வழிகாட்டுதல் உள்ளடக்கத்தை அறிமுகப்படுத்துகிறது. இது அரசாங்க நிறுவனங்களுக்கான (அ) தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை (Information and Cyber Security Policy), (ஆ) குறைந்தபட்ச தகவல் பாதுகாப்புத் தரநிலைகள் (Minimum Information Security Standards), (இ) தகவல் மற்றும் சைபர் பாதுகாப்பு நடைமுறைப்படுத்தல் வழிகாட்டி (Information and Cyber Security Implementation Guide), மற்றும் (ஈ) தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையின் அமுலாக்கத்தைக் கண்காணித்து மதிப்பாய்வு (Monitoring and Evaluation Methodology) செய்வதற்கான ஒரு முறை ஆகியவற்றினை உள்ளடக்குகின்றது. உரு - 1 ஆனது தகவல் பாதுகாப்பு கொள்கை கட்டமைப்பின் கண்ணோட்டத்தினை வழங்குகின்றது.



உரு 1 –: தகவல் பாதுகாப்பு கொள்கை கட்டமைப்பு

2.2. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை கட்டமைப்பில் பின்வருவன உள்ளடங்குகின்றன:

அ. தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை) Information and Cyber Security Policy :(கொள்கை கட்டமைப்பின் முக்கிய அங்கமாக தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை விளங்குகின்றது. இது அரசாங்க நிறுவனங்கள் இணங்க வேண்டிய கொள்கைகளின் தொகுப்பை வழங்குகிறது, அத்தியாவசிய கட்டுப்பாடுகளை கோடிட்டுக் காட்டுவதுடன் தகவல் பாதுகாப்பு நிகழ்வுகளிலிருந்து தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதில் அரசாங்க நிறுவனங்களுக்கு வழிகாட்டுதலையும் வழங்குகிறது.

ஆ. குறைந்தபட்ச தகவல் பாதுகாப்பு நியமங்கள் (Minimum Information Security Standards): அரசு நிறுவனங்களால் கடைபிடிக்கப்படும் தகவல் பாதுகாப்பு கட்டுப்பாடுகளின் குறைந்தபட்ச ஏற்றுக்கொள்ளக்கூடிய நியமங்களை இந்த ஆவணம் கோடிட்டுக் காட்டுகிறது. இலங்கை சேர்ட்டினது www.onlinesafety.lk இணையத்தளத்தில் உசாத்துணைக்காக குறைந்தபட்ச தகவல் பாதுகாப்பு நியமங்கள் உள்ளன.

இ. தகவல் மற்றும் சைபர் பாதுகாப்பு அமலாக்க வழிகாட்டி (Information and Cyber Security Implementation Guide): இது கொள்கையை செயல்படுத்துவதில் குறிப்பிட்ட விவரங்கள் தேவைப்படும் ஊழியர்கள் மற்றும் பங்குதாரர்களுக்கு விரிவான வழிமுறைகளை வழங்குகிறது. இந்த வழிகாட்டியில் தகவல் பாதுகாப்பு நிருவாகக் கட்டமைப்பை நிறுவுதல், சொத்துக்களின் வகைப்பாடு, இடர் மேலாண்மை, சொத்துக்களின் பாதுகாப்பு, பேரிடர் மீட்பு மற்றும் காப்புப் பிரதிகள், சம்பவங்களை நிருவகித்தல், அடையாளம் மற்றும் அணுகல் கட்டுப்பாடு மற்றும் பலவற்றின் வழிமுறைகள் உள்ளன. இந்த ஆவணம் இலங்கை சேர்ட் நிறுவனத்தின் www.onlinesafety.lk எனும் இணையத்தளத்தில் உசாத்துணைக்காகக் கிடைக்கிறது.

ஈ. கண்காணிப்பு மற்றும் மதிப்பீட்டு முறை (Monitoring and Evaluation Methodology): இது கொள்கையை ஏற்றுக்கொள்வதில் அரசு நிறுவனங்களின் தயார்நிலையை மதிப்பிடுவதற்கும், அதன் செயலாக்கத்தின் முன்னேற்றத்தை மதிப்பிடுவதற்கும் மதிப்பீட்டு அளவுகோல்களை வழங்குகிறது. இலங்கை சேர்ட் நிறுவனம், இந்த ஆவணத்தின் 6 ஆவது பிரிவில் குறிப்பிடப்பட்டுள்ள வழிமுறைகளைப் பயன்படுத்தி, அரசாங்க நிறுவனங்களின்

தகவல் மற்றும் சைபர் பாதுகாப்பு நடவடிக்கைகளின் முதிர்ச்சியை முன் வரையறுக்கப்பட்ட காலக்கெடுவிற்குள் மதிப்பீடு செய்கிறது.

உ. தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை கட்டமைப்பானது தொடர்புடைய சட்டங்கள் மற்றும் ஒழுங்குமுறைகள், இலங்கையின் தகவல் மற்றும் சைபர் பாதுகாப்பு மூலோபாயம், இ-அரசாங்க கொள்கைகள் மற்றும் அமைச்சரவை உத்தரவுகளால் நிருவகிக்கப்படுகிறது.

3. தகவல் மற்றும் சைபர் பாதுகாப்பு கொள்கை

3.1அறிமுகம்

3.1.1. தகவல் மற்றும் சைபர் பாதுகாப்பு என்பது தகவல்களின் ரகசியத்தன்மை (Confidentiality), நேர்மைத்தன்மை (Integrity) மற்றும் கிடைக்கும் தன்மையை (Availability) உறுதி செய்வதற்காக அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, மாற்றுதல், மற்றும் அழித்தல் ஆகியவற்றிலிருந்து தகவல் சொத்துக்களைப் பாதுகாப்பதைக் குறிக்கிறது. சைபர் தொழில்நுட்பம் அல்லது ஏனைய வழிகளைப் பயன்படுத்தி தனிநபர்களின் தீங்கிழைக்கும் செயல்களிலிருந்து தகவல் சொத்துக்களைக் கொண்ட தகவல் சொத்துக்களைப் பாதுகாப்பது மற்றும் வெள்ளம் மற்றும் தீ போன்ற பிற இயற்கை பேரழிவுகளிலிருந்து சொத்துக்களைப் பாதுகாப்பது ஆகியவை இதில் உள்ளடங்கும்.

3.1.2. இந்தச் சூழலில், தனிநபர்களின் தீங்கிழைக்கும் செயல்பாடுகள் மற்றும் இயற்கை பேரிடர்களால் ஏற்படும் சேதங்களிலிருந்து தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாக்க அரச நிறுவனங்கள் பின்பற்ற வேண்டிய விதிகள் மற்றும் வழிகாட்டுதல்களின் தொகுப்பை அறிமுகப்படுத்துவதே தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையின் முக்கிய நோக்கமாகும்.

3.1.3. கொள்கையின் மற்ற நோக்கங்கள்

அ. பொதுத் துறை முழுவதும் பொதுவான தகவல் மற்றும் சைபர் பாதுகாப்பு தரநிலையை நிறுவுதல்,

ஆ.தகவல் அமைப்புகள் மற்றும் டிஜிற்றல் உட்கட்டமைப்பின் வடிவமைப்பு, செயல்படுத்தல், பயன்பாடு மற்றும் செயல்பாடுகள் தொடர்பான பாதுகாப்பு தரநிலைகள், விதிகள் மற்றும் செயல்முறைகளை கட்டாயப்படுத்துவதன் மூலம் தகவல் மற்றும் சைபர் பாதுகாப்பு நிகழ்வுகளுக்கு அரசாங்க நிறுவனங்களின் பின்னடைவை வலுப்படுத்துதல்,

இ.தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களை சரியான நேரத்தில் கண்டறிவதற்கான ஒரு பொறிமுறையை நிறுவுதல், நிறுவனங்களுக்கு இதுபோன்ற சம்பவங்களின் தாக்கத்தை குறைத்தல் மற்றும் இதுபோன்ற

சம்பவங்களால் பாதிக்கப்பட்ட எந்தவொரு திறன்கள் அல்லது சேவைகளை திறமையாக மீட்டெடுக்கவும், மற்றும்

ஈ. தகவல் மற்றும் சைபர் பாதுகாப்பின் விதிகள், சிறந்த நடைமுறைகள், தரநிலைகள் மற்றும் செயல்முறைகள் குறித்து ஊழியர்களுக்குக் கற்பித்தல் மற்றும் நிறுவனத்தின் பாதுகாப்பு நிலை குறித்த ஊழியர்களின் நம்பிக்கையை உருவாக்குதல்

3.1.4. இந்தக் கொள்கை எளிய மொழியில் எழுதப்பட்டுள்ளது. அனைத்து ஊழியர்களும் தொடர்புடைய மூன்றாம் தரப்பு சேவை வழங்குநர்களும், அவர்கள் பாடம் பற்றிய அறிவைப் பொருட்படுத்தாமல், கொள்கையைச் செயல்படுத்துவது தொடர்பாக அவர்களின் பொறுப்புகள் மற்றும் கடமைகளைப் புரிந்து கொள்ள முடியும்.

3.1.5 நல்ல தகவல் பாதுகாப்பு நடைமுறைகளை ஆதரிப்பதற்கு அரசு நிறுவனங்களுக்கு தொழில்நுட்ப மற்றும் பாதுகாப்பு வழிகாட்டுதலை வழங்க இந்த ஆவணம் அவ்வப்போது புதுப்பிக்கப்படும்.

3.2 கொள்கையின் நோக்கம்

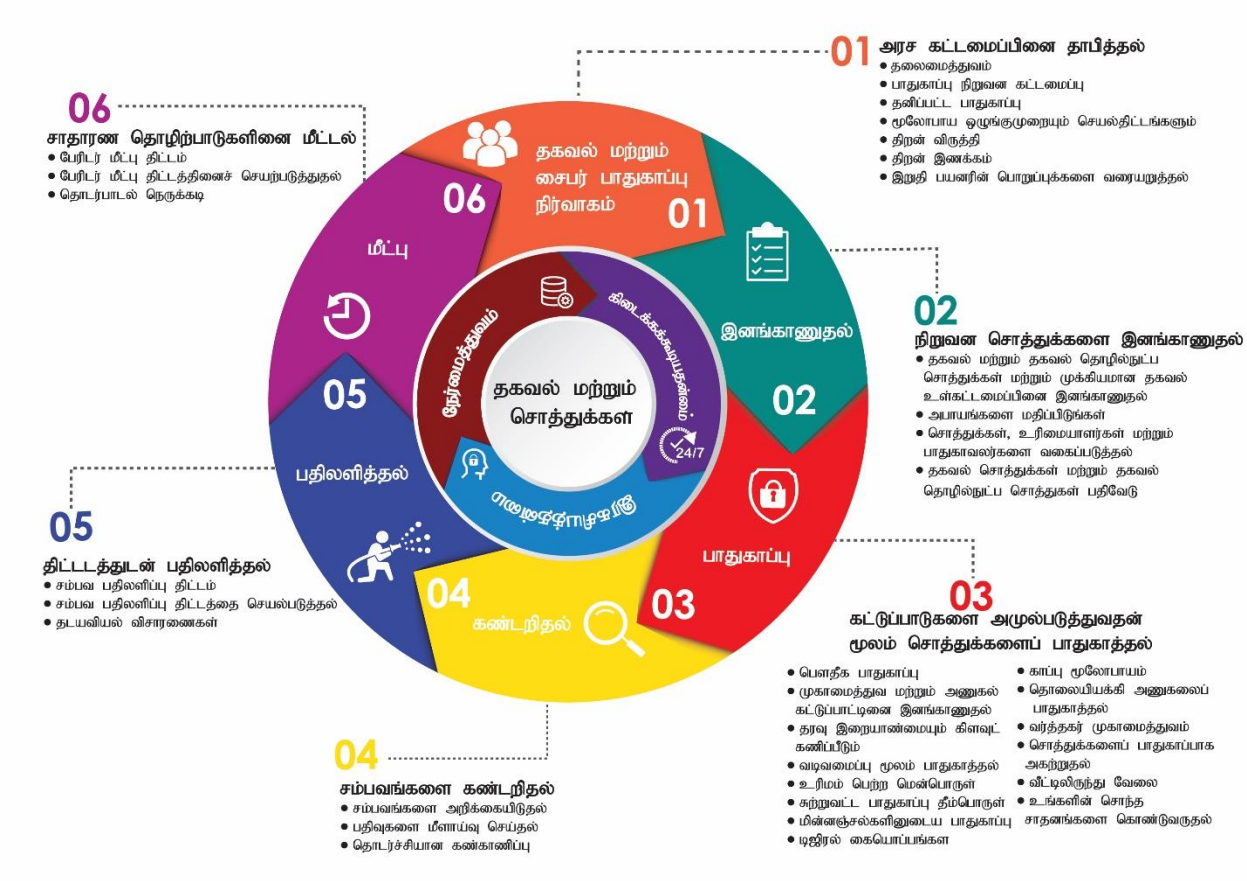
3.2.1 இந்தக் கொள்கையானது அமைச்சகங்கள், துறைகள், பொதுக் கூட்டுத்தாபனங்கள், உள்ளூராட்சி நிறுவனங்கள் மற்றும் 2016 ஆம் ஆண்டின் 12 ஆம் இலக்க தகவலுக்கான உரிமைச் சட்டத்தில் 'பகிரங்க அதிகாரசபை' என வரையறுக்கப்பட்டுள்ள எந்தவொரு அரசு நிறுவனத்திற்கும் பொருந்தும். இந்தக் கொள்கையானது அரசாங்க நிறுவனங்களின் சார்பில் தகவல் தொழில்நுட்ப சேவைகளை நிருவகிக்கும் உரிய மூன்றாம் தரப்பு சேவை வழங்குநர்களுக்கும் எற்புடையதாதல் வேண்டும்.

3.2.2. இங்கு வழங்கப்பட்ட கொள்கைகள் இரண்டு நிலைகளின் அடிப்படையில் உருவாக்கப்பட்டுள்ளன. அவை, (அ) அனைத்து அரசு நிறுவனங்களுக்கும் பொருந்தும் கொள்கைகள், மற்றும் (ஆ) முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கு பொருந்தும் கொள்கைகள். முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்கள் இந்தக் கொள்கையில் குறிப்பிடப்பட்டுள்ள அனைத்து கொள்கைகளுக்கும் இணங்குதல் வேண்டும். ஏனைய நிறுவனங்கள் அனைத்து அரசு நிறுவனங்களுக்கும் ஏற்புடையதான

கொள்கைகளுடன் இணங்கி நடத்தல் வேண்டும். எவ்வாறாயினும், சிறந்த பாதுகாப்பிற்காக முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கு பொருந்தக்கூடிய கொள்கைகளுக்கு இணங்க ஏனைய நிறுவனங்களுக்கு பரிந்துரைக்கப்படுகிறது.

3.2.3 முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்கள், தேசிய பாதுகாப்பு, நிர்வாகம், பொருளாதாரம், சுகாதாரம் மற்றும் சமூக நல்வாழ்வு ஆகியவற்றில் பலவீனமான தாக்கத்தை ஏற்படுத்தும் தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை பராமரிக்கும் நிறுவனங்களாக வரையறுக்கப்படுகின்றன. முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களின் பட்டியல் இலங்கை சேர்ட் நிறுவனத்தினால் வெளியிடப்படும்.

3.2.4 இந்தக் கொள்கையானது தகவல் மற்றும் சைபர் பாதுகாப்பு நிருவாகக் கோட்பாடுகள் மற்றும் அமெரிக்காவின் தேசிய தரநிலைகள் மற்றும் தொழில்நுட்ப நிறுவனத்தினால் முன்மொழியப்பட்ட பல ஒரே நேரத்தில் மற்றும் தொடர்ச்சியான தகவல் பாதுகாப்பு செயல்பாடுகளின் அடிப்படையில் உருவாக்கப்பட்டது. இந்த செயற்பாடுகளில் (அ) நிறுவனத்தின் தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை அடையாளம் காணுதல் (உதாரணம். தரவு, தகவல், கணினிகள் மற்றும் பிற டிஜிற்றல் உட்கட்டமைப்பு), (ஆ) சொத்துக்களைப் பாதுகாக்க தேவையான நடவடிக்கைகளை எடுத்தல், (இ) தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களைக் கண்டறிதல், (ஈ) சம்பவங்களுக்கு பதிலளிப்பது, மற்றும் (இ) ஒரு சம்பவத்தால் பாதிக்கப்பட்ட சேவையை மீட்டெடுத்தல். அரசாங்க நிறுவனத்திற்குள் தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான நடவடிக்கைகளை இயக்குவதற்கும் கட்டுப்படுத்துவதற்கும் தகவல் மற்றும் சைபர் பாதுகாப்பு நிர்வாக பொறிமுறையும் இந்தக் கொள்கையில் அடங்கும். தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாக்க அரசு நிறுவனங்கள் பின்பற்ற வேண்டிய செயற்பாடுகளை படம் 2 காட்டுகிறது.



உரு – 2 – தகவல் மற்றும் இணைய பாதுகாப்புக்கான படிமுறைகள்

3.2.5 தகவல் பாதுகாப்பு செயல்பாடுகளின் அடிப்படையில் உருவாக்கப்பட்டுள்ள 3.2.4 இல் குறிப்பிடப்பட்டுள்ளபடி, இந்தக் கொள்கையைச் செயல்படுத்துவதன் மூலம் சொத்துக்களைப் பாதுகாப்பதற்காக ஒரு நிறுவனத்தால் எடுக்கப்படும் நடவடிக்கைகள் கீழே விவரிக்கப்பட்டுள்ளன.

அ. தகவல் மற்றும் சைபர் பாதுகாப்பு நிர்வாகம் (Information and Cyber Security Governance) : தகவல் மற்றும் சைபர் பாதுகாப்பு நிர்வாகம் என்பது பொதுவாக ஒரு நிறுவனத்தின் தகவல் மற்றும் சைபர் பாதுகாப்பை இயக்கும் மற்றும் கட்டுப்படுத்தும் நிர்வாக பொறிமுறையை குறிப்பிடுகின்றது. தகவல் மற்றும் சைபர் பாதுகாப்பு நிருவாகத்தை செயற்படுத்த, நிறுவனங்கள் ஒரு பாதுகாப்பு நிறுவன கட்டமைப்பை நிறுவுதல் வேண்டும் மற்றும் தகவல் பாதுகாப்பிற்கு பொறுப்பு வாய்ந்த அதிகாரிகளை நியமித்தலும் வேண்டும், அத்தகைய அதிகாரிகளின் திறனை மேம்படுத்துதல், நிறுவனங்களின் தகவல் மற்றும் சைபர் பாதுகாப்பு நோக்கங்களை வரையறுத்தல், செயல் திட்டங்களை

உருவாக்குதல். மற்றும் தொடர்புடைய நடவடிக்கைகளுக்கான ஆதாரங்களை ஒதுக்குதல். (பிரிவு 4.1 ஐப் பார்க்கவும்).

ஆ. செயற்பாடுகளை அடையாளம் காணுதல் (Identify Function): தரவு, தகவல், கணினிகள், அமைப்புகள் மற்றும் டிஜிற்றல் உட்கட்டமைப்பு போன்ற சொத்துக்களை அடையாளம் காணவும், அந்த சொத்துக்களுடன் தொடர்புடைய அபாயங்களைக் கண்டறிந்து திறம்பட நிருவகிக்கவும் இது அரசாங்க நிறுவனங்களுக்கு உதவுகிறது (பிரிவு 4.2 ஐப் பார்க்கவும்).

இ. பாதுகாப்பு செயற்பாடு (Protect Function): தடையற்ற சேவைகளை வழங்குவதற்காக தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பை உறுதி செய்ய தேவையான பொருத்தமான கட்டுப்பாடுகளை பாதுகாக்கும் செயல்பாடு கோடிட்டுக் காட்டுகிறது. பாதுகாப்புச் செயல்பாட்டிற்கு இணங்க, நிறுவனங்கள் சொத்துக்களுக்கான பயனர் அணுகலை நிருவகித்தல், ஃபயர்வால்கள் மற்றும் ஆண்டிமால்வேர் மென்பொருளை நிறுவுதல், அமைப்புகளின் தணிக்கைகளை நடத்துதல், காப்புப் பிரதி உத்தியை நிறுவுதல் மற்றும் பிரிவு 4.3 இல் குறிப்பிடப்பட்டுள்ள கொள்கைகளைச் செயற்படுத்துதல் போன்ற பொருத்தமான கட்டுப்பாடுகளை செயற்படுத்த வேண்டும்.

ஈ. கண்டறிதல் செயற்பாடு (Detect Function): கண்டறிதல் செயற்பாடு, சரியான நேரத்தில் தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்கள் நிகழ்வதை அடையாளம் காண தேவையான செயற்பாடுகளை வரையறுக்கிறது. கணனிகள் மற்றும் தொடர்புடைய சாதனங்கள் மூலம் உருவாக்கப்படும் பதிவுகளை ஆய்வு செய்ய நிறுவனங்கள் தகுந்த கருவிகளைப் பயன்படுத்தி சம்பவங்களை திறமையான முறையில் கண்டறிதல் வேண்டும் (பிரிவு 4.4 ஐப் பார்க்கவும்).

உ. பதிலளிக்கும் செயற்பாடு (Respond Function): கண்டறியப்பட்ட சம்பவத்திற்கு பதிலளிக்கும் வகையில் எடுக்கப்பட வேண்டிய செயல்களை மறுமொழி செயல்பாடு வரையறுக்கிறது. ஒரு சம்பவத்திற்கு திறமையான மற்றும் பயனுள்ள முறையில் பதிலளிப்பதற்காக, பிரிவு 4.5 இல் வரையறுக்கப்பட்டுள்ளபடி நிறுவனங்கள் ஒரு சம்பவ மறுமொழி திட்டத்தை உருவாக்கி செயற்படுத்தல் வேண்டும்.

ஊ. மீட்டெடுக்கும் செயற்பாடு (Recover Function): தகவல் மற்றும் சைபர் பாதுகாப்புச் சம்பவத்தால் பாதிக்கப்பட்ட எந்தத் திறன்கள் அல்லது சேவைகளை

மீட்டெடுப்பதற்கான பொருத்தமான செயற்பாடுகளை மீட்டெடுப்பு செயற்பாடு அடையாளம் காட்டுகின்றது. மீட்புச் செயற்பாட்டிற்கு இணங்க, நிறுவனம் பேரழிவு மீட்புத் திட்டத்தை உருவாக்கி, ஒரு சம்பவத்தின் போது இயல்பான செயற்பாடுகளை மீட்டெடுப்பதற்கான திட்டத்தை செயற்படுத்துதல் வேண்டும் (பிரிவு 4.6 ஐப் பார்க்கவும்).

4. கொள்கை கூற்றுக்கள்

அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையானது ஆறு முக்கிய கொள்கை விடயப் பரப்புக்களைக் கொண்டுள்ளது, அதாவது (அ) நிறுவனத்திற்குள் ஒரு தகவல் மற்றும் சைபர் பாதுகாப்பு நிருவாக அமைப்பை நிறுவுதல், (ஆ) சொத்துக்கள், சொத்து உரிமையாளர்கள், பாதுகாவலர்கள் மற்றும் இடர்களை அடையாளம் காணுதல், (இ) சொத்துக்களைப் பாதுகாத்தல், (ஈ) தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களை அடையாளம் காணுதல் (உ) பாதுகாப்புச் சம்பவங்களுக்குப் பதிலளிப்பது, மற்றும் (ஊ) ஒரு சம்பவத்தால் சீர்குலைந்துபோன செயற்பாடுகளை மீட்டெடுத்தல். மேற்கண்ட ஆறு தொடர்பாக அரசு நிறுவனங்கள் கடைப்பிடிக்க வேண்டிய கொள்கை விடயப் பரப்புக்கள் கீழே கொடுக்கப்பட்டுள்ளன

4.1. தகவல் பாதுகாப்பு நிருவாக முறைமை

தகவல் பாதுகாப்பு நிருவாக முறைமையானது நிறுவனமொன்றில் தகவல் பாதுகாப்பினை நெறிமுறைப்படுத்துவதற்கும் கட்டுப்படுத்துவதற்குமான பொறிமுறையொன்றினை முன்மொழிகின்றது. இது தகவல் பாதுகாப்பு நடவடிக்கைகள் உரிய முறையில் நிருவகிக்கப்படுவதனை உறுதி செய்வதற்குத் தேவையான தலைமைத்துவம் மற்றும் பொறுப்புக் கூறல் கட்டமைப்பு குறித்து விதித்துரைக்கின்றது. தகவல் மற்றும் சைபர் பாதுகாப்புச் செயல்பாடுகளை நிறுவனத்தின் தொலைநோக்குப் பார்வை மற்றும் நோக்கத்துடன் சீரமைக்க வேண்டியதன் அவசியத்தையும், பொறுப்பான மற்றும் பொறுப்புள்ள அதிகாரிகளின் திறன் மேம்பாட்டிற்கான தேவை, பயனுள்ள தகவல் மற்றும் சைபர் பாதுகாப்புத் திட்டமிடல் மற்றும் இந்தக் கொள்கையை ஏற்றுக்கொள்ளும் அரசு நிறுவனங்களின் முக்கியத்துவம் ஆகியவற்றையும் இது எடுத்துக்காட்டுகிறது.

4.1.1. தலைமைத்துவம் மீதான கொள்கை

நிறுவனத்தின் தலைமைத்துவமானது தாபனத்தின் தகவல் பாதுகாப்பு நடவடிக்கைகளுக்கான தலைமைத்துவத்தினை வழங்குவதுடன் தாபனத்தின் தகவல் மற்றும் சொத்துக்களைப் பாதுகாப்பதற்கான இறுதிப் பொறுப்புக்கும் பொறுப்புக் கூறலுக்கும் பொறுப்பு வாய்ந்ததாகும்.

நிறுவனத்தின் தலைமைத்துவமானது நிறுவனத்தின் நோக்கு மற்றும் செயற்பணியினை ஆதரிக்கும் தகவல் பாதுகாப்பு இலக்குகள் மற்றும் முன்னுரிமைகளினை அமைக்கும் நிறுவனத்தின் தகவல் மற்றும் சைபர் பாதுகாப்பு நிகழ்ச்சித் திட்டமொன்றினைத் தாபிப்பதுடன் தகவல் பாதுகாப்பு நடவடிக்கைகளினை ஆதரவளிப்பதற்கும் அதனை வெற்றிகரமாக முன்னெடுப்பதற்கும் கிடைக்கக்கூடிய மூலவளங்களையும் உறுதி செய்யும்.

பயனர்கள் தகவல் பாதுகாப்புக் கொள்கைகள் மற்றும் வழிகாட்டுதல்களுக்கு இணங்க, அவர்கள் பயன்படுத்தும் தகவல் மற்றும் அமைப்புகளைப் பாதுகாப்பதில் முனைப்புடன் செயற்படும் நிறுவனத்திற்குள் ஒரு தகவல் பாதுகாப்பு கலாச்சாரத்தை உருவாக்குவதற்கான தலைமைத்துவத்தை நிறுவனத்தின் தலைவர் வழங்குவார்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.2. பாதுகாப்பு நிறுவன கட்டமைப்பு மீதான கொள்கை

நிறுவனமானது தகவல் பாதுகாப்பு நிறுவனசார் கட்டமைப்பொன்றினைத் தாபித்தல் வேண்டும். அமைப்பின் தகவல் பாதுகாப்பு நடவடிக்கைகளை இயக்கவும், வழிகாட்டவும் மற்றும் நிர்வகிக்கவும், தகவல் மற்றும் சைபர் பாதுகாப்பு மீறல்கள், ஊடுருவல்கள் மற்றும் குறுக்கீடுகளுக்கு எதிராக நிறுவனத்தைப் பாதுகாக்கவும் இந்த அமைப்பு அவசியம்.

பயனுறுதி வாய்ந்த தகவல் பாதுகாப்பு நிறுவனசார் கட்டமைப்பானது (அ) தகவல் பாதுகாப்பு உத்தியோகத்தர், (ஆ) பிரதான புத்தாக்க உத்தியோகத்தர் மற்றும் (இ) (பிரதான) உள்ளக கணக்காய்வாளர் போன்ற பிரதான பதவிகளினை உள்ளடக்குகின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

(அ) தகவல் பாதுகாப்பு உத்தியோகத்தர் தொழிற்பாடு மீதான கொள்கை

நிறுவனமானது தகவல் பாதுகாப்பு உத்தியோகத்தர் ஒருவரை நியமித்தல் வேண்டும். அத்தகைய தகவல் பாதுகாப்பு உத்தியோகத்தரானவர், நிறுவன தலைமை அதிகாரி உடன் கலந்தாலோசித்து நிறுவனத்தின் தகவல் பாதுகாப்பு நோக்கங்களை நிறுவுதல், தகவல் பாதுகாப்பு அபாயங்களை நிருவகித்தல் மற்றும் தகவல் பாதுகாப்பு மூலோபாயங்கள், கொள்கைகள் மற்றும் செயல்திட்டங்களைச் செயல்படுத்துதல் ஆகியவற்றின் மூலம் நிறுவனத்தின் தகவல் மற்றும் சொத்துக்கள் போதுமான அளவு பாதுகாக்கப்படுவதை உறுதி செய்யும் வகையில் ஒரு சிரேஷ்ட தரத்திலான உத்தியோகத்தராக இருத்தல் வேண்டும். தகவல் பாதுகாப்பு உத்தியோகத்தரின் தொழிற்பாடானது த.தொ. தொழிற்பாட்டிலிருந்து வேறுபட்டதாக இருத்தல் வேண்டும் என்பதுடன் தகவல் பாதுகாப்பு உத்தியோகத்தரானவர் தகவல் பாதுகாப்பு தொடர்பான நடவடிக்கைகள் தொடர்பில் நிறுவனத்தின் தலைவரிற்கு நேரடியாக அறிக்கையிடுதல் வேண்டும்.

இணக்கம்:அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

(ஆ) பிரதான புத்தாக்க உத்தியோகத்தரின்தொழிற்பாடு மீதான கொள்கை

பிரதான புத்தாக்க உத்தியோகத்தர் (அல்லது தகவல் தொழில்நுட்ப விடயத்துக்குப் பொறுப்பான அலுவலர்) தகவல் மற்றும் ஏனைய தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதற்கும், நிறுவனத்தின் வர்த்தகச் செயல்பாடுகளின் தொடர்ச்சியை உறுதி செய்வதற்கும் தகுந்த நடவடிக்கைகளை எடுப்பதற்குப் பயிற்றுவிக்கப்பட்டு பொறுப்புகள் வழங்கப்படுதல் வேண்டும்.

குறிப்பு: தகவல் பாதுகாப்பு உத்தியோகத்தரினை நியமிப்பதற்குத் தகுந்த அதிகாரி இல்லாத நிறுவனத்தில், பிரதான புத்தாக்க உத்தியோகத்தர் அல்லது தகவல் தொழில்நுட்ப விடயத்திற்குப் பொறுப்பான உத்தியோகத்தர் ஒருவர் தகவல் பாதுகாப்பு உத்தியோகத்தரின் பாத்திரத்தை வகிக்க அதிகாரம் அளிக்கப்படுவார்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

(இ) (பிரதான) உள்ளக கணக்காய்வாளரின் தொழிற்பாடு மீதான கொள்கை

(பிரதான) உள்ளக கணக்காய்வாளருக்கு, நிறுவனத்தின் தகவல் பாதுகாப்பு கணக்காய்வுகளை ஆரம்பித்தல் மற்றும் மேற்பார்வை செய்தல், தகவல் மற்றும் சைபர் பாதுகாப்பு கொள்கையை ஏற்றுக்கொள்வதன் முன்னேற்றத்தை மதிப்பிடுதல் மற்றும் தகவல் பாதுகாப்பு தொடர்பான கண்டுபிடிப்புக்களை கணக்காய்வு மற்றும் முகாமைத்துவக் குழுவுக்கு (Audit and Management Committee) அறிக்கையிடுதல் போன்ற பொறுப்புகள் உரித்தளிக்கப்பட்டுள்ளன.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.1.3. தகவல் பாதுகாப்புக் குழு மீதான கொள்கை

நிறுனமானது தகவல் பாதுகாப்பு தொடர்பான நடவடிக்கைகளுக்கு மூலோபாய வழிகாட்டுதல்களை வழங்கும் நோக்குடன் தகவல் பாதுகாப்புக் குழுவை தாபித்தல் வேண்டும். தகவல் பாதுகாப்பு உத்தியோகத்தரினால் உருவாக்கப்பட்ட அனைத்து தகவல் பாதுகாப்பு கட்டுப்பாடுகள், செயல் திட்டங்கள், சொத்து வகையீட்டுத் திட்டங்கள், பாதுகாப்பு கொள்கைகள், சம்பவ மறுமொழி திட்டங்கள் மற்றும் பேரழிவு மீட்பு திட்டங்கள் ஆகியவற்றை மதிப்பாய்வு செய்து அங்கீகாரம்

அளிப்பதற்கு இந்த குழு பொறுப்பு வாய்ந்ததாகும், மேலும் அத்தகைய திட்டங்களின் அமுலாக்கங்களினையும் கண்காணிக்கும். நிறுவனத்தின் தலைவர், குழுவின் தலைவராக இருப்பதுடன், மேலும் குழுவானது தகவல் பாதுகாப்பு உத்தியோகத்தர், பிரதான புத்தாக்க உத்தியோகத்தர், (பிரதான) உள்ளக கணக்காய்வாளர் மற்றும் சொத்து உரிமையாளர்களையும் கொண்டிருக்கும்.

சொத்து உரிமையாளர்கள் மீதான கொள்கையானது பிரிவு 4.2.3 இல் தரப்பட்டுள்ளது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.4. இடர் முகாமைத்துவ குழு மீதான கொள்கை

நிறுவனமானது இடர் முகாமைத்துவக் குழுவொன்றினைத் தாபித்தல் வேண்டும். இந்தக் குழு, நிறுவனத்தின் தலைவருக்கு நேரடியாக முறைப்பாடு செய்யும் ஒரு சுயாதீனக் குழுவாக இருக்கும், மேலும் தகவல் மற்றும் தகவல் தொழில்நுட்பச் சொத்துக்கள் தொடர்பாக நிறுவனத்தின் இடர் முகாமைத்துவத்தினை மேற்பார்வையிடும் பொறுப்பைக் கொண்டுள்ளது.

இடர் முகாமைத்துவ குழுவானது சொத்துக்கள் தொடர்பான இடர்களைக் கண்டறிந்து மதிப்பீடு செய்யும், மேலும் இடர்களைக் குறைப்பதற்குத் தேவையான நடவடிக்கைகளை எடுக்க தகவல் பாதுகாப்புக் குழுவுக்கு பொருத்தமான கட்டுப்பாடுகளை முன்மொழிகிறது. இந்தக் குழுவில் பிரிவுத் தலைவர்கள், சொத்து உரிமையாளர்கள் மற்றும் தகவல் பாதுகாப்பு உத்தியோகத்தர் ஆகியோர் உள்ளடங்குகின்றனர். நிறுவனத்தின் பிரதித் தலைவர் குழுவின் தலைவராக இருப்பார்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.1.5. இறுதிப் பயனர் பொறுப்புக்கள் மீதான கொள்கை

தகவல் பாதுகாப்பானது ஒவ்வொருவரினதும் பொறுப்பாகும். அனைத்து இறுதி பயனர்களும் பொறுப்புடன் நடந்து கொள்ள வேண்டும் என்பதுடன் அவர்கள் அணுகக்கூடிய தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துகளின் பாதுகாப்பு தொடர்பான நிறுவனக்கொள்கைக்கு இணங்குதலும் வேண்டும்.

இறுதிப் பயனர் பொறுப்புகளில் தகவல், கணினி சாதனங்கள், மின்னஞ்சல்கள், இணையம், சமூக ஊடகங்கள், தொலைபேசிகள் மற்றும் தொலைநகல்களின் சரியான பயன்பாடு ஆகியவை அடங்கும். ஆனால் அவை மட்டுப்படுத்தப்படவில்லை.

அனைத்து பயனர்களும் தகவல் மற்றும் சைபர் பாதுகாப்பு அமலாக்க வழிகாட்டியில் குறிப்பிட்டுக்

காட்டப்பட்டுள்ள இறுதிப் பயனர் பொறுப்புகள் மற்றும் இந்தக் கொள்கையால் தேவைப்படும் பொருந்தக்கூடிய தகவல் பாதுகாப்பு நடைமுறைகளைப் புரிந்துகொண்டு கடைப்பிடித்தல் வேண்டும். அத்தகைய வளங்களை தவறாகப் பயன்படுத்தினால், தாபன விதிக் கோவையில் குறிப்பிடப்பட்டுள்ள ஒழுங்கு நடவடிக்கைகளுக்கும், கணினி குற்றச் சட்டம் அல்லது வேறு ஏதேனும் பொருந்தக்கூடிய சட்டவிதிகளின் சட்டங்களின் கீழும் சட்ட நடவடிக்கைகள் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.6. திறன் விருத்தி மீதான கொள்கை

தகவல் பாதுகாப்பு விழிப்புணர்வு மற்றும் பயிற்சியை நடத்துவதன் மூலம் பொறுப்பான தனிநபர்கள் (தகவல் பாதுகாப்பு உத்தியோகத்தர், பிரதான புத்தாக்க உத்தியோகத்தர், பிரதான உள்ளக கணக்காய்வாளர், சொத்துகளின் உரிமையாளர்கள், முதலியன) மற்றும் இறுதி பயனர்களின் தகவல் பாதுகாப்பு திறனை நிறுவனம் உருவாக்குகிறது. சம்பந்தப்பட்ட அதிகாரிகளின் இத்தகைய திறன் மேம்பாட்டு நடவடிக்கைகள் சரியான முறையில் மேற்கொள்ளப்பட வேண்டும், மேலும் இது போன்ற நடவடிக்கைகள் அமைப்பின் வருடாந்திர பயிற்சித் திட்டத்தில் சேர்க்கப்பட வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.7. பதவியினரின் பாதுகாப்பு அனுமதி மீதான கொள்கை

மிக இரகசியமான அல்லது இரகசியமான என வகைப்படுத்தப்பட்ட தகவலைக் கையாளும் ஒரு பதவிக்கு ஒதுக்கப்பட்ட அல்லது மாற்றப்பட்ட அல்லது முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுடன் அணுகல் உள்ளவர்கள் எந்தவொரு நபரும், நியமனம் அல்லது அந்த பதவிக்கு மாற்றுவதற்கு முன் பாதுகாப்பு அனுமதிச் சோதனைக்கு உட்படுத்தப்பட வேண்டும். அவர்களின் சேவையின் போது பின்னணி சோதனைகள் மற்றும் அவ்வப்போது பாதுகாப்பு அனுமதி சோதனைகள் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.1.8. மூலோபாய சீரமைப்பு மீதான கொள்கை

திட்டங்கள் மற்றும் செயல்பாடுகளை உள்ளடக்கிய நிறுவனத்தின் தகவல் பாதுகாப்பு செயல்திட்டங்கள், அத்தகைய முயற்சிகள் நிறுவனத்தின் தூரநோக்கு, பணிக்கூற்று மற்றும் நோக்கங்களுடன் இணைக்கப்படும் வகையில் வடிவமைக்கப்பட வேண்டும்.

நிறுவனத்திற்குள் செயல்படுத்தப்படும் அனைத்து தகவல் மற்றும் இணைய பாதுகாப்பு உத்திகள், திட்டங்கள், திட்டங்கள் மற்றும் செயல்பாடுகள் நிறுவனத்தின் பார்வை, நோக்கம்

மற்றும் நோக்கங்களுக்கு ஏற்ப வடிவமைக்கப்பட வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.9. செயல்திட்டங்கள் மீதான கொள்கை

நிறுவனம் தகவல் பாதுகாப்பு செயல்திட்டங்களை (நீண்டகால, நடுத்தர மற்றும் குறுகியகால திட்டங்கள்) உருவாக்கி அமுல்படுத்துதல் வேண்டும், இது நிறுவனத்தின் தூரநோக்கு, பணிக்கூற்று மற்றும் நோக்கங்களை அடைவதில் பாதுகாப்பு உத்தரவாதம் அளிக்கப்பட வேண்டிய வழியை வரையறை செய்கின்றது.

இடர் மதிப்பீட்டின் மூலம் நிர்ணயிக்கப்பட்ட தகவல் பாதுகாப்பு முன்னுரிமைகளின் அடிப்படையில், செயல்திட்டங்களில் தகவல் பாதுகாப்பு நடவடிக்கைகளுக்கான வரவு செலவுத் திட்டத்தையும் நிறுவனம் ஒதுக்கீடு செய்கின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.10. இணக்கம் மீதான கொள்கை

தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கைக்கு நிறுவனம் இணங்குதல் வேண்டும்.

பிரிவுகள் 4.1.1 மற்றும் 4.1.2 (அ) ஆகியவற்றில் குறிப்பிடப்பட்டுள்ளபடி, நிறுவனத்தின் தலைவர் மற்றும் தகவல் பாதுகாப்பு அதிகாரி இந்தக் கொள்கைக்கு இணங்குவதற்கான நிறுவனத்தின் இறுதிப் பொறுப்பை வைத்திருத்தல் வேண்டும்.

இலங்கை சேர்ட் நிறுவனம் இணங்கும் நிலையைத் தீர்மானிக்க வருடாந்தத் தகவல் பாதுகாப்புத் தயார்நிலை மதிப்பீடுகளை மேற்கொள்ளும், மேலும் அத்தகைய மதிப்பீடுகளை நடத்துவதற்கு தாபனமானது இலங்கை சர்ட்க்கு வசதிகளினை ஏற்படுத்திக் கொடுத்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.2. சொத்துக்கள், உரிமையாளர்கள், பயனர்கள் மற்றும் இடர்களை அடையாளம் காணுதல்

நிறுவன சொத்துக்களுக்கான தகவல் பாதுகாப்பு அபாயங்களை நிருவகிப்பதற்கு அவர்களின் செயற்பாட்டு சூழலைப் பற்றிய புரிதலை நிறுவனம் உருவாக்குதல் வேண்டும். நிறுவனத்திற்கு மதிப்புள்ள தகவல், முறைமைகள் மற்றும் தகவல் தொழில்நுட்ப சாதனங்கள்

(சொத்துக்கள்), சொத்துக்களின் உரிமையாளர்கள் மற்றும் சொத்துக்களின் பாவனையாளர்கள் அவர்களின் தொழிற்பாடுகள் மற்றும் பொறுப்புகள் மற்றும் சொத்துகளுடன் தொடர்புடைய தற்போதைய அபாயங்கள் ஆகியவற்றை நிறுவனம் அடையாளம் காணுதல் வேண்டும்.

இது தொடர்பில், நிறுவனமானது பின்வரும் கொள்கைகளினை கடைப்பிடித்தல் வேண்டும்.

4.2.1. தகவல் சொத்துக்கள் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள் அடையாளம் காணுதல் மீதான கொள்கை

நிறுவனம் அதன் முக்கியமான தகவல் சொத்துக்களை (information assets) அடையாளம் காணுதல் வேண்டும். ஒரு தகவல் சொத்து என்பது அதன் நிறுவன செயற்பாடுகளை நிறைவேற்றுவதில் நிறுவனத்திற்கு மதிப்புள்ள எத்தகைய தகவலும் ஆகும்.

வர்த்தக ரகசியங்கள், கேள்வி மனு ஆவணங்கள், வரவு செலவுத் தாள்கள் மற்றும் ஊழியர்களின் தனிப்பட்ட பதிவுகள், நிறுவனத்தால் வழங்கப்படும் சேவைகள் தொடர்பான பயன்பாட்டு மென்பொருள் மூலம் சேகரிக்கப்பட்ட தரவு போன்றவை தகவல் சொத்துக்களுக்கான எடுத்துக்காட்டுகளாகும். தகவல் சொத்துக்கள் காகித ஆவணம், டிஜிட்டல் ஆவணம், தரவுத்தளம், கடவுச்சொல் அல்லது குறியாக்க விசை (encryption key) அல்லது வேறு ஏதேனும் டிஜிட்டல் கோப்பு போன்ற பல்வேறு வடிவங்களில் வரலாம்.

தாபனமானது தகவல் தொழில்நுட்ப சொத்துக்களையும் (IT assets) அடையாளம் காணும். தகவல் தொழில்நுட்ப சொத்து என்பது ஒரு தகவல் தொழில்நுட்ப சூழலிலுள்ள ஒரு மென்பொருள் (உதாரணம். இயக்க முறைமை, சம்பள முறைமை, முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு) அல்லது வன்பொருள் (உதாரணம். கணினிகள், வன்தட்டுகள், சர்வர்கள், ரவுட்டர்கள், ஃபயர்வால்கள்) வலையமைப்புக்கள் அல்லது பிற டிஜிட்டல் உள்கட்டமைப்பு வசதிகள் குறிப்பிடுகின்றது.

சொத்துக்களை அடையாளம் காணுதல் (தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள்) அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, வெளிப்படுத்துதல், இடையூறு, மாற்றம் அல்லது அழித்தல் ஆகியவற்றிலிருந்து சொத்துக்களைப் பாதுகாக்கும் நோக்கத்துடன் ஒருமைப்பாடு (integrity), ரகசியத்தன்மை (confidentiality) மற்றும் சொத்துகளின் கிடைக்கும் தன்மையினை (availability) உறுதிசெய்யும் நோக்கத்துடன் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.2.2. முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு அடையாளம் காணுதல் மீதான கொள்கை

முக்கியமான தேசிய தகவல் உள்கட்டமைப்புக்கள் என்பது தேசிய பாதுகாப்பு, நிருவாகம், பொருளாதாரம், சுகாதாரம் மற்றும் ஒரு நாட்டின் சமூக

நல்வாழ்வில் பேரழிவுகரமான தாக்கத்தை ஏற்படுத்தும் தோல்வி அல்லது அழிவினை ஏற்படுத்துகின்ற முறைமைகள் அல்லது வசதிகளினைக் குறிப்பிடும்.

முக்கியமான தேசிய தகவல் உள்கட்டமைப்பினைப் பராமரிக்கும் நிறுவனங்கள் இந்தக் கொள்கையில் குறிப்பிடப்பட்டுள்ள அத்தகைய உட்கட்டமைப்பைப் பாதுகாக்க தகுந்த நடவடிக்கைகளை எடுத்தல் வேண்டும். முக்கியமான தேசிய தகவல் உள்கட்டமைப்பினை அடையாளம் காண்பது இலங்கை கணினி அவசர தயார்நிலை அணியினால் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.2.3. சொத்து உரிமையாளர்கள், பாதுகாவலர்கள் மற்றும் பயனர்களின் பொறுப்புகள் மீதான கொள்கை

நிறுவனமானது உரிமையாளர்கள் மற்றும் பாதுகாவலர்களை அடையாளம் கண்டு கொள்ளுதல் வேண்டும். சொத்து உரிமையாளர் ஒரு சிரேஷ்ட நிறைவேற்றுத் தரத்திலான அதிகாரி அல்லது ஒரு சொத்தின் வாழ்க்கைச் சுழற்சியைக் கட்டுப்படுத்தும் அங்கீகரிக்கப்பட்ட நிருவாகப் பொறுப்பைக் கொண்ட ஒரு தாபனமாக இருத்தல் வேண்டும். சொத்து உரிமையாளர் சொத்துக்களுக்கான இடர்களைப் புரிந்து கொள்ளுதல் வேண்டும் என்பதுடன் அத்தகைய சொத்துக்களைப் பாதுகாப்பதற்கான சொத்து உருவாக்கப்படும்போது அல்லது நிறுவனத்திற்கு சொத்துக்கள் மாற்றப்படும் போது அல்லது தாபனத்தால் கையகப்படுத்தப்படும் போது அதன் உரிமையை முறையாக ஒதுக்குவது அவசியமாகும்.

தகவல் சொத்தின் பாதுகாவலர், என்பவர் சொத்தின் பாதுகாப்பிற்கு பொறுப்பான ஒரு நபர் அல்லது ஒரு நிறுவனம் மற்றும் சொத்தின் பாதுகாப்பு தொடர்பான கட்டுப்பாடுகளை (தகவல் சொத்தின் உரிமையாளரால் அடையாளம் கண்டு அங்கீகரிக்கப்பட்ட) செயல்படுத்துவதற்கான பொறுப்பாளியாவார்.

சொத்து உரிமையாளரும் பாதுகாவலரும் சொத்துக்களுக்கான பதிவேடுகளை விருத்தி செய்தல், சொத்துக்களை வகைப்படுத்துதல் மற்றும் சொத்துக்களைப் பாதுகாத்தல், சொத்துகளுக்கான அணுகல் கட்டுப்பாடுகளை வரையறுத்தல் மற்றும் மறுபரிசீலனை செய்தல், சொத்து நீக்கப்படும் போது அல்லது அழிக்கப்படும் போது சரியான கையாளுதலை உறுதி செய்தல் ஆகியவற்றுக்கும் பொறுப்பாளிகளாவர்.

நிறுவனம் அதன் சொத்துகளைப் பயன்படுத்தும் பயனர்களையும் அடையாளம் காண வேண்டும். உத்தியோகபூர்வ நோக்கங்களுக்காக சொத்துகளைப் பயன்படுத்தும் பணியாளர்கள் பயனர்கள். உத்தியோகபூர்வ நோக்கங்களுக்காக சொத்துக்களை பயன்படுத்த வேண்டிய பயனர்களை சொத்து உரிமையாளர்கள் துல்லியமாக அடையாளம் காணுதல் வேண்டும், மேலும் பிரிவு 4.3.4 மற்றும் 4.3.5 இல் குறிப்பிடப்பட்டுள்ளபடி

அந்த சொத்துகளுக்கான அணுகலைக் கட்டுப்படுத்துதலும் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.2.4. தகவல் சொத்துக்கள் மற்றும் தகவல் தொழில்நுட்ப சொத்துகள் பதிவேடுகளினைப் பேணுவது மீதான கொள்கை

நிறுவனமானது தகவல் சொத்துக்களை தகவல் சொத்து பதிவேட்டில் (Information Assets Register) பதிவு செய்தல் வேண்டும். ஒரு தகவல் சொத்துக்கள் பதிவு என்பது ஒரு தாபனம் வைத்திருக்கும் மற்றும் செயலாக்கும் தகவல் சொத்துக்களின் முறையான இருப்பு ஆகும்.

குறைந்தபட்சம், ஒரு தாபனமானது, தகவல் சொத்தின் பெயர், தகவல் சொத்தின் அமைவிடம், தகவல் சொத்தின் உரிமையாளர் மற்றும் பாதுகாவலர், வகைப்படுத்தப்பட்ட திகதி, சொத்துக்களை செயலாக்கும் கணினி முறைமை, வகைப்படுத்தலுக்கான காரணம், அகற்றல் தேவைகள், வகைப்படுத்தல் மீளாய்வு திகதி, இழப்பு/ இணக்கப்பாடு அல்லது வெளிப்படுத்துதல் ஆகியவற்றின் தாக்கம் என்பவற்றினைப் பதிவு செய்யும். தகவல் சொத்துக்கள் பதிவேடு துல்லியமாகவும், புதுப்பித்ததாகவும், சீரானதாகவும் மற்ற சரக்குகளுடன் சீரமைக்கப்பட்டதாகவும் இருத்தல் வேண்டும்.

நிறுவனமானது தகவல் தொழில்நுட்ப சொத்துகள் பதிவேட்டில் (IT Assets Register) தகவல் தொழில்நுட்ப சொத்துகளின் விவரங்களை பதிவு செய்யும். தகவல் தொழில்நுட்பசொத்துப் பதிவேட்டில் குறைந்தபட்சம், சொத்துகளின் வகை (உதாரணம். வன்பொருள், மென்பொருள், சர்வர்), சொத்தின் இருப்பிடம், இயக்க முறைமை, உரிம விவரங்கள், பயனர்கள், ஆபத்து, வகைப்பாடு நிலை, மதிப்பிடப்பட்ட மதிப்பு மற்றும் பலவற்றைக் கொண்டிருத்தல் வேண்டும். தகவல் தொழில்நுட்ப சொத்துப் பதிவேடானது துல்லியமாகவும், புதுப்பித்ததாகவும், மற்ற இருப்புகளுடன் சீரானதாகவும் இருத்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.2.5. இடர் மதிப்பீடுகள் மீதான கொள்கை

நிறுவனத்தின் சொத்துக்களுக்கு ஏற்படும் அச்சுறுத்தல்கள் மற்றும் பாதிப்புகள் மற்றும் சொத்துக்களின் மீதான அவற்றின் தாக்கம் ஆகியவற்றைத் தீர்மானிக்க தாபனமானது இடர் மதிப்பீட்டை மேற்கொள்ளும்.

இடர் மதிப்பீட்டின் நோக்கம், சொத்துக்களுக்கு (தரவு, கணினி அமைப்புகள் அல்லது ஏனைய டிஜிட்டல் உட்கட்டமைப்பு) ஏற்படும் பாதிப்புகள் மற்றும் அச்சுறுத்தல்களைக் கண்டறிவது மற்றும்

ஏற்றுக்கொள்ளக்கூடிய அளவிற்கு ஆபத்தை குறைப்பதற்கு எத்தகைய பாதுகாப்பு நடவடிக்கைகள் எடுக்கப்பட வேண்டும் என்பதை தீர்மானிப்பதுமேயாகும்.

இடர் மதிப்பீட்டின் அடிப்படையில், தாபனமானது இடர் பதிவேட்டில் இடர்களுக்கு முன்னுரிமை அளித்து இடர்களை பதிவு செய்தல் வேண்டும்.

பிரிவு 4.3 இல் குறிப்பிடப்பட்டுள்ள கொள்கைப் பரிசீலனைகளை கணக்கில் எடுத்துக்கொண்டு, இடர் பதிவேட்டில் (Risk Register) பதிவு செய்யப்பட்ட இடர்களுக்கான தகுந்த பாதுகாப்பு முன்னெச்சரிக்கைகளை நிறுவனம் எடுத்தல் வேண்டும். இடர் மதிப்பீடு தாபனத்தின் இடர் முகாமைத்துவ குழுவினால் மேற்கொள்ளப்படும். தாபனமானது பொருத்தமான திறன்களைக் கொண்டிருக்கவில்லை என்றால், இந்த நோக்கத்திற்காக ஒரு தகுதி வாய்ந்த மற்றும் அனுபவம் வாய்ந்த நிறுவனமொன்று பணியில் அமர்த்தப்படும்.

இலங்கை கணினி அவசர தயார் நிலை அணியானது முக்கியமான தேசிய தகவல் உள்கட்டமைப்புகளுக்கு இடர் மற்றும் பாதிப்பு மதிப்பீடுகளை மேற்கொள்ளுவதற்கு உதவியளிக்கும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.2.6. சொத்துக்களின் வகையீடு மீதான கொள்கை

நிறுவனமானது சொத்துக்களை வகைப்படுத்தி, சொத்துக்களின் உணர்திறனை தீர்மானிக்க வேண்டும்.

ஒரு சொத்தானது தாபனத்திற்கான அதன் மதிப்பு மற்றும் அதன் உணர்திறன் ஆகியவற்றிற்கு ஏற்ப பொருத்தமான அளவிலான பாதுகாப்பைப் பெறுவதை உறுதி செய்வதே வகைப்படுத்தலின் பிரதான நோக்கமாகும். தகவல் சொத்து வகையீடானது ஏற்றுக் கொள்ளப்பட்ட வழிகாட்டுதல்களின் அடிப்படையில் மேற்கொள்ளப்படுதல் வேண்டும்.

தகவல் சொத்துக்களுக்கான வகையீட்டு மட்டங்கள் “மிக இரகசியமானவை” (secret), “இரகசியமானவை” (confidential), “வரையறுக்கப்பட்ட பகிர்வு” (limited sharing), “பொது” (public), மற்றும் “வகைப்படுத்தப்படாத” (unclassified) என்பனவாகும்.

தகவல் தொழில்நுட்பச் சொத்துக்களானவை "மிகவும் முக்கியத்துவம் வாய்ந்த" (very critical), "முக்கியத்துவம் வாய்ந்த" (critical), "முக்கியத்துவம் அல்லாத" (non-critical) மற்றும் “வகைப்படுத்தப்படாத” (unclassified) என நான்கு நிலைகளாக வகைப்படுத்தப்படும்.

தகவல் தொழில்நுட்ப சொத்துக்கள் வகைப்படுத்தல் திட்டத்தின் விபரணமானது “தகவல் மற்றும் சைபர் பாதுகாப்பு அமலாக்கல் வழிகாட்டி[4]” இல் உள்ளது. (பிரிவு 2.2. (இ) இனைப் பார்க்கவும்)

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3. சொத்துக்கள் பாதுகாப்பு

சொத்துக்களை இனங்காண்பதன் பேரில், அந்த நிறுவனமானது, சாத்தியமான தகவல் பாதுகாப்பு நிகழ்வு அல்லது சம்பவத்தின் தாக்கத்தைத் தடுப்பதற்கு, மட்டுப்படுத்துவதற்கு அல்லது கட்டுப்படுத்துவதற்கு பொருத்தமான கட்டுப்பாடுகளை நடைமுறைப்படுத்துதல் வேண்டும். பிரயோகிக்கப்படுகின்ற கட்டுப்பாடுகள் ஒவ்வொரு சொத்தின் வகைப்பாட்டின் அடிப்படையில் அமைந்திருத்தல் வேண்டும்.

கொள்கையுடன் ஒத்திணங்குவதற்காக, இந்த நிறுவனம், சொத்தை அடைவதனைக் கட்டுப்படுத்தும், தரவைப் பாதுகாப்பதற்கு நடைமுறையிலுள்ள செயல்முறைகளை செயற்படுத்தும், தரவு அனுப்பப்படுகின்ற போது மற்றும் தரவு ஓய்விலுள்ள போது தரவுக்கான பாதுகாப்பு கட்டுப்பாடுகளை வரையறுக்கும், உரிமம் பெற்ற, அதிகாரமளிக்கப்பட்ட மென்பொருளைப் பயன்படுத்தும். நிறுவனத்தின் கொள்கைகள் கீழே தரப்பட்டுள்ளவற்றுடன் இணங்குதல் வேண்டும்.

4.3.1. ஓய்விலுள்ள தரவினைப் பாதுகாத்தல் மீதான கொள்கை

நிறுவனமானது, ஓய்விலுள்ள தரவினைப் பாதுகாத்தல் வேண்டும். ஓய்விலுள்ள தரவு என்பது சாதனத்திலிருந்து சாதனம் அல்லது வலைப் பின்னலிலிருந்து வலைப்பின்னலுக்கு தீவிரமாக நகராத தரவு (உ.ம். சேவையகம், கிளவுட், வன்செலுத்தி, மடிக்கணினி, ஃபிளாஷ் டிரைவ் அல்லது காப்பகப்படுத்தப்பட்ட/சேமிக்கப்பட்ட தரவு) ஆகும்.

சேமிப்பதற்கு முன்னர் "மிக இரகசியமானது" (confidential) அல்லது "இரகசியமானது" (secret) என வகைப்படுத்தப்படுகின்ற எந்தவொரு தரவினையும் (தகவல் ஆதனங்கள்) குறியாக்கம் (encrypt) செய்வதும் சொத்துக்களுக்குப் பௌதீக ரீதியான பாதுகாப்பு, இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு வழங்குவதும் அத்தியவசியமானதாகும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.2. பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாத்தல் மீதான கொள்கை

நிறுவனமானது பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாத்தல் வேண்டும். பரிமாற்றப்படுகின்ற தரவு என்பது இணையம் முழுவதும் அல்லது ஒரு தனிப்பட்ட வலையமைப்பினூடாக போன்ற அத்தகையதொரு இடத்திலிருந்து பிறிதொரு இடத்திற்கு தீவிரமாக நகரும் தரவு (உ.ம். தரவு ஒரு நிறுவனத்திற்கு சொந்தமான வைஃபை உள்ளடங்கலாக தனிப்பட்ட வலையமைப்பினூடாக தளம் 'அ' இலிருந்து தளம் 'ஆ' க்கு மாற்றப்படுகின்றது) ஆகும்.

பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாக்கும் நோக்கில், நிறுவனம், தரவு பரிமாற்றத்திற்காக நகர்த்துவதற்கும், பாதுகாப்பான இணைப்புகளை (HTTPS, TLS, SFTP போன்றன) பயன்படுத்துவதற்கு முன்னர் உணர்வுபூர்வமான தகவல்களை ("மிக இரகசியமானது" அல்லது "இரகசியமானது" என்று தகவல்களை வகைப்படுத்தி) குறியாக்கம் செய்தல் வேண்டும். மேலும், தாபனமானது, வைஃபை ஏற்பாடுகள் தொடர்பில் பாதுகாப்பு அளபுருக்களை (security parameters) மேற்கொண்டுள்ளது என்பதை உறுதி செய்தலும் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.3. பௌதீக ரீதியான பாதுகாப்பு மீதான கொள்கை

நிறுவனமானது, பௌதீக தலையீடு மற்றும் அதிகாரமற்ற அணுகலைத் தடுப்பதற்காக சொத்துக்களுக்கு பௌதீக ரீதியான பாதுகாப்பை வழங்குதல் வேண்டும்.

சொத்துக்களின் பாதுகாப்பு தேவைகளின் அடிப்படையில், ஒவ்வொரு நிறுவனமும் அதற்கு முக்கியமான ஆதனங்களை சேமிப்பதற்கு அல்லது செயல்முறைக்கு பாதுகாப்பான பகுதிகளை வரையறுத்தல் வேண்டும். "மிக இரகசியமானது" மற்றும் "இரகசியமானது" என்று வகைப்படுத்தப்பட்ட தகவல் ஆதனங்கள் குறிப்பிடப்பட்ட பாதுகாப்பான பகுதிகளில் சேமிக்கப்பட்டு, செயல்படுத்தப்படுதல் வேண்டும்.

மேலும், "(மிகவும்) முக்கியமானவை" என வகைப்படுத்தப்படும் தகவல் தொழில்நுட்ப சொத்துக்கள் பாதுகாப்பான பகுதிகளில் சேமிக்கப்பட்டு செயல்படுத்தப்படும்.

பாதுகாப்பான பகுதிகள் இயற்பொருள் சார்ந்த சுவர்கள், பூட்டக்கூடிய கதவுகள் மற்றும் பல் ஆக்கக்கூறு பதிவு முறைமைகளால் (multi-factor entry systems) பாதுகாக்கப்படுதல் வேண்டும் என்பதுடன், பௌதீக தலையீடுகள் மற்றும் அதிகாரமற்ற அணுகலைத் தடுப்பதற்கு தொடர்ந்து இரகசிய கமராக்கள் (CCTV) மூலம் கண்காணிக்கப்படுதல் வேண்டும்.

தீ, வெள்ளம், ஈரப்பதம், மின்காந்த துறைகள் மற்றும் வெப்பநிலை ஆகியவற்றிலிருந்து அச்சுறுத்தல்களைத்

தடுப்பதற்கு பாதுகாப்புப் பகுதிகள் பாதுகாக்கப்படுதல் வேண்டும்.

இதற்கு மேலதிகமாக, தாபனம், தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களைப் பயன்படுத்துபவர் அணுகுவதைக் கட்டுப்படுத்துவதற்கு பல்வேறு தொழில்நுட்பங்களைப் பயன்படுத்துதல் வேண்டும். அத்தகைய தொழில்நுட்பங்கள், பயன்படுத்துபவரின் அடையாளம், கடவுச்சொற்கள், அணுகல் அட்டைகள், தனிப்பட்ட அடையாள எண் மற்றும் மரபணுக்கள் ஆகியவற்றை உள்ளடக்குகின்றது, ஆனால் அதற்குள் மட்டுப்படுத்தப்படவில்லை.

இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடுச் செயன்முறையை (கொள்கைக் கூற்று 4.3.4 இனைப் பார்க்கவும்) நடைமுறைப்படுத்துவதன் மூலம் கணினிகள், முறைமைகள் அல்லது ஏதேனும் சாதனங்களைஅணுகுவதனை கட்டுப்படுத்தப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.4. இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு மீதான கொள்கை

நிறுவனமானது, பயன்படுத்துபவர் தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்கள் இரண்டினையும் அணுகுவதைக் கட்டுப்படுத்துதல் வேண்டும். இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்துதல் என்பது தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களை பாதுகாப்பாக வைத்திருப்பதற்காக அணுகுவதை முகாமை செய்கின்ற அணுகுமுறையொன்றாகும்.

இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்துதல் என்பது, முறைமைகளையும் தகவல்களையும் அவர்கள் அணுகுவதற்கு அனுமதிப்பதற்கு முன்னர் பயன்படுத்துபவரின் அடையாளத்தையும் அவர்கள் அணுகுகின்ற அளவையும் சரிபார்ப்பதில் கவனம் செலுத்துகின்றது, பயன்படுத்துபவர் தங்கள் பணி இலக்குகளை (தெரிந்து கொள்ள வேண்டியவை) ஆற்றுவதற்குத் தேவையான ஆதனங்களை மட்டுமே அணுகுவதற்கும் மற்றும் பணி இலக்குகளை (பயன்படுத்த வேண்டிய தேவையுள்ள) ஆற்றுவதற்கும் அனுமதி வழங்கப்படுதல் வேண்டும். பயன்படுத்துபவர் அவர்களின் வகிபாகத்திற்கு ஏற்ப தேவையான முறைமைகளும், தகவல்களுக்கும் எப்போதும் குறைந்தபட்ச அணுகல் வழங்கப்படுதல் வேண்டும். கொடுக்கப்பட்ட கொள்கைகளின் அடிப்படையில், நிறுவனமானது அதன் பயன்பாட்டிற்கான இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாட்டுச் செயன்முறையினை விருத்தி செய்தல் வேண்டும்.

இலங்கை சர்ட், நிறுவனத்தால் தனிப் பயனாக்கக் கூடியதும், பின்பற்றக்கூடியதுமான அரச நிறுவனங்களுக்கான "இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறை" என்பதை வரைந்துள்ளது.

நிறுவனத்தால் செயல்படுத்தப்படும் இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறை போதுமானதாகவும்

புதுப்பித்ததாகவும் இருப்பதை நிறுவனம் உறுதி செய்ய வேண்டும். மேலும், அனைத்து ஊழியர்களும், மூன்றாம் தரப்பு சேவை வழங்குநர்களும் அரசு நிறுவனத்தால் செயல்படுத்தப்படும் இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறையை கடைப்பிடிக்க வேண்டும்.

இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறையின் ஏதேனும் மீறல்கள், ஏற்படுமிடத்து தேவையான நடவடிக்கைக்காக தகவல் பாதுகாப்பு செயற்குழுவிற்கு தெரிவிக்கப்படும். ஒரு தகவல் பாதுகாப்பு செயற்குழு நிறுவப்படாத சூழ்நிலையில், அத்தகைய மீறல்கள் சர்வதேச தரநிர்ணய அமைப்பு மூலம் நிறுவன தலைமைத்துவத்திற்கு தெரிவிக்கப்பட வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.5. வலுவான உறுதிப்படுத்தல் மீதான கொள்கை

அதிகாரமளித்தலானது பயனரொருவரின் இனங்காணல் செயன்முறையாகும்.
அதிகாரமளித்தலானது சான்றின் மூலம் பயனர் அதிகாரமளித்தல் செயன்முறையானது (இனங்காணுதல்) மற்றும் பயனர் உறுதிப்படுத்தல் (அடையாளத்தினை உறுதிப்படுத்துதல்) என்பவற்றினூடாக நிறுவனத்தின் சொத்துக்களுக்கு அணுகலினை வழங்குகின்றது.

கொள்கையின் 4.6.4 இல் குறிப்பிடப்பட்டவாறு நிறுவனத்தின் இனங்காணல் முகாமைத்துவ மற்றும் அணுகல் கட்டுப்பாட்டுச் செயன்முறைக்கமைவாக, பயனர் அடையாளத்தினை உறுதிப்படுத்துவதற்கு நிறுவனமானது வலுவான அதிகாரத்தினைப் பயன்படுத்துதல் வேண்டும்.

பயன்படுத்துபவரின் பெயர் மற்றும் கடவுச்சொல் சேர்க்கை மற்றும் பல் காரணி அங்கீகாரத்தினை (multi-factor authentication) பயன்படுத்துதல் ஆகியவை பயன்படுத்துபவரின் அடையாளத்தை உறுதிப்படுத்துவதற்கு பரிந்துரைக்கப்படுகின்றன.

ஒரு வலுவான உறுதிப்படுத்தல் செயல்முறையை உறுதி செய்வதற்கு, பின்வரும் காரணிகளை, (ஆனால் மட்டுப்படுத்தப்படவில்லை) நிறுவனத்தின் இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாட்டுக் கொள்கையினை உருவாக்குவதில் கவனம் செலுத்துதல் வேண்டும்.

(அ) வலுவான கடவுச்சொல்:

- கடவுச்சொற்கள் குறைந்தபட்சம் 8 எழுத்துக்களைக் கொண்ட நீளத்திலும், மற்றும் மேல், மற்றும் கீழ் நிலை எழுத்துக்கள் ஆகிய இரண்டையும் (உ.ம். a-Z), இலக்கங்கள் (0,9), மற்றும் சிறப்பு எழுத்துக்கள் (!@$+/) கொண்டிருத்தல் வேண்டும்.
- அனைத்து கடவுச்சொற்களையும் வழக்கமான அணுகலுக்கு 90 நாட்கள் என்று முன்கூட்டியே தீர்மானிக்கப்பட்ட இடைவெளிகளுக்குப் பின்னர்

மாற்றப்படுதல் வேண்டும். சிறப்புரிமை அணுகல் (privileged access) ஒரு தேவையொன்றின் அடிப்படையில் மட்டுமே வழங்கப்படுதல் வேண்டும்.

(ஆ) பல்காரணி அங்கீகாரம் (MFA)

- மிக இரகசிய மற்றும் இரகசியத் தகவல்களை அணுகக்கூடிய பயனர் கணக்குகளைப் பாதுகாப்பதற்காக பல்காரணி அங்கீகார அணுகலை நிறுவனம் செயல்படுத்தும்.
- பல்காரணி அங்கீகாரத்தினை வடிவமைப்பதில், நிறுவனம் குறைந்தபட்சம் பயனரின் அறிவு (உங்களுக்குத் தெரிந்தது: what you know, உ.ம். கடவுச்சொல்), உடைமை (உங்களிடம் என்ன உள்ளது: what you have , உ.ம். குறி அடையாளம், அணுகல் அட்டை) அல்லது உள்ளார்ந்தவை (inherence) (உங்கள் உள்ளார்ந்த தன்மையாக இருப்பது: what you are, உ.ம். மரபணுக்-கைரேகை) ஆகியவற்றின் சேர்க்கையினை கவனத்தில் எடுத்துக் கொள்ளுதல் வேண்டும்.

நிறுவனத்தை விட்டு வெளியேறுகின்ற பணியாளர் ஒருவருக்கு வழங்கப்பட்ட கடவுச் சொற்கள் மற்றும் பிற வேறு உறுதிப்படுத்தல் சான்றுகளும், மேலும் பணியாளர் அணுகுவதைத் தடுப்பதற்கு அனைத்து சொத்துக்களிலிருந்தும் திரும்பப் பெறப்பட்டு அகற்றப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.6. கணினி கிளவுட் மற்றும் தரவு இறையாண்மை மீதான கொள்கை

தரவு இறையாண்மை (data sovereignty) என்பது நாட்டிற்குள் உள்ள சட்டங்கள் மற்றும் நிருவாக கட்டமைப்புகளுக்கு உட்பட்ட தரவுகளை குறிக்கிறது, அத்தகைய தரவு சேகரிக்கப்பட்டு, செயலாக்கப்பட்டு சேமிக்கப்படுகிறது. இந்தச் சூழலில், சேகரிக்கப்பட்ட தரவைச் சேமித்து செயலாக்க மற்ற நாடுகளிலிருந்து கிளவுட் சேவைகள் பெறப்படும்போது, குறிப்பாக தரவு இறையாண்மையில் அரசாங்க நிறுவனம் அதிக கவனம் செலுத்த வேண்டும்.

கிளவுட் கணினி என்பது பொதுவாக தகவல் தொடர்பாடல் தொழில்நுட்ப ஆதாரங்களைக் குறிக்கிறது (எ.கா. சேமிப்பகம், செயலாக்கம், பயன்பாட்டு மேம்பாடு தளங்கள் போன்றவை) பயனரின் நேரடி மேலாண்மை இல்லாமல் தேவைக்கேற்ப பயனர்களுக்குக் கிடைக்கும். இப்போதெல்லாம் பல நிறுவனங்கள் செலவீன சேமிப்பு, அளவிடுதல் மற்றும் அதிகரித்த செயல்திறன் காரணமாக கிளவுட் சேவைகளுக்கு நகர்கின்றன.

இருப்பினும், நிறுவனமானது, கிளவுட் சேவைகளைப் பயன்படுத்துவதன் ஆபத்து பற்றி குறிப்பாக, பொது கிளவுட்டைப் (பொது கிளவுட் என்பது,அவற்றை வாங்க விரும்பும் எவருக்கும் கிடைக்கப் பெறுகின்ற கிளவுட் சேவையொன்றாகும்) பயன்படுத்தும் போது மிகவும் எச்சரிக்கையாக இருத்தல் வேண்டும். வெவ்வேறு அதிகார வரம்புகளில் செயல்படுவதால் கிளவுட் மீது

வரையறுக்கப்பட்ட கட்டுப்பாடு, கட்டிடக்கலைஞர்களின் வரையறுக்-கப்பட்ட தெரிவுநிலை மற்றும் செயல்பாடுகளின் வரையறுக்-கப்பட்ட வெளிப்படைத்தன்மை, சேவை மட்ட ஒப்பந்தங்களில் சாத்தியமான குறிப்பிடத்தக்க பொருத்தமின்மைகள் ஆகியவை பொதுவான கிளவுட் அபாயங்கள் ஆகும்.

தங்கள் கிளவுட் சேவைத் தேவைகளைப் பூர்த்தி செய்வதில், நிறுவனங்கள் லங்கா அரசு கிளவுட் (Lanka Government Cloud) மூலம் சேவைகளைப் பெறுவதற்கு முன்னுரிமை அளிக்க வேண்டும். லங்கா அரசு கிளவுட் என்பது அரசாங்கத்திற்குச் சொந்தமான தனியார் கிளவுட் சேவையாகும், இது தகவல் மற்றும் தொடர்பாடல் தொழில்நுட்ப நிறுவனத்தால் இயக்கப்படுகிறது, இது அரசாங்கத்தின் கிளவுட் சேவைத் தேவைகளைப் பூர்த்தி செய்யும் வகையில் வடிவமைக்கப்பட்டுள்ளது. எவ்வாறாயினும், எந்தவொரு கிளவுட் சேவை வழங்குநரிடமிருந்தும் சேவைகளைப் பெறுவதற்கு முன், சரியான இடர் மதிப்பீட்டைச் செய்ய நிறுவனங்களுக்கு கண்டிப்பாக பரிந்துரைக்கப்படுகிறது.

மேலும், தரவுகளை சேகரித்தல், சேமித்தல் மற்றும் செயலாக்குதல் அல்லது பிற அதிகார வரம்புகளில் மென்பொருள் பயன்பாடுகளை ஹோஸ்ட் செய்தல் தொடர்பான அமைப்பின் அனைத்து நடவடிக்கைகளும் தரவு பாதுகாப்பு தொடர்பாக இலங்கையில் உள்ள தொடர்புடைய சட்டங்கள் மற்றும் ஒழுங்குமுறைகளுக்கு இணங்க மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.7. உரிமம் பெற்ற மென்பொருள் மற்றும் இணைப்புகளை இற்றைப்படுத்தல்கள் மீதான கொள்கை

நிறுவனமானது, செல்லுபடியாகும் இற்றைப்படுத்தல்களுடன் உரிமம் பெற்ற மென்பொருளைப் பயன்படுத்துதல் வேண்டும். இது முறைமை மென்பொருள், பயன்பாட்டு நிரல்கள் மற்றும் பிரயோக மென்பொருள் (உ.ம். வார்த்தை செயலாக்க பொதிகள்: word processing packages, தரவுத்தளங்கள்: databases, உலாவிகள்: browsers, தீம்பொருள் எதிர்ப்பு: antimalware போன்றவை) ஆகியவற்றை உள்ளடக்குகின்றது, ஆனால் அதற்குள் மட்டுப்படுத்தப்படவில்லை.

விற்பனையாளர் வழங்கிய சமீபத்திய இணைப்புகள் மற்றும் திருத்தங்களுடன் இயக்க முறைமைகள் மற்றும் பிற தொடர்புடைய மென்பொருள்களை நிறுவனம் புதுப்பிக்க வேண்டும். மேலும், நிறுவனங்கள் தானியங்கி புதுப்பிப்புகளை இயக்க வேண்டும்.

முன்னதாக, அவற்றினை நிறுவுவதால் ஏற்படும் உள்ளார்ந்த பாதிப்பு குறித்து உரிய வகையில் மதிப்பீடு செய்யப்படுதல் வேண்டும். (குறிப்பாக மிகவும் சிக்கல் வாய்ந்த மற்றும் சிக்கலான முறையில் வகைப்படுத்தப்பட்ட தகவல் தொழில்நுட்ப சொத்துக்களுக்கானவை)

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.8. தீம்பொருள் எதிர்ப்பு மீதான கொள்கை

நிறுவனமானது, செல்லுபடியாகும் உரிமத்துடன் தீம்பொருள் எதிர்ப்பு மென்பொருளை நிறுவுதல் வேண்டும். தீம்பொருள் எதிர்ப்பு கருவிகள், எந்த சாத்தியமான நுழைவு புள்ளியிலும் செயலில் இருக்கும் என்பதுடன், மிகப் புதிய தீம்பொருள் கையொப்பங்கள் நாளாந்தம் வரைப்படுத்தப்படுவதுடன், தானியங்கு முறையில் இற்றைப்படுத்தல்கள் செயல்படுத்தப்படுதலும் வேண்டும்.

கோப்புகளை பதிவிறக்கம் செய்தல் அல்லது திறத்தல், அகற்றக்கூடிய அல்லது தொலைநிலை சேமிப்பகத்தில் உள்ள கோப்புறைகள் மற்றும் வலைப் பக்க ஸ்கானிங் உள்ளடங்கலாக அணுகுகின்ற போதான பரிசோதனைக்கு ஏற்ப தீம்பொருள் கண்டறிதல் கட்டமைக்கப்படுதல் வேண்டும்.

அரசாங்க நிறுவனமொன்று இன்னொரு நிறுவனத்துடன் அல்லது பொது மக்களுடன் இலத்திரனியல் முறையினூடாக தொடர்பு கொள்ளும் போது, அனுப்புபவர் தகவலானது தீம்பொருள் தாக்கத்திலிருந்து விடுபட்டது என்பதனை உறுதி செய்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.9. உத்தியோகபூர்வ மின்னஞ்சல்கள் மீதான கொள்கை

நிறுவனம், உத்தியோகபூர்வ தகவல் தொடர்புகளுக்கு உத்தியோகபூர்வ மின்னஞ்சல்களைப் பயன்படுத்துதல் வேண்டும். ஊழியர்கள் தனிப்பட்ட தொடர்பாடல்களுக்கு உத்தியோகபூர்வ மின்னஞ்சல்களைப் பயன்படுதுதலாகாது.

உத்தியோகபூர்வ மின்னஞ்சல்கள் என்பது "gov.lk" என்ற தளப் பெயருடன் அரசாங்கத்தால் வழங்கப்பட்ட மின்னஞ்சல் ஆகும். உத்தியோகபூர்வ மின்னஞ்சல் கணக்குகள், உத்தியோகபூர்வ தளங்கள் என்பதுடன், நிறுவனம், கணக்கை அணுகுவதற்கு, மின்னஞ்சல்களைப் படிப்பதற்கு அல்லது கணக்கை நீக்குவதற்கான உரிமையைக் கொண்டுள்ளது.

அனைத்து மின்னஞ்சல் இணைப்புகளும், மூலம் அல்லது உள்ளடக்கத்தைப் பொருட்படுத்தாது, எந்தவொரு அரசாங்க நிறுவனத்தின் கணினி முறைமையில் திறக்கப்படுவதற்கு அல்லது சேமிக்கப்படுவதற்கு முன்பு வைரஸ்கள் மற்றும் பிற அழிவுத் திட்டங்களுக்காக ஸ்கான் செய்யப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.10. மின்னஞ்சல்களின் பாதுகாப்பு மீதான கொள்கை

நிறுவனமானது, பொருந்தக் கூடிய அனைத்து பாதுகாப்பு அம்சங்களுடன் அவர்களது மின்னஞ்சல் கணக்குகளை கட்டமைத்தல் வேண்டும். தகவல் பாதுகாப்பை உறுதிப்படுத்துவதற்கு, மின்னஞ்சல் சேவையகமானது, தரவு பாதுகாப்பு தொடர்பான உரிய சட்டங்களுடன் இணங்கி ஒழுகுதல் வேண்டும்.

தீம்பொருள் இணைக்கப்பட்டுள்ளதாக அறியப்பட்ட மின்னஞ்சல்களை அகற்றவும், கோரப்படாத மற்றும் விரும்பத்தகாத ("ஸ்பாம்") மின்னஞ்சல் மூலம் இன்பாக்ஸ் குழப்பப்படுவதைத் தடுப்பதற்கும் தாபனம் மின்னஞ்சல் வடிகட்டிகளை அமைத்தல் வேண்டும்.மேலும், மின்னஞ்சல்கள் மூலம் உணர்திறன்மிக்க தகவல்களை அனுப்புகின்ற போது, அது குறியாக்கம் செய்யப்படுதல் வேண்டும்.

இலங்கை அரசாங்க வலையமைப்பினால் வழங்கப்பட்ட மின்னஞ்சல் கணக்குகளைப் பொறுத்த வரையில், மின்னஞ்சல் சேவை பாதுகாப்பாக உருவாக்கப்படுவதை உறுதிப்படுத்துவதற்கு தகவல் மற்றும் தொடர்பாடல் தொழில்நுட்ப முகவராண்மை தேவைப்படுவதுடன், மேற்பார்வை அல்லது ஒழுங்குபடுத்தும் தேவைப்பாடுகளுக்கு காலமுறை அடிப்படையில் பாதுகாப்பு ஆய்வு அறிக்கைகள் இலங்கை சேர்ட் இடமிருந்து பெறப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.11. டிஜிட்டல் கையொப்பங்கள் மீதான கொள்கை

பொருத்தமானவிடத்து, நிறுவனமானது டிஜிட்டல் கையொப்பங்களை நடைமுறைப்படுத்துதல் வேண்டும். அதேபோன்று, நம்பகத்தன்மை (authenticity), நேர்மை (integrity), மற்றும் மறுதலிப்பு (nonrepudiation) ஆகியவற்றை உறுதி செய்வதற்கு மின்னஞ்சல்களுக்கு டிஜிட்டல் கையொப்பங்கள் பயன்படுத்தப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.12. சுற்றுவட்டப் பாதுகாப்பு கட்டுப்பாடுகள் மீதான கொள்கை

இணைய தாக்குதல்களுக்கு எதிராக ஆதனங்களுக்கு (தகவல், கணினிகள், வலையமைப்புகள் மற்றும் முறைமைகள் ஆதனங்கள்) பாதுகாப்பை வழங்கவும், தீங்கிழைக்கும் மென்பொருள் இணையம் வழியாக ஆதனங்களை அணுகுவதிலிருந்து தடுப்பதற்கும் தாபனமானது, ஃபயர்வால்ஸ், ஊடுருவலைக் கண்டறியும் முறைமைகள் (intrusion detection systems) மற்றும் ஊடுருவலைக் தடுக்கும் முறைமைகள் (intrusion prevention systems) போன்ற அத்தகைய சுற்றுவட்டப் பாதுகாப்பு கட்டுப்பாடுகளை நிறுவுதல் வேண்டும்.

நிறுவனமானது, சுற்றுவட்டப் பாதுகாப்பு அச்சுறுத்தல் தரவுத்தளத்தை (threat databases) கிரமமாக இற்றைப்படுத்துதல் வேண்டும், தானியங்கும் இற்றைப்படுத்தல் ஏற்பாடுகளுடன் தீம்பொருள் எதிர்ப்பு நிறுவப்படுதல் வேண்டும், பொருத்தமான கட்டமைப்புகளுடன் இயல்புநிலை அமைப்புகளை (default settings) இற்றைப்படுத்துதல் வேண்டும், மற்றும் அத்தகைய சாதனங்களுக்கும், முறைமைகளுக்குமாக வழங்கப்பட்ட பயன்படுத்துபவரின் கணக்குகளின்

இயல்புநிலையை விற்பனையாளர் முடக்குதல் வேண்டும்.

தகவல் மற்றும் சைபர் பாதுகாப்பு நடைமுறைப்படுத்தல் வழிகாட்டியில் வழங்கப்பட்டுள்ள சாதனங்களைக் கட்டுப்படுத்தும் பாதுகாப்பு கட்டமைப்பு விபரங்கள் பற்றிய கண்ணோட்-டமொன்றை வழங்குகின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.13. தொலையியக்கி அணுகலைப் பெறுதல் மீதான கொள்கை

நிறுவனமானது, புவியியல் ரீதியாக தொலைதூர அமைவிடங்களினூடாக அதிகாரமளிக்கப்படாத அணுகலைத் தடுப்பதற்கு உள் வலையமைப்புகளுக்கு தொலையியக்கி அணுகலைப் பெறுதல் வேண்டும்.

தொலையியக்கி அணுகலானது, நிறுவனத்திற்கு பல தகவல் பாதுகாப்பு அச்சுறுத்தல்களை கொண்டு வருகின்றது. பொது இணையத்தில் தகவல்கள் செல்கின்றபோது ஒட்டுக்கேட்கும் ஆபத்து, முறைமைகள் அல்லது தரவினை அதிகாரமின்றி அணுகுதல் மற்றும் தரவு மற்றும் தீம்பொருள் தொற்றுகளை கண்காணித்தலும் கையாளுதலும் ஆகியவை தொலையியக்கி அணுகலுடன் இணைந்து காணப்படுகின்ற பொதுவான பாதுகாப்பு அபாயங்களாகும்.

தொலையியக்கி அணுகல் அபாயத்தைக் குறைப்பதற்கு, தாபனம் பாதுகாப்பான மெய்நிகர் தனியார் வலையமைப்புகளைப் (Virtual Private Networks) பயன்படுத்துதல் வேண்டும், அதிகாரமளிக்கப்பட்டு பயன்படுத்துபவர்கள் மட்டுமே தாபனத்தின் இனங்காணும் முகாமைத்துவத்தின் மற்றும் அணுகல் கட்டுப்பாட்டு கொள்கையின் அடிப்படையில் முறைமைகளை அணுகுவதற்கு அனுமதித்தல் வேண்டும், பல் காரணி உறுதிப்படுத்தலை நடைமுறைப்படுத்துதல் வேண்டும், வாடிக்கையாளர் சாதனங்களில் இருந்து தொலைநிலை அணுகலை பாதுகாக்க வேண்டும் என்பதுடன், நம்பகமான வலையமைப்புகளைப் பயன்படுத்துதலும் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.14. காப்பு மூலோபாயம் மீதான கொள்கை

நிறுவனமானது, அனர்த்தமொன்று ஏற்படுகின்ற சந்தர்ப்பத்தில், வழமையான செயற்பாடுகளை மீண்டும்கொண்டு வருவதற்குத் தேவையான காப்புத் தரவு, பதிவுகள், முறைமைகள், மென்பொருள், உருவாக்க விபரங்கள் மற்றும் பிறவேறு தகவல்களை மீட்டெடுக்க மூலோபாயமொன்றைக் கொண்டிருத்தல் வேண்டும். இந்த மூலோபாயம் தாபனத்தின் அனர்த்த மீட்பு திட்டத்துடன் இணைக்கப்படுதல் வேண்டும் (பிரிவு 4.6.1இனைப் பார்க்கவும்).

நிறுவனமானது எவையேனும் சீர்குலைந்த சேவைகளினை முழுமையாக மீளமைப்பதற்கு அல்லது மீட்பதற்கு காப்பு ஊடகங்கள் பயன்படுத்தப்பட முடியுமென்பதனை உறுதி செய்தல் வேண்டும்.

அரசாங்கத்தின் ஒழுங்குமுறைப்படுத்தும் தேவைப்பாடுகளின்படி, காப்பு ஊடகத்தில் எழுதப்பட்ட தரவானது பாதுகாக்கப்படுதல் வேண்டும்.

நிறுவனமானது, காப்பு அதிர்வெண்ணைத் தீர்மானிப்பதற்கு மீட்பு நேரம் நோக்கம் (Recovery Time Objective: RTO) மற்றும் மீட்பு புள்ளி நோக்கம் (Recovery Point Objective: RPO) ஆகியவற்றையும் வரையறுத்தல் வேண்டும்.

இது, ரன்சம்வெயார் மென்பொருள் உள்ளடங்கலாக எந்தவொரு தீங்கிழைக்கும் தாக்குதல்களிலிருந்தும் நேரடித் தரவினைப் பாதுகாப்பதற்காக நேரடித் தரவு மற்றும் காப்பு தரவுக்கு இடையே காற்று இடைவெளியொன்று (air gap) இருத்தல் வேண்டும் என்று பரிந்துரைக்கின்றது.

இது, காப்பு தரவு செயலாக்க தளத்தில் இருந்து பௌதீகரீதியில் தொலைவிலிருக்கின்ற தீப்பற்றாத, பாதுகாப்பான அமைவிடத்தில் சேமிக்கப்படுதல் வேண்டும் என்று மேலும்பரிந்துரைக்கின்றது. இது ஒரு தீ ஆதாரம், பாதுகாப்பான இடத்தில் சேமிக்கப்படும் என்று காப்புப்பிரதிகளில் ஏதேனும் மாற்றங்கள் மேற்கொள்ளப்பட்டுள்ள-னவா என்பதைக் கண்டறிவதற்கான பொறிமுறையொன்றும் நடைமுறைப்படுத்தப்படுதல் வேண்டும்.

"மிக இரகசியமானது" மற்றும் "இரகசியமானது" என்று பெயரிடப்பட்ட தகவல் ஆதனங்களைக் கொண்ட காப்புப்பிரதிகள், ஆதனங்கள் பதிவேட்டில் குறிப்பிடப்பட்டுள்ள பாதுகாப்பு தேவைப்பாடுகளுக்கு ஏற்ப சேமிக்கப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.15.அரசாங்க நிறுவனங்களால் வழங்கப்பட்ட சொத்துக்களின் பாதுகாப்பு மீதான கொள்கை

இன்று பல அரச மற்றும் அரச சார்பற்ற நிறுவனங்கள் அரசாங்கத்தால் வழங்கப்படும் தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களில் (டிஜிட்டல் உள்கட்டமைப்பு, இலத்திரனியல் சேவைகள், பயன்பாடுகள்) செயல்படுகின்றன. இச்சூழலில், தகவல் தொடர்பாடல் தொழில்நுட்ப நிறுவனம் (Information Communication Technology Agency: ICTA) அல்லது பிற அரசு நிறுவனங்கள் தங்களால் உருவாக்கப்பட்ட தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பு, நம்பகத்தன்மை (reliability), நேர்மைத்துவம் (integrity) மற்றும் துல்லியம் (accuracy) ஆகியவற்றை உறுதி செய்ய வேண்டும். உதாரணமாக, லங்கா அரச வலையமைப்பு (Lanka Government Network), லங்கா அரச கிளவுட் (Lanka Government Cloud), மின்னஞ்சல் சேவை (Email Service), லங்கா அரசு கட்டண முறை (Lanka Government Payment System), குறுஞ்செய்தி சேவை (Short Message Service), ஆவண மேலாண்மை அமைப்பு (Document Management System) அல்லது பிற சேவைகளின் பாதுகாப்பு, அத்தகைய உள்கட்டமைப்பை உருவாக்கிய தொடர்புடைய நிறுவனத்தால் உத்தரவாதம்

அளிக்கப்பட வேண்டும். இந்த உள்கட்டமைப்புகளுக்கு தேவையான பாதுகாப்பு சான்றிதழ்கள் இலங்கை சேர்ட் இலிருந்து அல்லது வேறு ஏதேனும் தகுதி வாய்ந்த நிறுவனத்திடம் இருந்து சம்பந்தப்பட்ட நிறுவனங்களால் பெறப்படுதல் வேண்டும்.

இணக்கம்: தகவல் தொடர்பாடல் தொழில்நுட்ப நிறுவனம் மற்றும் அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.16. வடிவமைப்பு மூலமான பாதுகாப்பு மீதான கொள்கை

இந்த அமைப்பு மென்பொருள் பெறுகைகள் மற்றும் உள்ளக மென்பொருள் உருவாக்கத்தில் வடிவமைப்பு மூலம் பாதுகாப்பு என்ற அணுகுமுறையைப் பின்பற்றுதல் வேண்டும். வடிவமைப்பு மூலம் பாதுகாப்பு என்ற அணுகுமுறை மென்பொருள் வளர்ச்சி வாழ்க்கை சுழற்சியின் ஒவ்வொரு கட்டத்திற்கும் பாதுகாப்பு அவதானிப்புகளை சேர்ப்பதன் மூலம் பாரம்பரிய மென்பொருள் வளர்ச்சி அணுகுமுறையை நீடிக்கின்றது.

மென்பொருளை உருவாக்குவதில் (அல்லது மென்பொருளைப் பெறுவதில்), நிறுவனம், பாதுகாப்பு திட்டமிடல் மற்றும் கருத்திட்ட திட்டமிடல் நிலையில் ஆபத்து பற்றிய மதிப்பீடுகளை நடத்துதல், விலைமனு ஆவணங்களில் பாதுகாப்பு தேவைப்பாடுகளை வரையறுத்தல்.

வடிவமைப்பில், அபிவிருத்திக் கட்டத்தில் பாதுகாப்பு கட்டிடமைப்பை மதிப்பாய்வு செய்தல், பாதுகாப்பு தொடர்பான பலவீனங்களை (குறைபாடுகள்) கண்டறிவதற்கான வளர்ச்சி கட்டத்தில் குறியீட்டை மதிப்பாய்வு செய்தல் மற்றும் அமைப்புகளில் உள்ள பாதுகாப்பு பலவீனங்களை அடையாளம் காண செயல்படுத்தும் கட்டத்தில் பாதிப்பு மதிப்பீடுகளைச் செய்தல்.

இறுதியில், முறைமை நீக்கப்படுகின்ற நிலையில், அமைப்புகள் அதன் தரவு மற்றும் பிற தகவல் ஆதனங்களை அனுமதியளிக்கப்படாத தனிநபர்களால் அணுகவும் மீட்கவும் முடியாது என்பதை உறுதி செய்வதற்கு முறைமைகள் பாதுகாப்பாக அகற்றப்படுதல் வேண்டும்.

"தகவல் மற்றும் சைபர் பாதுகாப்பினை நடைமுறைப்படுத்தும் வழிகாட்டி" பாதுகாப்பான பிரயோகத்தை விருத்தி செய்யும் வாழ்க்கை சுழற்சி பற்றிய விபரங்களை வழங்குகின்றது.

இந்த நிறுவனம் சைபர் பிரயோகங்களை விருத்தி செய்கின்ற போது, இலங்கை 'சேர்ட்' டினால் வழங்கப்பட்ட அரச நிறுவனங்களுக்கான "இணைய தள பாதுகாப்பு வழிகாட்டுதல்கள், சைபர் பிரயோக பாதுகாப்புக்கான வழிகாட்டல்கள்", என்பவற்றை பின்பற்றுதல் வேண்டும்.

இந்த வழிகாட்டுதல்களை www.onlinesafety.lk எனும் இணைய தளத்திலிருந்து பதிவிறக்கம் செய்யலாம்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.17 சொத்துக்களை. பாதுகாப்பாக அகற்றுதல் மீதான கொள்கை

சொத்துக்கள் இதற்கு மேலும் தேவைப்படாத போது முறையான நடைமுறையைப் பயன்படுத்தி பாதுகாப்பாக அகற்றப்படுதல் வேண்டும்.

கட்புல ஊடகங்கள் (சிடிக்கள் அல்லது டிவிடிகள்), காந்த ஊடகம் (நாடாக்கள் அல்லது இறுவட்டுக்கள்), வட்டு இயக்கிகள் (வெளிப்புற, சிறிய அல்லது தகவல் முறைமைகளிலிருந்து அகற்றுதல்), ஃபிளாஷ் ஞாபக சேமிப்பு சாதனங்கள் (எஸ்எஸ்டிகள் அல்லது யுஎஸ்பி ஃபிளாஷ் டிரைவ்கள்) மற்றும் ஆவணங்கள் (காகித ஆவணங்கள், காகித வெளியீடு அல்லது புகைப்பட ஊடகம்) ஆகியவற்றை உள்ளடக்குகின்ற, ஆனால் அதற்குள் வரையறுக்கப்படாத நிறுவனங்களின் சேமிப்பு ஊடகம் பாதுகாப்பாக அகற்றப்படுதல் வேண்டுமென்று தேவைப்படுத்தப்படுகின்றது.

இனி தேவைப்படாத தகவல்கள் ஊடகத்தில் இருந்தால், அசல் தகவலை மீட்டெடுப்பதைத் தடுப்பதற்கு, தகவல் மீட்க முடியாத முறையில் நீக்கப்படுதல் வேண்டும். துறைசார் வடிவமைப்பு (sector-based formatting) என்பது ஊடகங்களில் உள்ள தகவல் ஆதனங்களை அகற்றுவதற்கான சாத்தியமான முறையாகும். தகவல் ஆதனங்களைக் கொண்ட ஊடகங்களை நிரந்தரமாக அழிப்பதற்கான சாத்தியமான வழிகள் துண்டாக்குதல் அல்லது குத்துதல் ஆகும்.

சேமிப்பு ஊடகத்தில் உள்ள ஆதனங்கள் "மிக இரகசியமானது" அல்லது "இரகசியமானது" என வகைப்படுத்தப்பட்டால், தகவல் பாதுகாப்பு குழுவிடமிருந்து அகற்றும் நடவடிக்கைக்கு முறையான அனுமதியைப் பெற்றதன் பின்னர், ஊடகங்களை பௌதீகரீதியாக அழிப்பதே பாதுகாப்பான முறையாகும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.18. உள்ளக தகவல் சைபர் பாதுகாப்பு கணக்காய்வுத் திட்டம் மீதான கொள்கை

நிறுவனமானது, தகவல் தொழில்நுட்ப பாதுகாப்பு கட்டுப்பாட்டு ஆய்வுகள், பிரயோகப் பாதுகாப்பு கட்டுப்பாட்டு மீளாய்வுகள், வலையமைப்பு நிருமாண மீளாய்வுகள், தகவல் தொழில்நுட்ப செயல்முறை ஆய்வுகள், பாதுகாப்பு இணக்க மீளாய்வுகள், உள்ளக மற்றும் வெளிப்புற பாதிப்பு பற்றிய மதிப்பீடுகள் (vulnerability assessments), ஊடுருவல் பற்றிய சோதனை மற்றும் வலையமைப்பு பிரயோக ஊடுருவல் சோதனை (penetration tests) ஆகியவற்றை உள்ளடக்கிய, ஆனால் அதற்குள் மட்டுப்படுத்தப்படாத வழக்கமான ஆய்வுகளை நடத்துவதற்கு நிறுவனம் முறையானதொரு உள்ளக தகவல் பாதுகாப்பு ஆய்வுத் திட்டத்தைக் கொண்டிருத்தல் வேண்டும்.

மதிப்பீடுகளானவை, சம்பவமொன்று நிகழ்ந்ததன் பின்னர், மாற்றமொன்று அறிமுகப்படுத்தப்பட்டதன் பின்னர் (பிரயோகத்திற்கு அல்லது பேணுகின்ற சூழலுக்கு), நியமத்தில் அல்லது வழிகாட்டல்களில் மாற்றங்கள்

ஏற்பட்டதன் பின்னர், வைரஸ் அல்லது தீம்பொருள் பரவியதன் பின்னர், அல்லது தகவல் பாதுகாப்பு குழுவினால் தீர்மானிக்கப்பட்டதன் பின்னர், காலத்திற்குக் காலம் (குறைந்தபட்சம் ஆண்டுதோறும்) மேற்கொள்ளப்படுதல் வேண்டும்.

நிறுவனத்தின் (பிரதான) உள்ளக கணக்காய்வாளர் ஆய்வினை ஒருங்கிணைத்தல் வேண்டும் என்பதுடன், ஒவ்வொரு அமைச்சினதும் பிரதான உள்ளக கணக்காய்வாளர் அதன் அதிகாரத்தின் கீழ் தாபனங்களின் தகவல் பாதுகாப்பு ஆய்வுகளை ஒருங்கிணைத்தல் வேண்டும்.

கணக்காய்வு அறிக்கைகளில் எழுப்பப்பட்ட பரிந்துரைகளை நடைமுறைப்படுத்துவதை பார்வையிடுவதற்காக முறைசார் செயன்முறை நிறுவனத்தால் நிறுவப்படவுள்ளது. அமைப்பின் (பிரதான) உள்ளக கணக்காய்வாளர் தலைமையை எடுத்து இந்த செயல்முறையினைப் பொறுப்பேற்றல் வேண்டும்.

அத்தகைய ஆய்வுகளை மேற்கொள்வதற்கு தகைமை வாய்ந்த தரப்பொன்றினால் ஆய்வுகள் மேற்கொள்ளப்படுதல் வேண்டும் அல்லது இலங்கை சேர்டின் சேவையைப் பெற வேண்டும். ஆய்வுகள் மூன்றாம் தரப்பினரால் மேற்கொள்ளப்பட வேண்டுமாயின், தாபனத்தின் ஆதனங்களின் இரகசியத்தன்மையை உறுதி செய்வதற்கு, வெளிப்படுத்தல் அல்லாத ஒப்பந்தம் (Non Disclosure Agreement) கைச்சாத்திடப்படுதல் வேண்டும் என்பது அத்தியவசியமானகும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.19. பயன்படுத்துவதற்கு முன்னரான கணக்காய்வுகள் மீதான கொள்கை

உள்ளக தகவல் பாதுகாப்பு ஆய்வுத் திட்டத்திற்கு இணையாக, தாபனமானது, நேரடி சூழலில் எந்தவொரு இணையத்தளத்தை, இணையப் பயன்பாட்டை அல்லது முறைமையைப் பயன்படுத்துவதற்கு முன்னர் பாதிப்புப் பற்றிய மதிப்பீடுகள் மற்றும் ஊடுருவல் சோதனைகளை (vulnerability assessment and penetration tests) மேற்கொள்ளுதல் வேண்டும்.

இந்த மதிப்பீடுகளை, இலங்கை சேர்ட் உடன் கலந்தாலோசித்து தகுதியான மூன்றாம் தரப்பினரால் நடத்துவதற்கு அல்லது இலங்கை சேர்ட் இனது சேவையை இந்நிறுவனம் பெறுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.20. முறைமைகளைக் கடினமாக்குதல் மீதான கொள்கை

நிறுவனமானது, சாத்தியமான தாக்குதல் வெக்டர்கள் நீக்குவதன் மூலம் மற்றும் முறைமைகளின் தாக்குதல் மேற்பரப்பினை ஒடுக்குவதன் மூலம் அவற்றின் மேற்பரப்பின் பாதிப்பினைக் குறைப்பதற்கு தகவல் தொழில்நுட்ப ஆதனங்களை கடினப்படுத்துதல் (hardening) வேண்டும். உதாரணமாக இயக்க அமைப்புகள்,

சேவையகங்கள், வலையமைப்புகள் மற்றும் வலையமைப்பு சாதனங்கள், தரவுத்தளங்கள், மற்றும் மெய்நிகர் தனியார் வலையமைப்புகளை நிறுவனமானது கடினப்படுத்துதல் வேண்டும். கணினிகள் கடினப்படுத்துதல் பற்றிய வழிகாட்டுதல்கள் தகவல் பாதுகாப்பு செயலாக்க வழிகாட்டியில் வழங்கப்பட்டுள்ளன.

அனுபவம் வாய்ந்த மற்றும் திறமையான பணியாளர்களின் ஆதரவுடன் மட்டுமே கடினப்படுத்தும் முறைமைகள் மேற்கொள்ளப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.21. வீட்டிலிருந்து பணியாற்றுதல் மீதான கொள்கை

வீட்டிலிருந்து பணியாற்றுவதற்கு மாறுகின்ற போது (அல்லது தொலைதூர இடங்களில் இருந்து வேலை செய்யும் பொழுது), தகவல் பாதுகாப்பு அச்சுறுத்தல்கள் அதிகரித்துள்ளன. ஆகவே, பணியாளர்கள், தொலைதூரத்திலிருந்து வேலை செய்கின்றபோது சிறந்த பாதுகாப்பு நடைமுறைகளின் தொகுப்பை எடுத்துக்காட்டுகின்ற இலங்கை சேர்ட் இனால் வெளியிடப்பட்ட, "வீட்டிலிருந்து பணியாற்றுவதற்கான தகவல் பாதுகாப்பு வழிகாட்டல்களை" கடைப்பிடித்தல் வேண்டும். இது தொலைவிலிருந்து வேலை செய்வதற்கு அனுமதிக்கப்படுகின்ற போது நிறுவனத்தின் தகவல் தொழில்நுட்ப ஆதனங்களை பாதுகாப்பாக அணுகுவதை உறுதி செய்வதற்கு இலங்கை சேர்ட் டினால் வழங்கப்பட்ட "தகவல் தொழில்நுட்ப நிருவாகிகளுக்கான குறைந்தபட்ச வழிகாட்டல்களை" தகவல் தொழில்நுட்ப நிருவாகிகள் பின்பற்றுதல் வேண்டும்.

இதனை www.onlinesafety.lk எனும் இணைய தளத்திலிருந்து பதிவிறக்கம் செய்யலாம்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.22. உத்தியோகபூர்வ வேலைக்காக தங்களது சொந்த சாதனத்தை பயன்படுத்துதல்

நிறுவனமானது, பணியாளர்கள் தமது தனிப்பட்ட மடிக்கணினிகள், ஸ்மார்ட்போன்கள் மற்றும் 'டப்'புகளைப் பயன்படுத்தி உத்தியோகபூர்வ கடமைகளை மேற்கொள்வதற்கான அனுமதி தவிர்க்கப்பட வேண்டும்.

எனினும், தகவல் பாதுகாப்பு குழுவினால் தீர்மானிக்கப்பட்ட குறிப்பிட்ட சூழ்நிலைகளில், தாபனமானது, தகவல் பாதுகாப்பு உத்தியோகத்தரின் மேற்பார்வையின் கீழ், தேர்ந்தெடுக்கப்பட்ட பணியாளர்களை உத்தியோகபூர்வ கடமைகளை ஆற்றுவதற்கு தமது தனிப்பட்ட சாதனங்களைப் பயன்படுத்துவதற்கு அனுமதிக்கலாம்.

இதுபோன்ற சூழ்நிலைகளில், சாதனங்கள் நிறுவனத்தில் சரியான முறையில் பதிவு செய்யப்படுவதும்,

அத்தகைய சாதனங்கள் இந்தக் கொள்கைக்கு இணங்குவதை உறுதி செய்வதும் அவசியமாகும்.

எந்த சந்தர்ப்பத்திலும் "மிக இரகசியமானது" (Confidential) மற்றும் "இரகசியமானது" (Secret) என்று வகைப்படுத்தப்பட்ட தகவலை செயற்படுத்த அல்லது சேமிக்க பணியாளர்களின் தனிப்பட்ட சாதனங்கள் பயன்படுத்தப்படுதலாகாது.

உத்தியோகபூர்வ கடமைகளை ஆற்றுவதற்கு ஊழியர்களது தனிப்பட்ட சாதனங்கள் பயன்படுத்தப்படும்போது, தாபனமானது, பயன்படுத்துபவர்களின் கணக்குகள் வரையறுக்கப்பட்ட சிறப்புரிமைகளைக் கொண்டவை, கணக்குகள் வலுவான கடவுச்சொற்கள் மற்றும் பல் ஆக்கக்கூற்று உறுதிப்படுத்தப்படுதலுடன் பாதுகாக்கப்படுகின்றன, தீம்பொருள் எதிர்ப்பு மென்பொருள் நிறுவப்பட்டு, தானியங்கி இற்றைப்படுத்தல்கள் செயற்படுத்தப்படுகின்றன, இயக்க முறைமைகள், பயன்பாட்டு மென்பொருள் மற்றும் பயன்படுத்தப்படுகின்ற ஏனைய பிரயோக மென்பொருள் தேவையான இணைப்பு இற்றைப்படுத்தல்களுடன் செல்லுபடியாகும் உரிமங்களைக் கொண்டுள்ளன என்பவற்றை உறுதிப்படுத்துதல் வேண்டும்.

மேலும் உத்தியோகபூர்வ வேலைக்கு தனிப்பட்ட சாதனங்ககளில் தனிப்பட்ட மற்றும் நிறுவனத் தகவல்களை மதிப்பாய்வு செய்ய அல்லது தக்க வைத்துக்கொள்ள அல்லது விசாரணை அல்லது சட்டத் தேவையின் போது அரசாங்க முகவர் அல்லது மூன்றாம் தரப்பினருக்கு தகவலை வெளியிடுவதற்கான உரிமையை நிறுவனம் கொண்டுள்ளது.

தனிப்பட்ட சாதனத்தின் பாதுகாப்பானது, சாதனத்தின் உரிமையாளரின் பொறுப்பாகும். சாதனத்தின் பயன்பாட்டின் காரணமாக தனிப்பட்ட தரவை இழப்பது உள்ளடங்கலாக சாதனத்திற்கு ஏற்படும் இழப்பு அல்லது சேதத்திற்கு தாபனம் பொறுப்பேற்காது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.23. பாதுகாப்பற்ற வலையமைப்புகளினைப் பயன்படுத்துவது மீதான கொள்கை

நிறுவனத்தின் ஊழியர்கள், உத்தியோகபூர்வ மின்னஞ்சல் மற்றும் உத்தியோகபூர்வ மென்பொருள் தீர்வுகளை அணுகுவதற்கு நம்பமுடியாத வைஃபை வலையமைப்புகள் (உ.ம். ஹோட்டல்கள், உணவகங்கள், பேருந்து தரிப்பிடங்களில் கிடைப்பவை) மற்றும் பிற பொதுவில் பகிரப்பட்ட தனிப்பட்ட கணினிகள், கியோஸ்க்குகள் (kiosks) மற்றும் ஏனைய தொடர்புடைய சாதனங்கள் போன்ற பாதுகாப்பற்ற வலையமைப்புகளைப் பயன்படுத்துவதைத் தவிர்த்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.24. வழங்குனர் முகாமைத்துவம் மீதான கொள்கை

தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை உருவாக்கி நிருவகிப்பதில் வெளிப்புறத் தரப்பினர்

(வன்பொருள், மென்பொருள், வலையமைப்புக்கள், ஹோஸ்டிங் மற்றும் நிருவகிக்கப்பட்ட சேவைகள் போன்றவை) ஈடுபடும் போது தகுந்த நடவடிக்கைகள் எடுக்கப்படுவதை நிறுவனம் உறுதி செய்யும்.

தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களை அபிவிருத்தி செய்வதிலும் முகாமைசெய்வதில் வெளித் தரப்பினர் ஈடுபடுகின்ற போது பொருத்தமான நடவடிக்கைகள் எடுக்கப்படுவதை நிறுவனம் உறுதி செய்யும். இது வன்பொருள், மென்பொருள் மற்றும் பேணுதல் சேவை வழங்குநர்களுக்கு மட்டுமே ஏற்புடையது, ஆனால் அதற்குள் மட்டுப்படுத்தப்பட்டதல்ல.

விற்பனையாளர் முகாமைத்துவத்தை மேற்கொள்வதில், தாபனம் குறைந்தபட்சம் பின்வருவனவற்றைக் கவனத்தில் கொள்ள வேண்டியிருக்கின்றது: (அ) காப்பு, சேமிப்பு, மீட்பு மற்றும் இடைநேர் ஏற்பாடுகள், பாதுகாப்பு கட்டமைப்புகள், தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்கள் போன்றவற்றை அணுகுதல் ஆகியன உள்ளடங்கலாக, ஆனால் இதற்குள் மட்டுப்படுத்தப்படாத ஒப்பந்தத் தரப்பினரின் பொறுப்புகள் மற்றும் கடமைகளை இனங்காணுதல், (ஆ) அரசாங்கத்தால் தெளிவுபடுத்தப்பட்ட-வாறு தாபனத்தால் உருவாக்கப்பட்ட தகவல் பாதுகாப்பு நடைமுறைகளைப் பின்பற்றுதல், (இ) ஒப்பந்தத்துடன் தொடர்புபட்டுள்ள ஒப்பந்த தரப்பின் செயல்முறைகளையும், கட்டுப்பாடு-களையும் ஆய்வு செய்யும் உரிமை, மற்றும் (ஈ) ஒப்பந்த நியதிகள் மற்றும் நிபந்தனைகளை பின்பற்றாதது பற்றிய கண்காணிப்பும், அறிக்கையிடலும். ஒப்பந்த தரப்புகளுடனான உறவுகளை முகாமை செய்கின்ற பொறுப்பு, நிறுவனத்தின் தலைமை உத்தியோகத்தரினால் தீர்மானிக்கப்-பட்டவாறு, நியமிக்கப்பட்ட சொத்து உரிமையாளர்கள், நியமிக்கப்பட்ட அதிகாரிகள் அல்லது நிறுவனங்களுக்கு ஒதுக்கப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.25. மாற்றல் முகாமைத்துவம் மீதான கொள்கை

நிறுவனமானது, அனைத்து மாற்றங்களையும் கட்டுப்படுத்துதல் வேண்டும். முகாமை செய்யப்படாத மாற்றங்கள் தகவல் மற்றும் தகவல் தொழில்நுட்ப சாதனங்களுக்கு அபாயங்களை ஏற்படுத்துகின்றன என்பதுடன், செயல்பாட்டு இடையூறுகளை ஏற்படுத்தும் திறனையும் கொண்டுள்ளன. உதாரணமாக, கட்டுப்பாடற்ற நிறுவல்கள் (அல்லது நிறுவல் நீக்கங்கள்), உட்புகுத்தல்கள், நீக்குதல்கள் மற்றும் முறைமைகளுக்கான மாற்றங்கள், இரகசியத்தன்மை, நேர்மை மற்றும் தரவு கிடைக்கும் பண்புக்கூறுகளை பாதிக்கலாம் அல்லது முறைமையின் தொகுப்பிற்கு வழிவகுக்கும் முறைமைக்கு பாதிப்புகளை ஏற்படுத்தலாம்.

மேலும், மாற்றங்களில் ஈடுபட்டுள்ள ஊழியர்கள், செயல்பாட்டுத் தகவலின் இரகசியத்தன்மைக்கு அச்சுறுத்தல்களை ஏற்படுத்தலாம். ஆகவே, முறைமைக்கான ஒட்டுமொத்த

பாதுகாப்பு ஆபத்தைக் குறைப்பதற்கு தகவல் பாதுகாப்பு குழு முறையானதொரு மாற்ற முகாமைச் செயல்முறையை அமுல்படுத்த வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.4. தகவல் பாதுகாப்பு சம்பவங்களைக் கண்டறிதல்

நிறுவனமானது, தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களை சரியான நேரத்தில் அடையாளம் காண பொருத்தமான நடவடிக்கைகளை செயற்படுத்துதல் வேண்டும். எந்தவொரு இணைய பாதுகாப்பு சம்பவங்கள், பாதிப்புகள் அல்லது கொள்கை மீறல்களை சம்பந்தப்பட்ட அதிகாரிகளுக்கு தெரிவிக்குமாறு அமைப்பு ஊழியர்களுக்கு அறிவுறுத்தும். மேலும், நிகழ்வுகளை அடையாளம் காண பதிவுகளை பகுப்பாய்வு செய்வதற்கான வழிமுறைகளை அமைப்பு வரிசைப்படுத்துகிறது மற்றும் தொடர்ச்சியான கண்காணிப்பு தீர்வுகளை பின்பற்றுகிறது, இது ஒழுங்கற்ற செயல்பாடுகள் மற்றும் செயல்பாட்டு தொடர்ச்சிக்கான பிற அச்சுறுத்தல்களைக் கண்டறியும்.

4.4.1. சம்பவங்களை அறிக்கையிடுதல் மீதான கொள்கை

சந்தேகத்திற்கிடமான நடவடிக்கை அல்லது ஏதேனும் பாதுகாப்பு மீறல் குறித்து உடனடியாக தகவல் பாதுகாப்பு உத்தியோகத்தருக்கு தெரிவிக்குமாறு பணியாளர்களுக்கு தெளிவாக ஆலோசனையளிக்கப்படுதல் வேண்டும். பாதுகாப்பு மீறல்களானவை, வலையமைப்பு, தொலைத்தொடர்பு அல்லது கணினி முறைமைகளுக்கு அதிகாரமளிக்கப்படாத அணுகல், கணினிகளில் வைரஸ் வெளிப்படையாக இருப்பது, நிறுவனங்களால் தடை செய்யப்பட்ட எந்தவொரு சொத்தின் வெளிப்படையான இருப்பு, அதிகாரமளிக்கப்படாத பயன்படுத்து-நரால் எந்தவொரு கோப்பிலும் வெளிப்படையான மோசடி, மற்றும் பிறிதொரு பயன்படுத்துநர் அல்லது ஒப்பந்தக்காரரால் இந்த வழிகாட்டல்கள் அல்லது பாதுகாப்புக் கொள்கை மீறப்படுதல் ஆகியவற்றை உள்ளடக்குகின்றன, ஆனால் அதற்குள் அவை மட்டுப்படுத்தப்படவில்லை. தகவல் தொழில்நுட்ப சொத்துக்களில் தற்போதுள்ள ஏதேனும் பாதிப்புகள் பற்றி தெரிவிக்குமாறு பயன்படுத்துபவர்களுக்கு ஆலோசனை வழங்கப்படுதல் வேண்டும்.

நிறுவனமானது, சம்பவங்களைக் கண்டறிதல், கண்டறியப்பட்ட தகவல் பாதுகாப்பு நிகழ்வுகளை அறிக்கையிடுதல் மற்றும் ஆதாரங்களைப் பாதுகாத்தல் போன்றவை பற்றி பணியாளர்களுக்கு போதுமான விழிப்புணர்வு மற்றும் பயிற்சிகளை வழங்குதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.4.2. பதிவுகளை மீளாய்வு செய்தல் மீதான கொள்கை

நிறுவனமானது, முறைமைகள் மற்றும் நிகழ்வுகளை கண்டறிவதற்கு இணைக்கப்பட்டுள்ள கூறுகள் மூலம் உருவாக்கப்பட்ட பதிவுகளைப் (அணுகல் பதிவுகள் (access logs), பிழையான பதிவுகள் (error logs), சேவையக பதிவுகள் (server logs), ஆய்வுப் பதிவுகள் (audit logs), பாதுகாப்புச்சுவர் பதிவுகள் (firewall logs) மற்றும் தீம்பொருள் எதிர்ப்பு பதிவுகளினைப் (antivirus logs) பேணுதல் மற்றும் மீளாய்வு செய்தல் வேண்டும்.

நிறுவனமானது, முறைமைகள் மீது தீங்கிழைக்கும் தாக்குதல்களைக் கண்டறிவதற்கும், பிழைகள் அல்லது பாதுகாப்பு மீறல்களுக்கான காரணங்களைத் தீர்மானிப்பதற்கும் கிரமமாக பதிவுகளை மீளாய்வு செய்தல் வேண்டும்.

பதிவுகள், மோசடி மற்றும் அதிகாரமளிக்கப்படாத அணுகலுக்கு எதிராக பாதுகாக்கப்படுதல் வேண்டும். முக்கியமான மற்றும் தனிப்பட்ட முறையில் அடையாளம் காணக்கூடிய தகவல்களைக் கொண்ட பதிவுகளைப் பொறுத்தவரை, சேமித்து பகுப்பாய்வு செய்வதற்கு முன்னர் பொருத்தமான தனியுரிமை பாதுகாப்பு நடவடிக்கைகள் எடுக்கப்படுதல் வேண்டும்.

பதிவுகளானவை, 12 மாத காலத்திற்கு அல்லது தகவல் பாதுகாப்பு குழுவினால் தீர்மானிக்கப்பட்டவாறு வைத்திருக்கப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.4.3. நிகழ்வுகளை தொடர்ந்தும் கண்காணித்தல் மீதான கொள்கை

நிறுவனமானது, தீங்கிழைக்கும் நடவடிக்கைகளைக் கண்டறிவதற்கான வலையமைப்புகள் அல்லது முறைமைகளைக் கண்காணித்தல் வேண்டும் என்பதுடன், ஊடுருவலைக் கண்டறியும் முறைமைகள் மற்றும் ஊடுருவலைத் தடுக்கும் முறைமையை (ஊடுருவலைக் கண்டறியும் முறைமைகள்/ ஊடுருவலைக் தடுக்கும் முறைமைகள்) நடைமுறைப்படுத்-துவதன் ஊடாக அத்தகைய நடவடிக்கைகளை எதிர்கொள்ளுதல் வேண்டும்.

நிறுவனமானது, பாதுகாப்பு கண்காணிப்பு மற்றும் அதிகளவான அச்சுறுத்தல் மற்றும் சம்பவத்தைக் கண்டறிவதற்கான பாதுகாப்பு தகவல் மற்றும் நிகழ்வு முகாமைத்துவ முறைமைகளைப் பயன்படுத்த முடியும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.4.4. இலங்கை சேர்ட்டிற்கு நிகழ்வுகளை அறிக்கையிடுதல் மீதான கொள்கை

தகவல் பாதுகாப்பு குழு தீர்மானித்ததன்படி, தொழில்நுட்ப ஆலோசனை மற்றும் கையாளுதல்

ஆகியவற்றிற்காக முக்கியமான தகவல் பாதுகாப்பு சம்பவங்களை உடனடியாக இலங்கை சேர்ட்டிற்கு அறிக்கையிடுமாறு நிறுவனத்திற்கு ஆலோசனை வழங்கப்படுகின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.5. சம்பவங்களுக்குப் பதிலளித்தல்

தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களுக்கு திறம்பட பதிலளிப்பதற்காக, நிறுவனம் ஒரு சம்பவ மறுமொழி திட்டத்தை உருவாக்கி, ஒரு சம்பவம் நடந்தால் திட்டத்தை செயல்படுத்த வேண்டும். தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களுக்கு பதிலளிப்பதில் நிறுவனம் இணங்க வேண்டிய கொள்கைகள் கீழே கொடுக்கப்பட்டுள்ளன.

4.5.1. சம்பவத்திற்கு பதிலளிக்கும் திட்டம் மீதான கொள்கை

ஒரு நிறுவனத்தின் சொத்துக்களுக்கு எதிரான தகவல் மற்றும் இணையப் பாதுகாப்பு சம்பவத்தின் எதிர்மறையான விளைவுகளைக் கண்டறிந்து, பதிலளிப்பதற்கு மற்றும் கட்டுப்படுத்துவதற்கு, முன்னரே தீர்மானிக்கப்பட்ட அறிவுறுத்தல்கள் மற்றும் நடைமுறைகளின் தொகுப்பைக் கொண்ட ஒரு சம்பவ மறுமொழித் திட்டத்தை நிறுவனம் உருவாக்கும். சம்பவத்திலிருந்து திறம்பட மீள்வதற்கான தெளிவான வழிமுறைகள் மற்றும் நடைமுறைகளும் இதில் அடங்கும்.

சம்பவத்திற்கு பதிலளிக்கும் திட்டமானது (Incident Response Plan), குறைந்தபட்சம், சம்பவத்தை அறிக்கையிடும் நடைமுறைகள், கண்டறிதல், பகுப்பாய்வுக்கான உபாயங்கள் மற்றும் சம்பவங்களைக் கட்டுப்படுத்துதல் (ஒழிப்பு அல்லது மீட்பு), நியமிக்கப்பட்ட பதவியினர்க்கு தகவல் பாதுகாப்பு பொறுப்புகளை ஒதுக்குதல் மற்றும் சம்பவங்களுக்கு பின்னரான மீளாய்வுகள் தொடர்பான நடைமுறைகள் ஆகியவற்றைக் கொண்டிருத்தல் வேண்டும்.

சம்பவத்திற்கு பதிலளிக்கும் திட்டமானது, அவ்வப்போது சோதிக்கப்பட்டு, நிறுவனத்தின் அனைத்து பதவியினர்க்கும் தெரிவிக்கப்படுதல் வேண்டும்.

ஒரு சம்பவ மறுமொழித் திட்டத்தை உருவாக்குவதற்கான வழிகாட்டுதல்கள் தகவல் மற்றும் சைபர் பாதுகாப்பு நடைமுறைப்படுத்தல் வழிகாட்டியில் வழங்கப்பட்டுள்ளன.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.5.2. சம்பவத்திற்கு பதிலளிக்கும் திட்டத்தைச் செயற்படுத்துதல் மீதான கொள்கை

ஒரு தகவல் பாதுகாப்பு சம்பவம் ஏற்பட்டால், நியமிக்கப்பட்ட அங்கீகரிக்கப்பட்ட நபர், நிறுவன நடவடிக்கைகளில் தாக்கத்தை குறைக்க, சம்பவத்திற்குப் பிறகு இயல்பான செயற்பாடுகளை மீண்டும் தொடங்க, சம்பவ மறுமொழி திட்டத்தை செயற்படுத்துதல் வேண்டும்.

சம்பவங்கள் தொடர்பான தகவல்களைப் பதிவு செய்ய ஒரு சம்பவப் பதிவேட்டை (Incidents Register) நிறுவனம் பேணுதல் வேண்டும். சம்பவப் பதிவேட்டில் குறைந்தபட்சம் பின்வரும் தகவல்கள் இருக்க வேண்டும்: சம்பவத்தின் தேதி மற்றும் நேரம், சம்பவத்தைப் புகாரளித்த பணியாளரின் பெயர் மற்றும் பதவி, சம்பவத்தின் விளக்கம், தாக்கத்தின் தன்மை, சம்பவத்தின் வகைப்பாடு, சம்பவத்திற்கு பதிலளிக்கும் வகையில் எடுக்கப்பட்ட நடவடிக்கை சம்பவம், சம்பவத்தை கையாளும் உத்தியோகத்தர், சம்பவத்தின் தற்போதைய நிலை மற்றும் ஏனைய விடயங்கள்.

சம்பவங்களுக்கு பதிலளிப்பதற்கான வழிகாட்டுதல்கள் தகவல் மற்றும் சைபர் பாதுகாப்பு அமுலாக்கல் வழிகாட்டியில் வழங்கப்பட்டுள்ளன.

ஒரு தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவம் நடந்தால், தடயவியல் விசாரணைகளில் பயன்படுத்தக்கூடிய ஆதாரமாக செயல்படக்கூடிய தகவலை அடையாளம் காணவும், சேகரிக்கவும் மற்றும் பாதுகாக்கவும் அமைப்பு நடைமுறைகளை தொடங்க வேண்டும். தடயவியல் விசாரணை தொடர்பான கொள்கைகள் பிரிவு 4.5.3 இல் வழங்கப்பட்டுள்ளன.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.5.3. தடயவியல் விசாரணைகள் மீதான கொள்கை

தடயவியல் விசாரணை (Forensic Investigation) தேவைப்படும் பட்சத்தில், அமைப்பு முறையான விசாரணை செயல்முறையை பின்பற்றுதல் வேண்டும். தடயவியல் விசாரணை தொடர்பான ஆதாரங்களை இயற்பியல் ஆவணங்கள், வன் இறுவட்டுக்களில் உள்ள தரவு, சாதனப் பதிவுகள், CCTV காட்சிகள், மின்னஞ்சல் பதிவுகள், குரல் பதிவுகள் மற்றும் ஏனைய மின்னணு பதிவுகள் போன்ற பரந்த அளவிலான மின்னணு வழிமுறைகள் மூலம் கைப்பற்ற முடியும்.

இலத்திரனியல் சான்றுகள் பாரம்பரிய ஆதாரங்களில் இருந்து வேறுபட்டதாக இருப்பதால், அதன் இயல்பு, நிலையற்ற தன்மை (volatility) மற்றும் பிரதிபலிப்பு (intangibility), அத்தகைய ஆதாரங்களைக் கையாள நிபுணத்துவ அறிவு அவசியம். அத்தகைய தொழில்நுட்ப திறன்களைக் கொண்ட இலங்கை சேர்ட் அல்லது தொடர்புடைய நிறுவனத்திடம் இருந்து இந்த அமைப்பு தொழில்நுட்ப உதவியைப் பெறுதல் வேண்டும்.

தடயவியல் விசாரணையில், குறைந்தபட்சம் பின்வரும் தகவல்கள் தேவைப்படும். நிறுவனத்தால் காவலில்

(chain of custody) வைக்கப்படும் போது பயன்படுத்தப்பட்ட சங்கிலி: சம்பவம் மற்றும் சேகரிக்கப்பட்ட ஆதாரங்களின் விவரங்கள், சேகரிக்கப்பட்ட ஆதாரங்களின் திகதி மற்றும் நேரம், ஆதாரம் பெறப்பட்ட பெயர் மற்றும் பதவி மற்றும் ஆதாரங்களை மாற்றிய வரலாறு. விசாரணையில் அளிக்கப்படும் காவலில் இருக்கும் சங்கிலியை தகவல் பாதுகாப்பு உத்தியோகத்தர் பராமரித்தல் வேண்டும்.

நடப்பு, நிலுவையில் உள்ள அல்லது எதிர்பார்க்கக்கூடிய உரிமை கோரல்களைப் பற்றிய அனைத்து ஆதாரங்களையும் தக்கவைத்து பாதுகாக்கும் பொறுப்பை நிறுவனத்தின் தகவல் பாதுகாப்பு உத்தியோகத்தர் கொண்டிருத்தல வேண்டும். ஆதாரமாகப் பயன்படுத்தக்கூடிய ஆவணங்கள், மின்னணுப் பதிவுகள் அல்லது ஒத்த கருவிகளை இழக்கவோ, அழிக்கவோ அல்லது வேண்டுமென்றே மாற்றவோ கூடாது என்ற பொறுப்பும் இதில் உள்ளடங்கும்.

தடயவியல் விசாரணையில், தனிப்பட்ட தரவு பாதுகாப்பு, கணினி குற்றங்கள், பணம் செலுத்தும் சாதன மோசடிகள் மற்றும் மின்னணு பரிவர்த்தனைகள் தொடர்பான சட்ட கட்டமைப்புகள் பயன்படுத்தப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.6. இயல்பான செயல்பாடுகளை மீட்டெடுத்தல் மீதான கொள்கை

நிறுவனமானது, அனர்த்தத்தின் காரணமாக பாதிக்கப்பட்ட எந்தவொரு இயலுமைகளையும் அல்லது சேவைகளையும் வழமைக்குக் கொண்டு வருவதற்குரிய பயனுள்ள நடவடிக்கைகளின் திட்டமொன்றை உருவாக்கி நடைமுறைப்படுத்துதல் வேண்டும்.

பேரழிவுகள் அல்லது தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களில் இருந்து மீள்வதில் நிறுவனம் இணங்க வேண்டும் என்ற கொள்கை அறிக்கைகள் கீழே தரப்பட்டுள்ளன.

4.6.1. அனர்த்த மீட்புத் திட்டம் மீதான கொள்கை

நிறுவனமானது, அனர்த்தமொன்று (அல்லது சம்பவம்) ஏற்படுகின்ற சந்தர்ப்பத்தில், அத்தகைய அனர்த்தத்திலிருந்து (அல்லது சம்பவம்) மீள்வதற்கு வசதியாக அனர்த்த மீட்புத் திட்டமொன்றை (Disaster Recovery Plan) கொண்டிருத்தல் வேண்டும்.

அனர்த்த மீட்புத் திட்டமானது, அனர்த்தத்திலிருந்து மீள்வதற்கு மேற்கொள்ளவேண்டிய செயற்பாடுகள்

மற்றும் திட்டத்தில் உள்ள ஒவ்வொரு குழு உறுப்பினரினதும் வகிபாகத்தையும், பொறுப்புகளையும் கொண்டிருத்தல் வேண்டும்.

அனர்த்த மீட்புத் திட்டமானது இடர் மதிப்பீடொன்றையும், தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களின் வணிக தாக்கம் பற்றிய பகுப்பாய்வையும் நடத்துவதன் மூலம் வடிவமைக்கப்படுதல் வேண்டும் என்பதுடன், மீட்பு நடவடிக்கைகளானவை தரவுகளை (மீட்பு நேர நோக்கம்) மீட்டெடுப்பதற்கு ஏற்றுக்கொள்ளக்கூடிய காலத்தின் ஆரம்ப புள்ளி மற்றும் அனர்த்தமொன்றுக்கு பின்னர் (மீட்பு புள்ளி நோக்கம்) தாபனத்தின் தொழிற்பாடுகள் மற்றும் முறைமைகளையும் ஆரம்பிக்க வேண்டிய முன்னைய புள்ளியைக் கருத்தில் கொண்டு வடிவமைக்கப்படுதல் வேண்டும்.

இந்த அனர்த்த மீட்புத் திட்டமானது, காலாந்தர அடிப்படையில் பரிசோதிக்கப்பட்டு இற்றைப்படுத்தப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.6.2. அனர்த்த மீட்புத் திட்டத்தைச் செயற்படுத்துதல் மீதான கொள்கை

அனர்த்தமொன்று ஏற்படுகையில், நியமிக்கப்பட்ட அதிகாரமளிக்கப்பட்ட நபர், நிறுவனத்தின் செயற்பாடுகளில் தாக்கத்தைக் குறைப்பதற்கும், நிகழ்வொன்றுக்குப் பின்னர் வழமையான நடவடிக்கைகளை மீள ஆரம்பிப்பதற்கும் அனர்த்த மீட்புத் திட்டத்தைச் செயற்படுத்துதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.6.3. நெருக்கடியின் போதான தொடர்பாடல் மீதான கொள்கை

நிறுவனத்தின் தலைமைத்துவத்தினால் தீர்மானிக்கப்பட்டபடி பாரியதொரு நெருக்கடி (முக்கியமான பேரழிவு, ணைய பாதுகாப்பு சம்பவம்) ஏற்படுகின்றவிடத்து திட்டமொன்றி-ன்படி, நிறுவனத்தின் பொறுப்பான அமைச்சுகள், இலங்கை சேர்ட், பாதிக்கப்பட்டவர்கள், ஊடகங்கள், சேவை நாடுநர்கள் மற்றும் சட்டத்தை நடைமுறைப்படுத்தும் அதிகாரிகள் போன்ற அத்தகைய உள்ளக மற்றும் வெளியகத் தரப்புகளுடன் தொடர்பு கொள்ளுதல் வேண்டும்.

இந்த நிறுவனம், நெருக்கடியை உரிய அக்கறைதாரர்களுக்குத் தெரிவிப்பதற்கு பொறுப்பு வாய்ந்த சிரேஷ்ட அதிகாரியை நியமித்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்

5.முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்

நிறுவனத்தின் தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையினை அமுல்படுத்தும் பொருட்டு, பின்வரும் கொள்கைகள் முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டியுள்ளன.

கொள்கை விடயம்	கொள்கை இல.	முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்	அனைத்து நிறுவனங்கள்	மு.தே.த.உ* வழங்குனர்கள்
தகவல் மற்றும் சைபர் பாதுகாப்பு நிர்வாக முறை	4.1.1	நிறுவனத் தலைவரினால் தகவல் மற்றும் சைபர் பாதுகாப்பு கொள்கையினை அமுல்படுத்துவதற்கான தலைமைத்துவத்தினை வழங்குதல்.	✓	✓
	4.1.2	தகவல் மற்றும் சைபர் பாதுகாப்பு நிருவாக கட்டமைப்பொன்றினைத் தாபித்தல்.	✓	✓
	4.1.2 (அ)	தகவல் பாதுகாப்பு உத்தியோகத்தர் மற்றும் தகவல் மற்றும் தகவல் பாதுகாப்பு பொறுப்புக்கள் குழுவொன்றினை நியமித்தல்		✓
	4.1.2 (ஆ)	தகவல் பாதுகாப்பு உத்தியோகத்தர் இல்லாவிடின், தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதற்கு பிரதம தகவல் உத்தியோகத்தரிடம் பொறுப்புக்களைக் கையளித்தல்.	✓	

	4.1.2 (இ)	தகவல் மற்றும் சைபர் பாதுகாப்பு கணக்காய்வுகளை ஒருங்கிணைப்பதற்கு (பிரதம) IA பொறுப்புக்களைக் கையளித்தல்.	✓	✓
	4.1.3	தகவல் பாதுகாப்பு குழு ஒருவரை நியமித்தல்	✓	✓
	4.1.4	இடர் முகாமைத்துவ குழு ஒருவரை நியமித்தல்.		✓
	4.1.5	பயனர் பொறுப்புக்களை அடையாளங் காணுதலும் பயனர்களுடன் தொடர்பு கொள்ளுதலும்.	✓	✓
	4.1.6	தகவல் மற்றும் சைபர் பாதுகாப்புக்கான உத்தியோகபூர்வ பொறுப்பின் திறன் விருத்தி.	✓	✓
	4.1.7	முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்களினை அல்லது மிக இரகசியமான மற்றும் இரகசியமான தகவல் சொத்துக்களைக் கையாளும் பதவியினர் மீது பாதுகாப்பு அனுமதி மற்றும் பின்னணி சோதனைகளை நிறைவேற்றுதல்.		✓
	4.1.8	நிறுவனத்தின் நோக்கு, செயற்பணி மற்றும் நோக்கங்களுடன் தகவல் மற்றும் சைபர் பாதுகாப்பு நடவடிக்கைகளினை ஒழுங்குமுறைப்படுத்துதல்.	✓	✓
	4.1.9	தகவல் மற்றும் சைபர் பாதுகாப்பு செயல்திட்டங்களை விருத்தி செயதலும் அமுல்படுத்துதலும்.	✓	✓

சொத்துக்கள், சொத்து உரிமையாளர்கள் மற்றும் இடர்களை அடையாளங் காணுதல்.	4.2.1	தகவல், தகவல் தொழில்நுட்ப சொத்துக்கள் மற்றும் முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்கள் என்பவற்றினை அடையாளங் காணுதல்.	✓	✓
	4.2.3	சொத்து உரிமையாளர்கள், பாதுகாவலர்களை அடையாளங் காணுதலும் சொத்துக்களைப் பாதுகாப்பதற்கான பொறுப்பினை கையளித்தலும்.	✓	✓
	4.2.4	தகவல் மற்றும் தகவல் சொத்துப் பதிவேடுகளினைப் பேணுதல்.	✓	✓
	4.2.5	தகவல் மற்றும் தகவல் சொத்துக்களுக்கான இடர் மதிப்பீடுகளினை மேற்கொள்ளுதல்.		✓
	4.2.6	தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை அவற்றின் பெறுமதி மற்றும் உணர்திறனின் அடிப்படையில் வகைப்படுத்துதல்.	✓	✓
சொத்துக்களைப் பாதுகாத்தல்	4.3.1	இறுதியில் தரவினைப் பாதுகாத்தல்	✓	✓
	4.3.2	இடைத்தங்கலில் தரவினைப் பாதுகாத்தல்	✓	✓
	4.3.3	தகவல் மற்றும் தகவல் சொத்துக்களின் பௌதீக ரீதியான பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
	4.3.4	தகவல் மற்றும் தகவல் சொத்துகளுக்கான பயனர் அணுகலினை கட்டுப்படுத்துதல்.	✓	✓
	4.3.5	உறுதியான அதிகாரத்தினை உறுதி செய்தல்.	✓	✓

	4.3.6	பொருத்தமான முறையில் தரவு இறைமையினை உறுதி செய்தல்.	✓	✓
	4.3.7	வலிதான உரிமம் பெற்ற மென்பொருட்களைப் பயன்படுத்துதலும் புதிய பொருட்களை இற்றைப்படுத்துதலும்.	✓	✓
	4.3.8	Antimalware மென்பொருளை நிறுவுதல்.	✓	✓
	4.3.9	உத்தியோகபூர்வ தொடர்பாடல்களுக்கு உத்தியோகபூர்வ மின்னஞ்சலினைப் பயன்படுத்துதல்.	✓	✓
	4.3.10	மின்னஞ்சல்களின் பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
	4.3.11	பொருத்தமான முறையில் டிஜிற்றல் கையொப்பங்களைப் பயன்படுத்துதல்.	✓	✓
	4.3.12	சுற்றளவு பாதுகாப்பு கட்டுப்பாடுகளை செயல்படுத்தவும்.	✓	✓
	4.3.13	தொலைவிலிருந்து அணுகும் பாதுகாப்பு முறைகளினைப் பயன்படுத்துதல்.	✓	✓
	4.3.14	காப்பு மூலோபாயத்தைப் பயன்படுத்துதல்	✓	✓
	4.3.16	மென்பொருள் விருத்தி மற்றும் கொள்ளல் நடவடிக்கைகளின் போது வடிவமைப்பு கோட்பாடுகளின் மூலமாக பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
	4.3.17	சொத்துக்களின் விற்பனைப் பாதுகாப்பினை உறுதி செய்தல்.	✓	✓

	4.3.18	உள்ளக தகவல் பாதுகாப்பு கணக்காய்வு செயன்முறையொன்றினை அமுல்படுத்துதல்.	✓	✓
	4.3.19	இடர் மதிப்பீடுகளினை மேற்கொள்ளுதல், உத்தியோகபூர்வ இணையத்தளத்தினை ஆரம்பிப்பதற்கு முன்பாக ஊடுருவல் சோதனைகளினை மேற்கொள்ளுதல், சைபர் பயன்பாடுகள் அல்லது வேறு ஏதேனும் முறைமையினை மேற்கொள்ளுதல்.	✓	✓
	4.3.20	தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பு கண்காணிப்பினை வலுப்படுத்துதல்	✓	✓
	4.3.21	தொலைவிலிருந்து வேலை செய்யும்போது வீட்டிலிருந்து வேலை செய்வதற்கான வழிகாட்டுதல்களைப் பின்பற்றவும்.	✓	✓
	4.3.23	நம்பகமற்ற வலையமைப்புக்களைப் பயன்படுத்துவதை தடுத்தல்	✓	✓
	4.3.24	வழங்குனர்களை முகாமை செய்தல்	✓	✓
	4.3.25	மாற்றங்களை முகாமை செய்தல்.	✓	✓
சம்பவங்களைக் கண்டறிதல்	4.4.1	சம்பவங்கள் தொடர்பில் அறிக்கையிடுமாறு பதவியினருக்கு அறிவுறுத்துதல்.	✓	✓
	4.4.2	சம்பவங்களை அடையாளங் காண்பதற்கு குறிப்பேடுகளினை மீளாய்வு செய்தல்	✓	✓
	4.4.3	நிகழ்வுகளினை தொடர்ச்சியாக கண்காணிப்பதன் மூலம் சம்பவங்களை அடையாளங் காணுதல்		✓

	4.4.4	இலங்கை சேர்ட்டிற்கு நிகழ்வுகளை அறிக்கையிடல்.	✓	✓
நிகழ்வுகளுக்குப் பதிலளித்தல்	4.5.1	நிகழ்வு பதிலளிப்பு திட்டமொன்றினை விருத்தி செய்தல்.	✓	✓
	4.5.2	சம்பவ நிகழ்வொன்றில் சம்பவ பதிலளிப்பு திட்டத்தினைச் செயற்படுத்துதல்.	✓	✓
	4.5.3	சம்பவங்கள் மீதான தடயவியல் விசாரணைகளினை மேற்கொள்ளுதல்.	✓	✓
சாதாரண தொழிற்பாடுகளினை மீட்டல்	4.6.1	பேரழிவு மீட்புத் திட்டமொன்றினை விருத்தி செய்தல்.	✓	✓
	4.6.2	பேரழிவு நிகழ்வின் போது பேரழிவு பேரழிவு மீட்புத் திட்டமொன்றினை செயற்படுத்துதல்.	✓	✓
	4.6.3	நெருக்கடித் தொடர்பாடல் திட்டத்தினை விருத்தி செய்தல்	✓	✓

* **மு.தே.த.உ வழங்குநர்கள்: முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்கள்**

6. தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையினை கண்காணித்தல் மற்றும் மதிப்பாய்வு செய்வதற்கான முறை

6.1 தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையை நடைமுறைப்படுத்துவதற்கு முன்பாக, அரசாங்க வளங்களைப் பாதுகாப்பதற்காக தகவல் பாதுகாப்பினைக் கடைப்பிடிப்பது தொடர்பில் அரச நிறுவனங்களின் தற்போதைய நிலையைக் கண்டறிவது அவசியமானதொன்றாகும். எனவே இத்தகைய மதிப்பீட்டுக் கருவியானது, தகவல் மற்றும் சைபர் பாதுகாப்புத் தயார் நிலையை அமுல்படுத்துவதில் அரசாங்க தாபனத்தின் தற்போதைய தகுதி நிலையைக் கண்டு பிடிக்கும் வகையில் வடிவமைக்கப்பட்டுள்ளது.

6.2 அதற்கிணங்க இலங்கை சேர்ட் ஆனது பிரிவு 6.6 இல் தரப்பட்டுள்ள வினாக்களின் அடிப்படையில் கொள்கையினை அமுல்படுத்துவது தொடர்பில் அரசாங்க நிறுவனங்களின் தயார் நிலை குறித்து பூர்வாங்க மதிப்பீட்டினை மேற்கொள்ளும். காண்புகளின் அடிப்படையில், கொள்கையினை அமுல்படுத்துவது தொடர்பில் அரசாங்க நிறுவனங்களுக்கு பரிந்துரைகள் வழங்கப்படும்.

6.3 இலங்கை சேர்ட் ஆனது வருடாந்த அடிப்படையில் ஒவ்வொரு அரசாங்க நிறுவத்தின் மூலமாகவும் கொள்கை இணக்கப்பாட்டு மட்டத்தினை மதிப்பாய்வு செய்து தகவல் மற்றும் சைபர் பாதுகாப்பு சுட்டெண் (Information and Cyber Security Index) மீதான இணக்கப்பாட்டு மட்டத்தினை வழங்கும். இலங்கை சேர்ட் ஆனது நிறுவனத்தின் ஒட்டுமொத்த தகவல் மற்றும் சைபர் பாதுகாப்பு தயார்நிலையை மேம்படுத்துவதற்கான பரிந்துரைகள் வழங்கும்.

6.4 நிறுவனத்தில் கொள்கை அமுலாக்கலினை செயலாற்றுகையினை (அல்லது தயார்நிலை) மதிப்பாய்வு செய்வதற்கு, ஏறக்குறைய 50 வினாக்கொத்துக்களைக் கொண்டுள்ள பிரிவு 6.6 இல் சமர்ப்பிக்கப்பட்ட வினாக்கொத்தானது பயன்படுத்தப்படும். தகவல் பாதுகாப்பு உத்தியோகத்தர், பிரதான புத்தாக்க உத்தியோகத்தர், அல்லது தகவல் தொழில்நுட்ப பாடத்திற்குப் பொறுப்பான உத்தியோகத்தர், இந்த மதிப்பீட்டை பூர்த்தி செய்து, ஒவ்வொரு வருடமும் அக்டோபர் 30 ஆம் திகதி அல்லது அதற்கு முன்னதாக நிறுவன தலைவரின் கையொப்பத்துடன் இலங்கை சேர்ட்க்கு அனுப்பி வைக்கப்படுதல் வேண்டும்.

6.5 ஒவ்வொரு வினாவுக்கும் விரிவாக பதிலளிக்க விரும்பும் பதிலளிப்பவர் மதிப்பீட்டு வினாக் கொத்தின் இறுதியில் குறிப்புக்கள் பிரிவில் விரிவாக பதிலளிக்க முடியும். பதிலளிப்பவர் உரிய பதங்களின் விரிவான விளக்கத்திற்காக இந்த ஆவணத்தின் சொற்களஞ்சியத்தினைப் பார்க்கலாம்.

6.6 **மதிப்பீட்டு வினாக் கொத்து**

அனைத்து அரசாங்க நிறுவனங்களும் அவற்றின் அறிவுக்கு எட்டிய வரையில் ஒவ்வொரு வினாவுக்கும் விடையளிக்குமாறு கேட்டுக் கொள்ளப்படுகின்றன.

கொள்கை உசாத்துணை	**மதிப்பீட்டு வகையீடு**	**கொள்கை**	**இணக்கம் ஆம்**	**இல்லை**	**குறிப்புக்கள்**
தகவல் மற்றும் சைபர் பாதுகாப்பு நிர்வாக முறை					
பாதுகாப்பு நிறுவன கட்டமைப்பு	1. தகவல் பாதுகாப்பு உத்தியோகத்தர் ஒருவரை நிறுவனம் நியமித்துள்ளதா?	4.1.2 (அ)			
	2. தாபனம் தகவல் பாதுகாப்பு உத்தியோகத்தருக்கு பொறுப்புக்களை உரித்தளித்துள்ளதா?	4.1.2 (அ)			
	3. தகவல் பாதுகாப்பு உத்தியோகத்தர் நியமிக்கப்பட்டிருக்கா விட்டால், நிறுவனமானது தகவல் தொழில்நுட்பம் உரித்தளிக்கப்பட்ட தகவல் பாதுகாப்பு பொறுப்புக்கள் விடயத்திற்குப் பொறுப்பான உத்தியோகத்தரோ அல்லது பிரதான புத்தாக்க உத்தியோகத்தரினையோ கொண்டுள்ளதா?	4.1.2 (அ)			
	4. நிறுவனமானது (பிரதான) உள்ளக கணக்காய்வாளருக்கு தகவல் பாதுகாப்பு கணக்காய்வு பொறுப்புக்களை வழங்கியுள்ளதா?	4.1.2 (இ)			

	5. நிறுவனமானது தகவல் பாதுகாப்பு அல்லது தகவல் தொழில்நுட்பம் குறித்த தீர்மானங்களை மேற்கொள்வதற்கான குழுவினைக் கொண்டுள்ளதா?	4.1.3			
	6. நிறுவனமானது தகவல் சைபர் பாதுகாப்பு தொடர்பான இடர்கள் குறித்த தீர்மானங்களை மேற்கொள்வதற்கான குழுவினைக் கொண்டுள்ளதா?	4.1.4			
இறுதிப் பயனர் பொறுப்புக்கள்	7. நிறுவனமானது பயனர்களுக்கு இறுதிப் பயனர் பொறுப்புக்களை குறித்து விளக்கமளித்துள்ளதா?	4.1.5			
திறன் விருத்தி	8. பொறுப்புக்கூறும் நபர்களின் தகவல் பாதுகாப்பு திறனை மேம்படுத்துவதற்கு நிறுவனம் ஏதேனும் நடவடிக்கை எடுத்திருக்கிறதா?	4.1.6			
பின்னணி செவ்வை பார்த்தல்கள்	9. “மிக இரகசியம்” மற்றும் “இரகசியம்", தகவல் சொத்துக்கள் அல்லது முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வழங்குநர்கள் அணுகல் ஆகியவற்றைக் கையாளும் அதிகாரிகளின் பின்னணிச் சோதனைகள் மற்றும் பாதுகாப்பு அனுமதியை தங்களின் நிறுவனம் மேற்கொள்கிறதா?	4.1.7			
மூலோபாய வரிசை	10. நிறுவனத்தின் செயல்பாடுகள், கொள்கைகள், உத்திகள் அல்லது திட்டங்களை வடிவமைத்து செயல்படுத்துவதில், உங்கள் நிறுவனம் தகவல் பாதுகாப்பை கணக்கில் எடுத்துள்ளதா?	4.1.8			
செயல்திட்டம்	11. தங்களது நிறுவனம் தகவல் பாதுகாப்பு நடவடிக்கைகளுக்கான	4.1.9			

	நிதி எற்பாடுகளினைக் கொண்டுள்ளதா?				
	12. தங்களது நிறுவனம் அதன் தகவல் பாதுகாப்பு நோக்கங்களை அடைவதற்கு விருத்தி செய்யப்பட்ட செயல்திட்டங்களை வைத்துள்ளதா?	4.1.10			
சொத்துக்கள், உரிமையாளர்கள், பயனர்கள் மற்றும் இடர்களினை அடையாளங் காணுதல்					
சொத்துக்களை அடையாளங் காணுதல்	13. நிறுவனத்திற்கு பெறுமதி சேர்க்கும் தகவல் சொத்துக்களை உங்களின் நிறுவனம் அடையாளங் கண்டு வைத்துள்ளதா?	4.2.1			
	14. உங்களின் நிறுவனமானது தகவல் சொத்துக்களுடன் இணைந்துள்ள இடரினை மதிப்பீடு செய்துள்ளதா?	4.2.5			
	15. உங்களின் நிறுவனமானது தகவல் சொத்துக்கைளை அவற்றின் முக்கியத்துவம் வாய்ந்த மற்றும் வேறு வழிகளிலான தாக்கத்தின் அடிப்படையில் வகைப்படுத்தியுள்ளதா?	4.2.6			
	16. உங்களின் நிறுவனமானது தகவல் சொத்து பதிவேட்டில் தகவல் சொத்துக்களைப் பதிவு செய்துள்ளதா?	4.2.4			
	17. உங்களின் நிறுவனம் தகவல் தொழில்நுட்பச் சொத்துக்களை அடையாளங் கண்டுள்ளதா?	4.2.1			
	18. உங்களின் நிறுவனம் தகவல் தொழில்நுட்ப சொத்துப் பதிவேடொன்றில் தகவல் தொழில்நுட்பச் சொத்துக்களைப் பதிவு செய்துள்ளதா?	4.2.4			
	19. உங்களின் நிறுவனம் தகவல் தொழில்நுட்ப சொத்துக்களை அவற்றின் முக்கியத்துவத்தின்	4.2.6			

	அடிப்படையில் வகையீடு செய்துள்ளதா?				
	20. உங்களின் நிறுவனம் சொத்துக்களின் உரிமையாளர்களை அடையாளங் கண்டுள்ளதா?	4.2.3			
சொத்துக்களைப் பாதுகாத்தல்					
குறியாக்கம்	21. உங்கள் நிறுவனம் முக்கியமான தகவலை சேமிப்பிற்கு முன் குறியாக்கம் (encrypt) செய்கிறதா?	4.3.1			
	22. இலத்திரனியல் அலைவரிசைகள் மூலம் நகரும் முன் உங்கள் நிறுவனம் முக்கியமான தகவல்களை குறியாக்கம் செய்கிறதா?	4.3.2			
பௌதீக பாதுகாப்பு	23. உங்கள் நிறுவனம் பாதுகாப்பான பகுதிகளில் முக்கியமான தகவல்களைச் செயலாக்குகிறதா அல்லது சேமிக்கிறதா?	4.3.3			
	24. தீ, வெள்ளம், ஈரப்பதம் மற்றும் வெப்பநிலை ஆகியவற்றிலிருந்து பாதுகாப்பான பகுதிகளைப் பாதுகாக்க உங்கள் நிறுவனம் தகுந்த நடவடிக்கைகளை எடுத்திருக்கிறதா	4.3.3			
	25. பாதுகாப்பான பகுதிகளுக்கு அங்கீகரிக்கப்படாத நுழைவை உங்கள் நிறுவனம் தடுக்கிறதா?	4.3.3			
அடையாள முகாமைத்துவமும் அணுகு முறைக் கட்டுப்பாடும்	26. உங்கள் நிறுவனத்திற்கு அடையாள முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு கொள்கை (Identity and Access Management) உள்ளதா?	4.3.4			

	27. உங்கள் நிறுவனம் வலுவான அங்கீகாரத்தைப் (strong authentication) பயன்படுத்துகிறதா?	4.3.5			
தரவு இறையாண்மை	28. தங்களின் நிறுவனம் தரவு இணையாண்மையினை (data sovereignty) உறுதி செய்கின்றதா?	4.3.6			
	29. கிளவுட் சேவையைப் பெறுவதற்கு முன் உங்கள் நிறுவனம் ஆபத்தை மதிப்பிடுகிறதா?	4.3.6			
உரிமம் பெற்ற மென்பொருள் மற்றும் இணைப்புக்கள் இற்றைப்படுத்தல்கள்	30. நிறுவனம் செல்லுபடியாகும் உரிமம்(கள்) கொண்ட இயக்க முறைமைகளை பயன்படுத்துகிறதா?	4.3.7			
	31. விற்பனையாளர் வழங்கிய சமீபத்திய இணைப்புகள் மற்றும் திருத்தங்களுடன் நிறுவனத்தின் இயக்க முறைமை (கள்) புதுப்பிக்கப்பட்டுள்ளனவா?	4.3.7			
	32. விற்பனையாளருக்கு வழங்கப்பட்ட முக்கியமான இணைப்புகள் நிறுவப்படுவதை உறுதி செய்வதற்கான நடைமுறை உங்கள் நிறுவனத்திடம் உள்ளதா?	4.3.7			
தீம்பொருள்	33. நிறுவனம் அனைத்து இயந்திரங்களிலும் செல்லுபடியாகும் உரிமத்துடன் தீம்பொருள் எதிர்ப்பு (Antimalware) மென்பொருளை நிறுவியுள்ளதா?	4.3.8			
மின்னஞ்சல்	34. உத்தியோகபூர்வ தகவல் தொடர்புகளுக்காக தனிப்பட்ட மின்னஞ்சல்களைப் பயன்படுத்தும்	4.3.9			

	பயனர்களை உங்கள் நிறுவனம் கட்டுப்படுத்துகிறதா?				
	35. தீம்பொருள் இணைக்கப்பட்டுள்ள மின்னஞ்சல்களை அகற்ற தங்கள் நிறுவனம் மின்னஞ்சல் வடிப்பான்களை அமைக்கிறதா?	4.3.10			
	36. மின்னஞ்சல் வழியாக முக்கியமான தகவலை அனுப்பும்போது தங்களின் நிறுவனம் குறியாக்கத்தைப் பயன்படுத்துகிறதா?	4.3.10			
சுற்றளவுப் பாதுகாப்பு சாதனங்கள்	37. உங்கள் கணனி வலையமைப்பில் உங்கள் நிறுவனத்திடம் ஃபயர்வால் உள்ளதா?	4.3.12			
தொலைநிலை அணுகல் பாதுகாப்பு	38. தொலைநிலை அணுகலுக்கு உங்கள் நிறுவனம் பாதுகாப்பான வேர்ச்சுவல் தனியார் வலையமைப்புக்களை (Virtual Private Network) பயன்படுத்துகிறதா?	4.3.13			
	39. தொலைதூரத்தில் இணைக்கும் அனைத்து பயனர்களும் வேர்ச்சுவல் தனியார் வலையமைப்புக்களைப் பயன்படுத்துகிறார்களா?	4.3.13			
காப்புப் பிரதி மூலோபாயம்	40. உங்கள் நிறுவனம் தரவை காப்புப் பிரதி (backup) எடுக்கிறதா?	4.3.14			
	41. காப்புப்பிரதிகள் தரவுச் செயலாக்கத் தளத்திலிருந்து உடல் ரீதியாக தொலைவில் உள்ள தீ தடுப்பு, பாதுகாப்பான இடத்தில் சேமிக்கப்பட்டுள்ளதா?	4.3.14			

சொத்துக்களின் பாதுகாப்பான அகற்றல்	42. முக்கியமான தகவல்களைக் கொண்ட மின்னணு ஊடகங்களை அப்புறப்படுத்த உங்கள் நிறுவனம் பின்வருவனவற்றில் ஏதேனும் ஒன்றைப் பின்பற்றுகிறதா? - துண்டாக்குதல், குத்துதல், உடல் ரீதியாக சேதப்படுத்துதல், தேய்த்தல்.	4.3.17			
உள்ளக தகவல் பாதுகாப்பு கணக்காய்வு நிகழ்ச்சித்திட்டம்	43. தங்களின் நிறுவனம் உள்ளக தகவல் பாதுகாப்பு கணக்காய்வு நிகழ்ச்சித் திட்டமொன்றினை வைத்திருக்கின்றதா?	4.3.18			
	44. உங்கள் நிறுவனம் பாதிப்பு மதிப்பீடு மற்றும் ஊடுருவல் சோதனைகளை இலங்கை சேர்ட் மூலம் மென்பொருள் பயன்பாடுகளை வரிசைப்படுத்துவதற்கு முன் செயல்படுத்துகிறதா?	4.3.19			
	45. தங்களின் கணனி வலையமைப்பு களுக்கு பாதிப்பு மதிப்பீடு மற்றும் ஊடுருவல் சோதனையினைச் செயற்படுத்தியுள்ளீர்களா?	4.3.19			
வீட்டிலிருந்து வேலை	46. உங்களின் நிறுவனமானது இலங்கை சேர்ட்டினால் வழங்கப்பட்ட வீட்டிலிருந்து வேலைக்குரிய வழிகாட்டுதல்களை பின்பற்றுகின்றதா?	4.3.21			
சொந்த சாதனத்தினை அலுவலக தேவைக்குப் பயன்படுத்துதல்	47. சொந்த சாதனங்களைப் பதிவு செய்வதற்கான முறையான நடைமுறை எதனையும் தங்களின் நிறுவனம் கொண்டுள்ளதா?	4.3.22			
	48. முக்கியமான தரவினை செயன்முறைப்படுத்துவதற்கு அல்லது களஞ்சியப்படுத்துவதற்கு	4.3.22			

	சொந்த சாதனங்களைப் பயன்படுத்துவதற்கு தங்களின் நிறுவனம் அனுமதியளிக்கின்றதா?				
தகவல் பாதுகாப்பு நிகழ்வினை கண்டறிதல்					
நிகழ்வுகளினை அறிக்கையிடுதல்	49. சந்தேகத்திற்கிடமான செயல்பாடு, தொடர்பு, திருட்டு, வைரஸ், பாதிப்பு, அங்கீகரிக்கப்படாத அணுகல், கோப்புகளை சேதப்படுத்துதல் அல்லது பாதுகாப்புக் கொள்கையை மீறுதல் ஆகியவற்றை தகவல் பாதுகாப்புக்கு பொறுப்பான நபரிடம் தெரிவிக்குமாறு ஊழியர்களுக்கு தங்களின் நிறுவனம் அறிவுறுத்தியுள்ளதா?	4.4.1			
	50. நீங்கள் எப்போதாவது இலங்கை சேர்ட் இற்கு அல்லது வேறு ஏதேனும் தரப்புக்கு சைபர் பாதுகாப்பு நிகழ்வுகள் குறித்து அறிவித்துள்ளீர்களா?	4.4.4			
நிகழ்வுகளுக்குப் பதிலளித்தல்					
நிகழ்வுப் பதிலளிப்புத் திட்டமும் திட்டத்தினைச் செயற்படுத்துதலும்.	51. உங்களின் நிறுவனம் நிகழ்வுப் பதிலளிப்புத் திட்டமொன்றினை (Incidents Response Plan) விருத்தி செய்துள்ளதா?	4.5.1			
	52. தகவல் மற்றும் சைபர் பாதுகாப்பு நிகழ்வொன்றில், அதன் தொழிற்பாடுகளின் தாக்கத்தினைக் குறைப்பதற்கு அல்லது அத்தொழிற்பாட்டினை மீளச் சேமிப்பதற்கு நிகழ்வு பதிலளிக்கும் திட்டமொன்றினை நிறுவனம் செயற்படுத்தியுள்ளதா?	4.5.2			

சம்பவங்களிலிருந்து மீளுதல்					
பேரிடர் மீட்புத் திட்டமும் திட்டத்தினைச் செயற்படுத்துதலும்.	53. உங்களின் நிறுவனம் பேரிடர் நிகழ்வொன்றில் மீட்பினை வசதிப்படுத்துவதற்கு விருத்தி செய்யப்பட்ட பேரிடர் மீட்புத் திட்டமொன்றினை (Disaster Recovery Plan) வைத்துள்ளதா?	4.6.1			
	54. பேரிடர் நிகழ்வில் (அல்லது நிகழ்வு), தங்களின் நிறுவனமானது சீர்குலைந்த சேவைகளினை மீளமைப்பதற்கு அதன் பேரிடர் மீட்பு திட்டமொன்றினை செயற்படுத்துன்றதா?	4.6.2			

சொற்களஞ்சியம்

தீம்பொருள் எதிர்ப்பு (Antimalware)	தீம்பொருள் எதிர்ப்பு என்பது சாதனங்களில் உள்ள தீம்பொருளைக் கண்டறிய அல்லது கணினி முறைமைகள் அல்லது மின்னணு சாதனங்களில் தீம்பொருளைத் தாக்குவதைத் தடுக்க வடிவமைக்கப்பட்ட மென்பொருளாகும். மால்வேர் என்பது கணினி, சேர்வர் அல்லது கணினி வலையமைப்பிற்கு (உதாரணம் - வைரஸ்கள், புழுக்கள், ransomware) சேதம் விளைவிப்பதற்காக வேண்டுமென்றே வடிவமைக்கப்பட்ட மென்பொருளாகும்.
சொத்துக்கள் வகையீடு (Assets Classification)	வகைப்படுத்தல் என்பது தகவல் சொத்துக்களை அதன் உணர்திறன் நிலை, சிக்கலான நிலை மற்றும் அந்த தகவலைப் பகிர்வதால் ஏற்படும் தாக்கம் ஆகியவற்றின் அடிப்படையில் வகைப்படுத்தும் செயல்முறையாகும். நிறுவனத்திற்கு அதன் முக்கியத்துவத்திற்கு ஏற்ப தகவல் பொருத்தமான அளவிலான பாதுகாப்பைப் பெறுவதை உறுதி செய்வதே முதன்மை நோக்கமாகும்.
சொத்துக்களின் பாதுகாவலர் (Assets Custodian)	தகவல் சொத்து உரிமையாளரால் வரையறுக்கப்பட்ட தேவைகளுக்கு ஏற்ப, சேமித்து வைத்து, கொண்டு செல்லப்பட்டு அல்லது செயலாக்கப்படுவதால், வாழ்க்கைச் சுழற்சி முழுவதும் ஒரு தகவல் சொத்தைப் பாதுகாக்கும் பொறுப்பைக் கொண்ட நிறுவனத்தில் உள்ள நபர்.
சொத்துக்கள் உரிமையாளர் (Assets Owner)	ஒரு சொத்து உரிமையாளர் என்பவர் சொத்துக்களின் அன்றாட நிர்வாகத்திற்கு பொறுப்பாகவுள்ள ஆளொருவராவார்.
தகவலின் கிடைப்பனவு (Availability of Information)	கிடைப்பனவானது சரியான நேரத்தில், நம்பகமான அணுகல் மற்றும் தகவலைப் பயன்படுத்துவதை உறுதி செய்கிறது.
தகவல் சொத்துக்களின் இரகசியத்தன்மை (Confidentiality of Information)	இரகசியத்தன்மை என்பது அங்கீகரிக்கப்படாத நபர்களுக்கும் நிறுவனங்களுக்கும் தகவல் வெளியிடப்படாது என்ற உத்தரவாதத்தைக் குறிக்கின்றது.
உணர்திறன் மிக்க தகவல் சொத்துக்கள் (Sensitive Information Assets)	எந்தவொரு தகவல் இழப்பு, மாற்றம், தவறாகப் பயன்படுத்துதல், வெளிப்படுத்துதல் அல்லது தோல்வி ஆகியவை நிறுவனம் அல்லது தொடர்புடைய தனிநபர்கள்

	அல்லது நிறுவனங்களின் நலன்களை மோசமாக பாதிக்கலாம். இந்த தகவல் சொத்துக்களை அரசு நிறுவனத்தால் "மிக ரகசியம்", "ரகசியம்" மற்றும் "வரையறுக்கப்பட்ட பகிர்வு" என வகைப்படுத்தலாம்.
முக்கியமான/ உணர்திறன் மிக்க தகவல் சொத்துக்கள் (Critical IT Assets)	முக்கியமான தகவல் தொழில்நுட்ப சொத்துக்கள் அமைப்பு எனப்படுவது அங்கீகரிக்கப்படாத அணுகல், தவறான பயன்பாடு அல்லது தகர்வு ஆகியவை தகவல்/ அமைப்பு அல்லது தனிநபர்களை மோசமாக பாதிக்கலாம். இந்த அமைப்புகளுக்கு உயர் மட்ட பாதுகாப்பு தேவைப்படுகிறது மேலும் கீழே வரையறுக்கப்பட்டுள்ளபடி முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு வடிவத்திலும் இருக்கலாம். இந்த தகவல் பாதுகாப்பு சொத்துக்களை நிறுவனத்தால் "முக்கியத்துவம் வாய்ந்த" மற்றும் "மிகவும் முக்கியமான" என வகைப்படுத்தலாம்.
முக்கியமான தேசிய தகவல் உள்கட்டமைப்பு (Critical National Information Infrastructure)	முக்கியமான தகவல் உட்கட்டமைப்பு என்பது அமைப்புகள் அல்லது வசதிகளினைக் குறிப்பிடுகின்றது, அதன் இயலாமை அல்லது அழிவானது தேசிய பாதுகாப்பு, நிருவாகம், பொருளாதாரம், சுகாதாரம் மற்றும் ஒரு தேசத்தின் சமூக நலனில் பலவீனமான தாக்கத்தை ஏற்படுத்தும்.
டிஜிரல் கையொப்பங்கள் (Digital Signatures)	டிஜிட்டல் கையொப்பங்கள் என்பது டிஜிட்டல் செய்திகள் அல்லது ஆவணங்களின் நம்பகத்தன்மையை சரிபார்க்கும் கணித ரீதியான முறைமையாகும். இது அனுப்புநரின் நம்பகத்தன்மை (பயனர்களின் அடையாளம்), செய்தி ஒருமைப்பாடு (முறையற்ற மாற்றம் அல்லது அழிவுக்கு எதிராக பாதுகாப்பு) மற்றும் நிராகரிப்பு (உரிமைகோரப்பட்ட அனுப்புநர் பின்னர் ஆவணத்தை உருவாக்குவதை மறுக்க முடியாது) ஆகியவற்றை வழங்குகிறது.
குறியாக்கம் (Encryption)	மறைகுறியாக்கம் என்பது ஒரு எளிய உரைச் செய்தியை பாதுகாப்பான-குறியீடு செய்யப்பட்ட உரை வடிவமாக மாற்றும் செயல்முறையாகும், மறைகுறியாக்கம் மூலம் அதனை மீண்டும் மாற்றாமல் புரிந்து கொள்ள முடியாது.
அரசாங்க நிறுவனங்கள் (Government Organizations)	2016 ஆம் ஆண்டின் 12 ஆம் இலக்க தகவலுக்கான உரிமைச் சட்டத்தில் வரையறுக்கப்பட்ட பகிரங்க அதிகாரசபைகள் அரசாங்க நிறுவனங்களாகும்.

தகவல் பாதுகாப்பு கட்டுப்பாடுகள் (Information Security Controls)	பாதுகாப்புக் கட்டுப்பாடுகள் என்பது தகவல் மற்றும் தகவல் தொழில்நுட்பச் சொத்துக்களுக்கான பாதுகாப்பு அபாயங்களைத் தவிர்ப்பதற்கான, கண்டறிவதற்கான, எதிர்ப்பதற்கான அல்லது குறைப்பதற்கான பாதுகாப்பு அல்லது எதிர் நடவடிக்கைகளாகும். கட்டுப்பாடுகள் என்பது தொழில்நுட்பங்கள், கொள்கைகள், நடைமுறைகள் அல்லது தகவல் சொத்துக்களைப் பாதுகாக்க வைக்கப்படும் செயலிகளாக இருக்கும்.
தகவல் பாதுகாப்பு உத்தியோகத்தர் (Information Security Officer)	தகவல் பாதுகாப்பு உத்தியோகத்தர் என்பவர் என்பது நிறுவனத்தின் குறிக்கோள்கள், மூலோபாயம் மற்றும் தகவல் சொத்துக்கள் போதுமான அளவு பாதுகாக்கப்படுவதை உறுதி செய்வதற்கான செயல் திட்டங்களை நிறுவுதல் மற்றும் பராமரிப்பதற்கு பொறுப்பான ஒரு சிரேஷ்ட நிலையிலான நிருவாகி ஆவார்.
தகவல் பாதுகாப்பு குழு (Information Security Committee)	தகவல் பாதுகாப்புக் குழுவானது, தகவல் பாதுகாப்புத் திட்டமிடல், நிதியளித்தல், செயற்படுத்துதல் மற்றும் தகவல் பாதுகாப்பு நடவடிக்கைகள் செயற்படுத்தப்படுவதைக் கண்காணித்தல் உள்ளிட்டதகவல் பாதுகாப்பு தொடர்பான அனைத்து நடவடிக்கைகளையும் நிறுவனத்திற்குள் வழிநடத்தும் மற்றும் நிருவகிக்கும் குழுவினைக் குறிப்பிடுகின்றது..
தகவல் மற்றும் நிகழ்வு முகாமைத்துவ முறைமைகள் (Security Information and Event Management Systems)	தகவல் மற்றும் நிகழ்வு முகாமைத்துவ முறைமைகள் என்பது பதிவுக் கோப்புகளிலிருந்து சேகரிப்புத் தரவை பகுப்பாய்வு செய்தல் மற்றும் பாதுகாப்பு அச்சுறுத்தல்கள் மற்றும் நிகழ்வுகள் பற்றிய அறிக்கைகள் மற்றும் நிகழ்நேர கணினி கண்காணிப்பை ஒருங்கிணைத்து, முக்கியமான சிக்கல்களைப் பற்றி வலையமைப்பு நிருவாகிகளுக்குத் தெரிவிக்கின்றதுடன் பாதுகாப்பின் நிகழ்நேர பகுப்பாய்வை வழங்க பாதுகாப்பு நிகழ்வுகளுக்கிடையே வலையமைப்பு வன்பொருள் மற்றும் பிரயோகங்கள் மூலம் உருவாக்கப்பட்ட விழிப்பூட்டல்கள் தொடர்புகளை ஏற்படுத்துகிறது.
தகவல் மற்றும் சைபர் பாதுகாப்பு (Information and Cyber Security)	தகவல் பாதுகாப்பு என்பது ஒருமைப்பாடு, ரகசியத்தன்மை மற்றும் கிடைக்கும் தன்மையை உறுதி செய்வதற்காக அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, வெளிப்படுத்தல், இடையூறு, மாற்றம் அல்லது அழிவிலிருந்து சொத்துகளைப் பாதுகாப்பதனைக் குறிப்பிடுகின்றது. இது வெளளப் பெருக்கு தீ போன்ற ஏனைய இயற்கை பேரழிவுகளிலிருந்தும், சைபர்

	தொழில்நுட்பம் அல்லது வேறு ஏதேனும் வழிகளிலான பயன்பாட்டுடன் நனிநபர்களின் கேடு விளைவிக்கும் நடவடிக்கைகளிலிருந்து தகவல் சார்ந்த சொத்துக்களினைக் கொண்டிருக்கின்ற அல்லது பயன்படுத்துகின்ற தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பினை உள்ளடக்குகின்றது.
தகவல் சொத்துக்கள் (Information Assets)	தகவல் சொத்து என்பது நிறுவனத்திற்கு மதிப்புள்ள தகவல் அல்லது தரவினைக் குறிப்பிடுகின்றது.மின்னணு வடிவத்தில் கிடைக்கும் ஆவணங்கள், தரவுத்தள பதிவுகள் மற்றும் காகித வடிவத்தில் கிடைக்கும் ஆவணங்கள், தகவல் சொத்துகளுக்கான எடுத்துக்காட்டுகள்: சொற் கோப்புக்கள், படங்கள், தரவுத்தளத்தில் பணியாளர்களின் தனிப்பட்ட பதிவு என்பன இதில் உள்ளடங்கும்.
தகவல் தொழில்நுட்ப சொத்துக்கள் (IT Assets)	தகவல் தொழில்நுட்பசொத்து என்பது நிறுவனத்திற்கு மதிப்புள்ள எந்தவொரு தகவல் தொழில்நுட்ப உபகரணங்கள், தகவல் அமைப்பு, மென்பொருள், சேமிப்பு ஊடகம். கணினிகள், சேவையகங்கள், திசைவிகள், வட்டுகள், வலையமைப்புக்கள், மென்பொருள், தகவல் அமைப்புகள் மற்றும் அதன் கூறுகள் ஆகியவை தகவல் தொழில்நுட்பசொத்துகளுக்கான எடுத்துக்காட்டுகளாகும்.
ஊடுருவலைக் கண்டறியும் முறைமைகள்/ ஊடுருவலைக் தடுக்கும் முறைமைகள் (IPS/IDS)	ஊடுருவல் கண்டறிதல் அமைப்புகள் என்பது அறியப்பட்ட சைபர் தாக்குதல்களை அடையாளம் காண வலையமைப்பு போக்குவரத்தை பகுப்பாய்வு செய்யும் சாதனங்கள். ஊடுருவல் தடுப்பு அமைப்புகள் சாதனங்கள் வலையமைப்பு நெரிசலினை பகுப்பாய்வு செய்து அறியப்பட்ட சைபர் தாக்குதல்களை அடையாளம் காணுவதனைக் குறிப்பிடுகின்றது. இருப்பினும், அது கண்டறியும் தாக்குதல்களின் வகையின் அடிப்படையில் பாக்கெட் வழங்கப்படுவதைத் தடுப்பதன் மூலம் தாக்குதல்களை நிறுத்த முடியும்.
தகவலின் நேர்மைத்துவம் (Integrity of Information)	தகவலின் நேர்மைத்துவம் என்பது தவறான மாற்றம் அல்லது அழிவுக்கு எதிராக தகவல்கள் பாதுகாக்கப்படுவதனைக் குறிப்பிடுகின்றது. தகவலானது அதன் மூல வடிவத்தில் இருப்பதை இது உறுதி செய்கிறது.
உத்தியோகபூர்வ மின்னஞ்சல் (Official Email)	அதிகாரப்பூர்வ மின்னஞ்சல்கள் என்பது “gov.lk” என்ற டொமைன் பெயருடன் அரசாங்கத்தால் வழங்கப்பட்ட மின்னஞ்சல் கணக்குகள் ஆகும்.

தனிப்பட்ட கிளவுட் (Private Cloud)	தேர்ந்தெடுக்கப்பட்ட பயனர்களுக்கு மட்டுமே இணையம் அல்லது தனிப்பட்ட உள்ளக வலையமைப்பு மூலம் வழங்கப்படும் சேவைகள். உதாரணம் - லங்கா அரச கிளவுட்
பொது கிளவுட் (Public Cloud)	பொது கிளவுட் சேவையினை வாங்க விரும்பும் எவருக்கும் கிடைக்கக் கூடியதாக இருக்கும்.
மீட்பு புள்ளி நோக்கம் (Recovery Point Objective: RPO)	மீட்பு புள்ளி நோக்கம் (RPO) என்பது நிறுவனம் எவ்வளவு அடிக்கடி காப்புப்பிரதிகளை எடுக்க வேண்டும் என்பதற்கான அளவீடு ஆகும், மேலும் மீட்டெடுக்கப்பட்ட தரவு எவ்வளவு புதுப்பிக்கப்படும் என்பதைக் குறிக்கிறது. தரவை மீட்டெடுப்பதற்கு ஏற்றுக்கொள்ளக்கூடிய ஆரம்ப காலத்தை இது குறிக்கிறது. உதாரணமாக, காப்புப்பிரதிகளுக்கு இடையில் ஒரு பேரழிவு ஏற்பட்டால், நிறுவனத்தால் 2 நிமிட மதிப்புள்ள தரவு அல்லது 2 மணிநேரம் அல்லது முழு நாளையும் இழக்க நேரிடும்.
மீட்பு நேர நோக்கம் (Recovery Time Objective: RTO)	ஒரு வர்த்தகம் பொறுத்துக்கொள்ளக்கூடிய வேலையில்லா நேரத்தை RTO குறிக்கிறது. ஒரு பேரழிவிற்குப் பிறகு நிறுவனத்தின் செயல்பாடுகள் மற்றும் அமைப்புகளை மீண்டும் தொடங்குவதற்கான ஆரம்ப கட்டம் இதுவாகும்.
முறைமைகள் கடினப்படுத்துதல்)Systems Hardening(	கணினி கடினப்படுத்துதல் என்பது தகவல் தொழில்நுட்பபாதிப்பு மற்றும் சமரசம் செய்யப்படுவதற்கான சாத்தியக்கூறுகளைக் குறைக்க இயல்புநிலை உள்ளமைவு மற்றும் முறைமைகளினை மாற்றுவதன் மூலம் ஒரு கணினியைப் பாதுகாப்பதற்கான செயன்முறையாகும்.தாக்குதல் மேற்பரப்பைக் குறைப்பதன் மூலமும், தீங்கிழைக்கும் செயற்பாட்டின் நோக்கத்திற்காக தாக்குபவர்கள் தொடர்ந்து பயன்படுத்த முயற்சிக்கும் திசையன்களைத் தாக்குவதன் மூலமும் இதைச் செய்யலாம்.
வேர்ச்சுவல் பிறைவேற் நெற்வேர்க் (Virtual Private Network)	விர்ச்சுவல் பிரைவேட் நெட்வொர்க், இணையத்தில் தரவுத் தொடர்புக்காக மறை குறியாக்கப்பட்ட சுரங்கப்பாதையைப் பயன்படுத்தி பாதுகாப்பான இணைப்பை ஏற்படுத்துகிறது.

உசாத்துணைகள்

1. தகவல் பாதுகாப்பு அமுலாக்க வழிகாட்டி. இலங்கை சேர்ட்டின் ஆராய்ச்சி, கொள்கை மற்றும் திட்டப் பிரிவினால் 2022 இல் வெளியிடப்பட்டது. இந்த ஆவணத்தை www.onlinesafety.lk மூலம் அணுகலாம்.

2. ஆகக்குறைந்த தகவல் பாதுகாப்பு வழிகாட்டிகள். இலங்கை சேர்ட் நிறுவனத்தின் ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவினால் பிரசுரிக்கப்பட்டது. இதனை https://www.onlinesafety.lk/ எனும் இணைப்பினூடாக அணுக முடியும்.

3. இலங்கை தகவல் மற்றும் இணைய பாதுகாப்பு மூலோபாயம். (2019:2023), இலங்கை சேர்ட் நிறுவனத்தின் ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவினால் 2019 நவம்பரில் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை https://cert.gov.lk/documents/NCS Strategy.pdf எனும் இணைப்பினூடாக அணுகலாம்.

4. NIST சைபர் பாதுகாப்பு கட்டமைப்பு. தேசிய கட்டளைகள் மற்றும் தொழில்நுட்ப நிறுவகத்தினால் பிரசுரிக்கப்பட்டது, ஐக்கிய அமெரிக்க வர்த்தக திணைக்களம். மூலத்தரவுகள் https://www.nist.gov/cyberframework/online-learning/five-functions எனும் இணைப்பினூடாக பெற்றுக்கொள்ள முடியும்.

5. வீட்டிலிருந்து வேலைக்கான தகவல் பாதுகாப்பு வழிகாட்டிகள். இலங்கை சேர்ட்டினால் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை https://www.onlinesafety.lk/ எனும் இணைப்பினூடாக அணுக முடியும்.

6. அரசு நிறுவனங்களுக்கான இணையத்தள பாதுகாப்பு வழிகாட்டுதல்கள். இலங்கை சேர்ட்டின் ஆராய்ச்சி, கொள்கை மற்றும் திட்டப் பிரிவினால் 2022 இல் வெளியிடப்பட்டது. இந்த ஆவணத்தை https://www.onlinesafety.lk எனும் இணைப்பின் மூலம் அணுகலாம்.

7. வலையமைப்பு பயன்பாடு மற்றும் இணையத்தள பாதுகாப்புக்கான தொழில்நுட்ப வழிகாட்டுதல்கள். 2022 இல் இலங்கை சேர்ட்டின் ஆராய்ச்சி, கொள்கை மற்றும் திட்டப் பிரிவினால் வெளியிடப்பட்டது. இந்த ஆவணத்தை https://www.onlinesafety.lk எனும் இணைப்பினூடாக அணுக முடியும்.

8. சைபர் விண்ணப்ப பாதுகாப்புக்கான தொழில்நுட்ப வழிகாட்டிகள். இலங்கை சேர்ட் நிறுவனத்தின் ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவினால் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை https://www.onlinesafety.lk/ எனும் இணைப்பினூடாக அணுக முடியும்.

9. ISO 27002 (2013) : தகவல் தொழில்நுட்பம் – பாதுகாப்பு உபாயங்கள் –தகவல் பாதுகாப்பு முகாமைத்துவ முறைமைகள் – தேவைப்பாடுகள், சர்வதேச நியமங்கள் நிறுவனம், சர்வதேச கட்டளைகள் நிறுவனத்தினால் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை https://www.iso.org/ எனும் இணைப்பினூடாக அணுக முடியும்.