රාජ්‍ය ආයතන සඳහා

තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය
(ශ්‍රී ලංකා සර්ට්)

තාක්ෂණ අමාත්‍යාංශය

රාජ්‍ය ආයතන සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය - සිංහල අනුවාදය
පළමු සංස්කරණය
නිකුත් කළ දිනය: < >
මෙම ප්‍රතිපත්තිය < > දින සිට ක්‍රියාත්මක කිරීමට අමාත්‍ය මණ්ඩල අනුමැතිය ලබා දී ඇත.

ලේඛන වර්ගීකරණය: පොදු

ප්‍රකාශනය

පර්යේෂණ, ප්‍රතිපත්ති සහ ව්‍යාපෘති අංශය
ශ්‍රී ලංකා සර්ට් ආයතනය
කාමර අංක 4-112, බණ්ඩාරනායක ජාත්‍යාන්තර සම්මන්ත්‍රණ ශාලාව
බෞද්ධාලෝක මාවත, කොළඹ 7
ශ්‍රී ලංකාව

දුරකථන: +94 11 269 1692, ෆැක්ස්: +94 11 269 1064
විද්‍යුත් තැපැල්: cert@cert.gov.lk
වෙබ්: www.cert.gov.lk, www.onlinesafety.lk

පටුන

1. හැඳින්වීම

1.1 ශ්‍රී ලංකාවේ බොහෝ රාජ්‍ය ආයතන වර්තමානයේ රඳා පවතින්නේ ඩිජිටල් පද්ධති සහ යටිතල පහසුකම්වල විශ්වාසනීය ක්‍රියාකාරිත්වය මත ය. කෙසේ වෙතත්, ඇතැම් පුද්ගලයන් විසින් ද්වේෂ සහගත අරමුණින් සයිබර් තාක්ෂණය අවභාවිතා කරමින් ඩිජිටල් පද්ධතිවලට අනවසරයෙන් ඇතුළු වී සංවේදී තොරතුරු සොරකම් කිරීම, ආයතනයේ මෙහෙයුම් කටයුතුවලට බාධා පැමිණවීම, වෙබ් අඩවිවල අන්තර්ගතය විකෘති කරමින් ආයතනවල කීර්ති නාමයට හානි කිරීම වැනි අනර්ථ ක්‍රියා සිදුකරනු දැකිය හැකිය. එහි ප්‍රතිඵලයක් ලෙස රජයේ ආයතනවල ඇති ඩිජිටල් පද්ධති සහ යටිතල පහසුකම් කෙරෙහි ජනතාව තුළ පවතින විශ්වාසය පළුදුවීම පමණක් නොව ජාතික ආරක්ෂාවට ද, රටෙහි ආර්ථික කටයුතුවලට සහ යහපැවැත්මට ද බලපෑම් ඇති විය හැකිය.

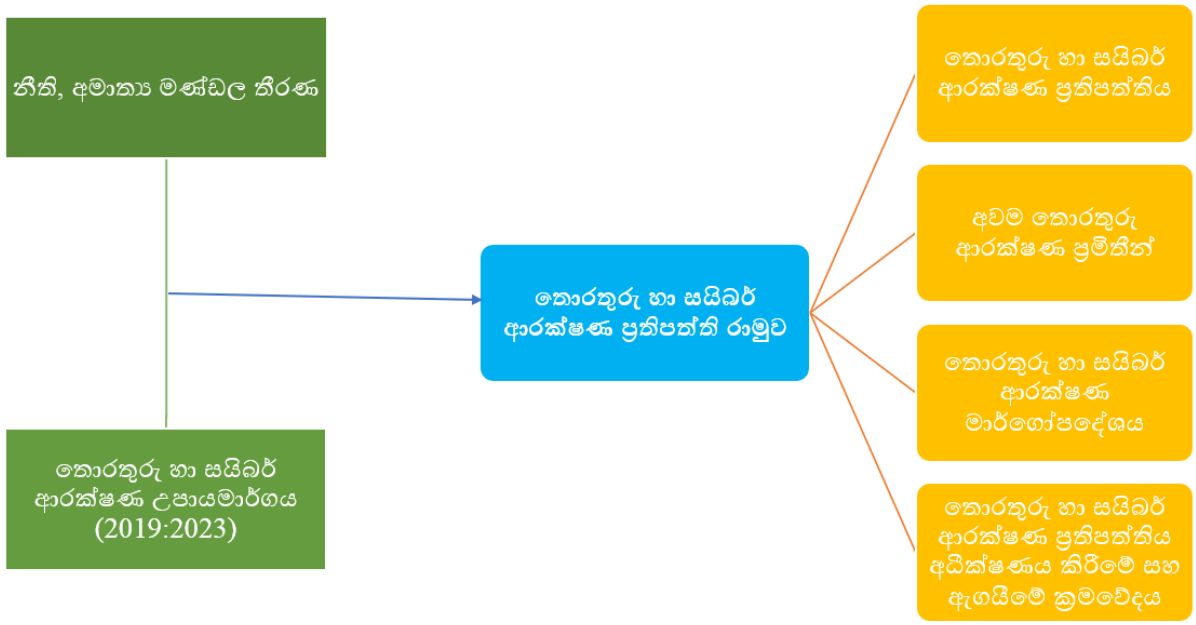
1.2 මෙම තොරතුරු හා සයිබර් ආරක්ෂණ අවදානම් ඵලදායී ලෙස කළමනාකරණය කර ගැනීම සඳහා රාජ්‍ය ආයතන අනුගත විය යුතු තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තියක්, ශ්‍රී ලංකාවේ සයිබර් අවකාශය ආරක්ෂා කිරීමේ අරමුණින් පිහිටුවා ඇති ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය (Sri Lanka Computer Emergency Readiness Team) හෙවත් ශ්‍රී ලංකා සර්ට් ආයතනය (Sri Lanka CERT) විසින් සකස් කර ඇත. මෙම ප්‍රතිපත්තිය මගින් ආයතනික මට්ටමින් තොරතුරු සහ සයිබර් ආරක්ෂණ වැඩපිළිවෙලක් ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය වන තොරතුරු හා සයිබර් ආරක්ෂණ අවදානම මූලික කර ගත් ආරක්ෂණ කළමනාකරණ ක්‍රමවේදයක් හඳුන්වා දී ඇත. තවද, ආයතනය විසින් ආරක්ෂා කළ යුතු වටිනා තොරතුරු සහ තොරතුරු තාක්ෂණ මෙවලම් (තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්) හඳුනා ගැනීම, ඒවායේ ආරක්ෂණයට බලපාන අවදානම් සහ සිදුවීම් හඳුනා ගැනීම, වත්කම් ආරක්ෂා කිරීම සඳහා සුදුසු ක්‍රියාමාර්ග ගැනීම සහ සයිබර් ප්‍රහාරයන්ට කාර්යක්ෂමව සහ ඵලදායීව ප්‍රතිචාර දක්වමින් බිඳ වැටුණු හෝ අඩපණ වූ වත්කම් යථා තත්ත්වයට පත් කිරීමට ආයතනය ගත යුතු ක්‍රියාමාර්ග මෙම ප්‍රතිපත්තියේ දැක්වේ.

1.3 රාජ්‍ය ආයතන සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ශ්‍රී ලංකාවේ තොරතුරු සහ සයිබර් ආරක්ෂණ උපායමාර්ගය (2019:2023) ක්‍රියාත්මක කිරීමට අනුකූලව සකස් කර ඇති අතර එය ජාත්‍යන්තර ප්‍රමිති සංවිධානය (International Organization for Standardization) සහ එක්සත් ජනපදයේ ජාතික ප්‍රමිති සහ තාක්ෂණ ආයතනය (National Institute of Standards and Technology) වැනි පිළිගත් අන්තර්ජාතික තොරතුරු ආරක්ෂණ ප්‍රමිතීන්ට අනුකූල වන පරිදි කෙටුම්පත් කර ඇති අතර තොරතුරු ආරක්ෂණ විශේෂඥයින් සහ රජයේ ජ්‍යෙෂ්ඨ නිලධාරීන් විසින් පුළුල් ලෙස සමාලෝචනය කර ඇත.

1.4 2016 අංක 12 දරණ තොරතුරු දැනගැනීමේ අයිතිවාසිකම් පිළිබඳ පනතේ ‘පොදු අධිකාරිය’ ලෙස අර්ථ දක්වා ඇති සියලුම රාජ්‍ය ආයතන මෙම ප්‍රතිපත්තියට අනුකූල විය යුතු අතර ආයතන ප්‍රධානීන් මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කර ආරක්ෂිත හා කාර්යක්ෂම සේවා සම්පාදනයක් ස්වකීය ආයතන තුළ සහතික කිරීමට වගකීමෙන් බැඳී සිටියි. මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේදී ශ්‍රී ලංකා සර්ට් ආයතනය රාජ්‍ය ආයතනවලට අවශ්‍ය තාක්ෂණික උපදෙස් හා මගපෙන්වීම් ලබා දෙනු ලබන අතර ප්‍රතිපත්තිය ආයතන තුළ ක්‍රියාත්මක කිරීමේ ප්‍රගතිය පිළිබඳව වාර්ෂික ඇගයීමක් ද සිදු කරනු ඇත.

2. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව

2.1 රාජ්‍ය ආයතන තුළ තොරතුරු සහ සයිබර් ආරක්ෂණ වැඩසටහන් වඩාත් කාර්යක්ෂම සහ ඵලදායී ලෙස ක්‍රියාවට නැංවීම සඳහා අවශ්‍ය මෙවලම් තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව මගින් හඳුන්වා දී ඇත. එමගින් (අ) තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය (Information and Cyber Security Policy), (ආ) රාජ්‍ය ආයතන අනුගමනය කළ යුතු අවම තොරතුරු ආරක්ෂණ ප්‍රමිතීන් (Minimum Information Security Standards), (ඇ) තොරතුරු හා සයිබර් ආරක්ෂණය ක්‍රියාත්මක කිරීමේ මාර්ගෝපදේශය (Information and Cyber Security Implementation Guide), සහ (ඈ) රාජ්‍ය ආයතනවල තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම අධීක්ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදයක්ද (Monitoring and Evaluation Methodology) ඇතුළත් වේ. තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව පිළිබඳ දළ විශ්ලේෂණයක් රූප සටහන අංක 1 මගින් ඉදිරිපත් කර ඇත.



රූප සටහන අංක 1: තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව

2.2 තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුවට පහත සඳහන් ප්‍රධාන සංරචක ඇතුළත් වේ:

අ. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය (Information and Cyber Security Policy): තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව තුළ ප්‍රමුඛතම අවධානය යොමු කෙරෙනුයේ රාජ්‍ය ආයතන සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට ය. එම ප්‍රතිපත්තිය තුළ රජයේ ආයතන විසින් තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සඳහා අනුගමනය කළ යුතු ආරක්ෂණ ක්‍රමවේදයන් ඇතුළත් ප්‍රතිපත්ති මාලාවක් ඉදිරිපත් කරයි.

ආ. අවම තොරතුරු ආරක්ෂණ ප්‍රමිතීන් (Minimum Information Security Standards): රජයේ ආයතන විසින් පිළිපැදිය යුතු අවම තොරතුරු ආරක්ෂණ ප්‍රමිතීන් මේ යටතේ දැක්වේ. මෙම ලේඛනය ශ්‍රී ලංකා සර්ට් ආයතනයේ www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැකිය.

ඇ. තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශය (Information and Cyber Security Implementation Guide): මෙමගින් නිලධාරීන්ට සහ පාර්ශවකරුවන්ට තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියේ අඩංගු එක් එක් ප්‍රතිපත්තිමය කරුණු ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය වන උපදෙස් මාලාවක් සපයයි. තොරතුරු ආරක්ෂණ පාලන ව්‍යුහයක් ස්ථාපිත කිරීම, වත්කම් වර්ගීකරණය, අවදානම් කළමනාකරණය, වත්කම් ආරක්ෂා කිරීම, උපස්ථ ක්‍රම සහ ආපදා ප්‍රතිසාධන ක්‍රම, සිදුවීම් කළමනාකරණය, අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය, සහ ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය යනාදී ක්‍රියා සඳහා අවශ්‍ය වන තාක්ෂණික උපදෙස් මෙම මාර්ගෝපදේශයෙහි ඇතුළත් වේ. මෙම මාර්ගෝපදේශය www.onlinesafety.lk යන ශ්‍රී ලංකා සර්ට් ආයතනයේ වෙබ් අඩවියෙන් බාගත කළ හැකිය.

ඈ. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම අධීක්ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදය (Monitoring and Evaluation Methodology): රාජ්‍ය ආයතනවල තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය අනුගමනය කිරීමට ඇති සූදානම සහ එය ක්‍රියාත්මක කිරීමේ කාර්යසාධනය අධීක්ෂණය සහ ඇගයීම සඳහා තක්සේරුකරණ නිර්ණායක අඩංගු ක්‍රමවේදයක් මෙමගින් සැපයේ. ශ්‍රී ලංකා සර්ට් ආයතනය මෙම ලේඛනයේ අංක 6 පරිච්ඡේදයේ විස්තර කර ඇති එම ක්‍රමවේදය භාවිතා කරමින් රාජ්‍ය ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරම්වල පරිණතභාවය නිශ්චිත කාල රාමුවක් තුළ ඇගයීමකට ලක් කෙරේ.

2.3 තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව, ශ්‍රී ලංකාවේ තොරතුරු සහ සයිබර් ආරක්ෂණ උපාය මාර්ගය, ඉ-රාජ්‍ය පිළිබඳ ප්‍රතිපත්තීන් සහ කලින් කලට පනවනු ලබන නීති, රෙගුලාසි සහ අමාත්‍ය මණ්ඩල තීරණවලට අනුකූලව ක්‍රියාත්මක කෙරෙනු ඇත.

3. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

3.1. අරමුණු

3.1.1 තොරතුරු හා සයිබර් ආරක්ෂණය යනු තොරතුරු වත්කම්වල රහස්‍යභාවය (confidentiality), උපයෝජ්‍යතාවය (availability) සහ විශ්වාසනීයභාවය (integrity) සහතික කිරීම සඳහා ඒවා වෙත අනවසරයෙන් වන ප්‍රවේශ වීම්, භාවිත කිරීම්, වෙනස් කිරීම්, හෝ විනාශ කිරීම්වලින් තොරතුරු වත්කම් ආරක්ෂා කිරීමයි. මේ යටතේ තොරතුරු වත්කම් අඩංගු හෝ භාවිතා වන තොරතුරු තාක්ෂණ මෙවලම් පුද්ගලයන් විසින් ද්වේශසහගතව සයිබර් තාක්ෂණය හෝ වෙනත් ක්‍රමවේදයන් භාවිතා කොට සිදු කරන හානිදායී ක්‍රියාවලින් ආරක්ෂා කර ගැනීම හෝ ජල ගැලීම්, ගිනි ගැනීම් වැනි වෙනත් ස්වභාවික විපත් මගින් සිදු වන හානිවලින් ආරක්ෂා කර ගැනීම ද ඇතුළත් වේ.

3.1.2 මෙම සන්දර්භය තුළ තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය මගින් රාජ්‍ය ආයතනයන්හි භාවිතා වන තොරතුරු වත්කම් සහ ඒවා පරිහරණය කරන තොරතුරු තාක්ෂණ වත්කම්, ස්වභාවික ආපදා සහ පුද්ගල ක්‍රියාකාරකම් මගින් වන හානිවලින් ආරක්ෂා කර ගැනීම සඳහා අනුගමනය කළ යුතු නීති රීති සහ මාර්ගෝපදේශ මාලාවක් හඳුන්වා දීම මෙම ප්‍රතිපත්තියේ මූලික අරමුණ වේ.

3.1.3 ප්‍රතිපත්තියේ අනෙකුත් අරමුණු වනුයේ,

අ. රාජ්‍ය අංශයේ සියලුම ආයතන සඳහා පොදු තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රමිතියක් ස්ථාපිත කිරීම.

ආ. තොරතුරු, පද්ධති සහ ඩිජිටල් යටිතල පහසුකම් සැලසුම් කිරීම, ක්‍රියාත්මක කිරීම, සහ භාවිතය සම්බන්ධයෙන් වන ආරක්ෂණ ප්‍රමිතීන්, නීති රීති සහ ක්‍රියාවලීන් රාජ්‍ය ආයතන සඳහා අනිවාර්ය කිරීම තුළින් තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම්වලට සාර්ථකව මුහුණ දීම සඳහා රාජ්‍ය ආයතනවල ප්‍රත්‍යවර්ථතාවය වැඩිදියුණු කිරීම.

ඇ. තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධීන් ක්ෂණිකව හඳුනාගැනීමට, එවැනි සිදුවීම්වලින් ආයතනවලට වන බලපෑම අවම කිරීමට සහ එවැනි සිදුවීම් හේතුවෙන් දුර්වල වූ හෝ බිඳ වැටුණු ඕනෑම ආයතනික සේවාවක් කාර්යක්ෂමව යථා තත්ත්වයට පත් කිරීමට සුදුසු යාන්ත්‍රණයක් ස්ථාපානය කිරීම.

ඈ. තොරතුරු සහ සයිබර් ආරක්ෂාව පිළිබඳ සුදුසුම භාවිතයන්, ආරක්ෂණ ප්‍රමිතීන්, නීති රීති සහ ක්‍රියාවලීන් පිළිබඳව කාර්ය මණ්ඩලය දැනුවත් කිරීම සහ ආයතනයේ සුරක්ෂිතභාවය පිළිබඳව කාර්ය මණ්ඩලයේ විශ්වාසය ගොඩනැගීම.

3.1.4 සියලුම රාජ්‍ය ආයතන වල කාර්ය මණ්ඩලයන්ට සහ අදාළ තෙවන පාර්ශවීය සේවා සපයන්නන්ට මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සම්බන්ධයෙන් ඔවුන් වෙත පැවරී ඇති වගකීම් සහ ඔවුන්ගේ වගවීම් පිළිබඳව පහසුවෙන් කියවා තේරුම් ගත හැකි ආකාරයට මෙම ප්‍රතිපත්තිය නිර්මාණය කර ඇත.

3.1.5 මෙම ප්‍රතිපත්තියේ අඩංගු තොරතුරු ආරක්ෂණ ප්‍රමිතීන්, සුදුසුම භාවිතයන් සහ තාක්ෂණික මාර්ගෝපදේශයන් රාජ්‍ය ආයතනයේ තොරතුරු, පද්ධති සහ ඩිජිටල් යටිතල පහසුකම් ආරක්ෂා කිරීම පිණිස කාලානුරූපීව යාවත්කාලීන කරනු ඇත.

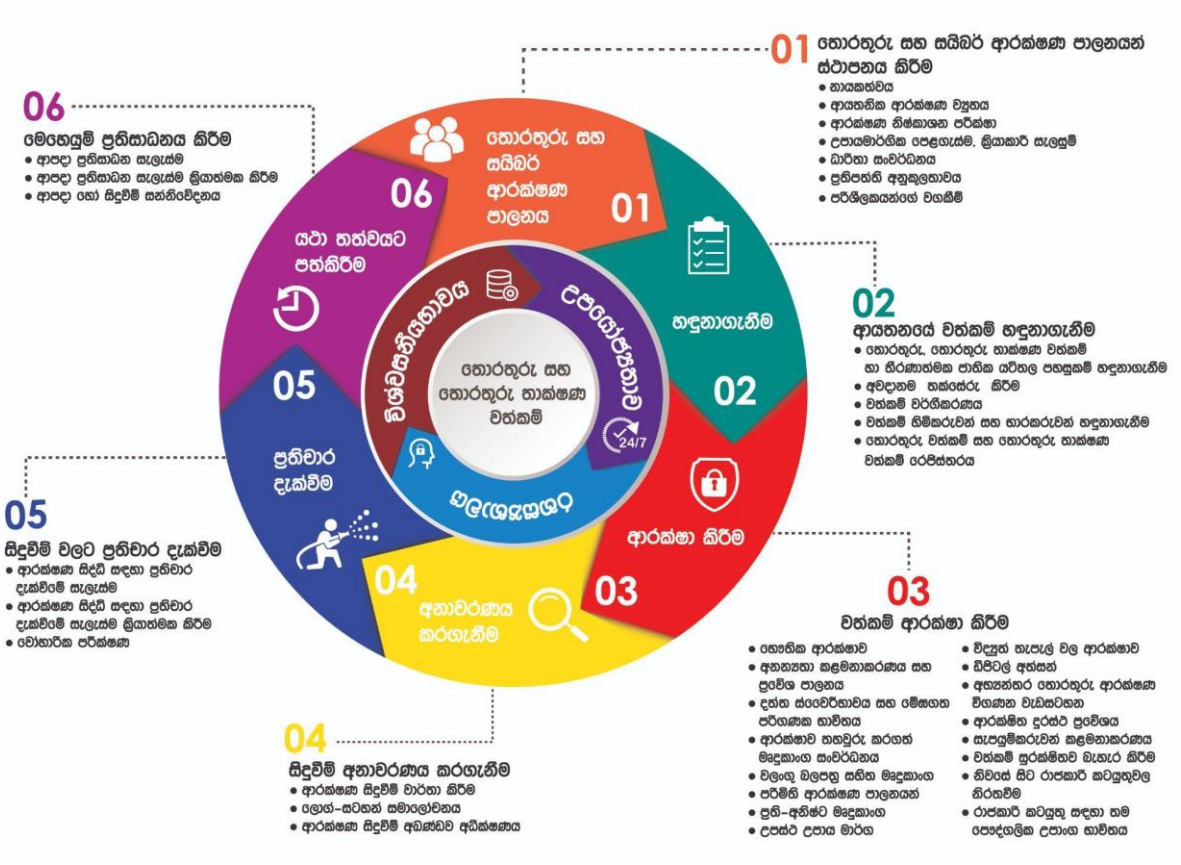
3.2. ප්‍රතිපත්තියේ විෂය පරාසය

3.2.1 මෙම ප්‍රතිපත්තිය ඕනෑම අමාත්‍යාංශයක්, දෙපාර්තමේන්තුවක්, රාජ්‍ය සංස්ථාවක්, පළාත් පාලන ආයතනයක්, රාජ්‍ය ආයතන වෙනුවෙන් තොරතුරු තාක්ෂණ සේවා කළමනාකරණය කරන අදාළ තෙවන පාර්ශව සේවා සපයන්නන් ද ඇතුළුව 2016 අංක 12 දරණ තොරතුරු දැනගැනීමේ අයිතිවාසිකම් පිළිබඳ පනතේ පොදු අධිකාරීන් ලෙස අර්ථ දක්වා ඇති ඕනෑම ආකාරයක ආයතනයකට මෙම ප්‍රතිපත්තිය අදාළ වේ.

3.2.2 මෙම ප්‍රතිපත්තියේ අඩංගු ප්‍රතිපත්ති ප්‍රකාශන කොටස් දෙකකින් සමන්විත වේ. ඒවානම්, සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශන සහ තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශන වේ. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන මෙම ප්‍රතිපත්තියේ අඩංගු ඔවුන් සඳහා විශේෂ වූ ප්‍රතිපත්ති ප්‍රකාශන ඇතුළුව අනෙකුත් සියලුම ප්‍රතිපත්තිවලට ද අනුගත විය යුතුය. අනෙකුත් ආයතන සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශනවලට අනුගත විය යුතු අතර තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශනවලටද සුදුසු පරිදි අනුගත වන්නේ නම් මැනවි.

3.2.3 මෙහි තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන ලෙස හඳුන්වන්නේ බිඳ වැටීමකදී හෝ අඩපණ වීමකදී ජාතික ආරක්ෂාව, රාජ්‍ය පාලනය, ආර්ථිකය, සෞඛ්‍ය සහ සමාජ යහපැවැත්ම කෙරෙහි ඍණාත්මක බලපෑමක් ඇති කරන තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් පවත්වාගෙන යන ආයතන වේ. එම ආයතන ශ්‍රී ලංකා සර්ට් ආයතනය විසින් හඳුනාගෙන ප්‍රකාශයට පත් කරනු ඇත.

3.2.4 තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය, එක්සත් ජනපදයේ ජාතික ප්‍රමිති සහ තාක්ෂණ ආයතනය විසින් හඳුන්වා දෙනු ලැබූ සුවිශේෂී තොරතුරු ආරක්ෂණ කාර්යයන් කිහිපයක් මත පදනම්ව සකස් කොට ඇත. ඒවා නම් (අ) ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් හඳුනා ගැනීම (හඳුනා ගැනීමේ කාර්යය), (ආ) එම වත්කම් ආරක්ෂා කිරීමට අවශ්‍ය ක්‍රියා මාර්ග ගැනීම (ආරක්ෂා කිරීමේ කාර්යය), (ඇ) එම වත්කම් සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් අනාවරණය කර ගැනීම (අනාවරණ කරගැනීමේ කාර්යය), (ඈ) එම සිදුවීම්වලට සාර්ථකව ප්‍රතිචාර දැක්වීම (ප්‍රතිචාර දැක්වීමේ කාර්යය) සහ (ඉ) යම් සිදුවීමක් හේතුවෙන් දුර්වල වූ හෝ බිඳ වැටුණු ඕනෑම සේවාවක් කාර්යක්ෂමව යථා තත්ත්වයට පත් කිරීම වේ (ප්‍රතිසාධන කාර්යය). තවද තොරතුරු සහ සයිබර් ආරක්ෂාව සම්බන්ධ ක්‍රියාකාරකම් මෙහෙයවීම සහ පාලනය කිරීම සඳහා ආයතනික මට්ටමින් පාලන ව්‍යුහයක් ස්ථාපිත කිරීම ද මෙයට ඇතුළත්ය. රූප සටහන් අංක 2 මගින් තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කරමින් ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට ආයතනය ගත යුතු ක්‍රියාමාර්ග දැක්වේ.



රූප සටහන අංක 2: තොරතුරු සහ සයිබර් ආරක්ෂණ පියවර

3.2.5 ඉහත අංක 3.2.4 හි සඳහන් වූ සුවිශේෂී තොරතුරු ආරක්ෂණ කාර්යයන් පදනම්ව නිර්මාණය කරන ලද මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කරමින් තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට ආයතනය ගත යුතු ක්‍රියාමාර්ග පහතින් විස්තර කෙරේ.

අ. තොරතුරු හා සයිබර් ආරක්ෂණ පාලනය (Information and Cyber Security Governance): මෙමගින් හඳුන්වනුයේ ආයතනයක තොරතුරු සහ සයිබර් ආරක්ෂාව මෙහෙයවන සහ පාලනය කරන ක්‍රමවේදය වේ. මේ යටතේ ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ කටයුතු ක්‍රියාත්මක කිරීම සඳහා ආයතනික ව්‍යුහයක් ස්ථාපනය කිරීම, තොරතුරු සහ සයිබර් ආරක්ෂාව සඳහා වගකිව යුතු සහ වගවිය යුතු නිලධාරීන් පත් කිරීම සහ එවැනි නිලධාරීන්ගේ ධාරිතාවන් සංවර්ධනය කිරීම, ආයතනික තොරතුරු සහ සයිබර් ආරක්ෂක අරමුණු ස්ථාපනය කිරීම, ක්‍රියාකාරී සැලසුම් සකස් කිරීම සහ තොරතුරු ආරක්ෂක කටයුතු සඳහා සම්පත් සැපයීම කළ යුතුය (පරිච්ඡේද අංක 4.1).

ආ. හඳුනා ගැනීමේ කාර්යය (Identify Function): ආයතනය සතු දත්ත, තොරතුරු, පරිගණක, පද්ධති, සහ තීරණාත්මක ඩිජිටල් යටිතල පහසුකම් වැනි තොරතුරු තාක්ෂණ වත්කම් හඳුනාගැනීමත්, ඒවා සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ අවදානම් හඳුනාගෙන එම අවදානම් ඵලදායී ලෙස කළමනාකරණය කරන්නේ කෙසේද යන්න පිළිබඳ උපදෙස් මේ යටතේ පෙළගස්වා ඇත. (පරිච්ඡේද අංක 4.2). මේ අනුව, රාජ්‍ය ආයතන

තමන් සතු තොරතුරු තාක්ෂණ වත්කම් හොඳින් හඳුනාගෙන, ඒවාට ඇති අවදානම තක්සේරුකරමින් එම වත්කම් මනාලෙස කළමනාකරණය කළ යුතුය.

ඇ. ආරක්ෂා කිරීමේ කාර්යය (Protect Function): ආරක්ෂා කිරීමේ කාර්යය මගින්, රාජ්‍ය ආයතන සිය තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කරගනිමින් සිය සේවාවන් අඛන්ඩව පවත්වාගෙන යාම සහතික කිරීම සඳහා ගතයුතු තොරතුරු සහ සයිබර් ආරක්ෂණ ක්‍රමවේදයන් විස්තර කෙරේ. ආයතනය සතු තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සඳහා ඒවා වෙත වන ප්‍රවේශය පාලනය කිරීම, ගිනිපවුරු (firewalls) සහ ප්‍රති-අනිෂ්ට මෘදුකාංග (anti-malware) ස්ථාපනය කිරීම, තොරතුරු ආරක්ෂණ විගණන පැවැත්වීම, සහ උපස්ථ පිටපත් (backups) තබා ගැනීම ඇතුළුව, පරිච්ඡේද අංක 4.3 හි සඳහන් ප්‍රතිපත්තීන් ක්‍රියාවට නැංවිය යුතුය.

ඈ. අනාවරණ කරගැනීමේ කාර්යය (Detect Function): මෙම කාර්යය මගින් තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීමක් අනාවරණය කර ගැනීමට අවශ්‍ය ක්‍රියාමාර්ග විස්තර කෙරේ. ආයතන විසින් සිදුවීම් ක්ෂණිකව හඳුනා ගැනීමට සුදුසු යාන්ත්‍රණයන් ක්‍රියාත්මක කළ යුතු අතර පරිගණක සහ අදාල මෙවලම් මගින් උත්පාදනය කරන ලොග් සටහන් විශ්ලේෂණය කරමින් සහ සිදුවීම් හඳුනා ගැනීමේ මෙවලම් භාවිතයෙන් එම සිදුවීම් කාර්යක්ෂම ලෙස හඳුනා ගැනීමට කටයුතු කළ යුතු වේ (පරිච්ඡේද අංක 4.4).

ඉ. ප්‍රතිචාර දැක්වීමේ කාර්යය (Respond Function): මෙම කාර්යය මගින්, හඳුනාගත් තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධීන්ට ප්‍රතිචාර දැක්විය යුතු ආකාරය විස්තර කෙරේ. ඒ සඳහා, පරිච්ඡේද අංක 4.5 හි සඳහන් කර ඇති පරිදි, රාජ්‍ය ආයතන, තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම්වලට කාර්යක්ෂම සහ ඵලදායී ලෙස ප්‍රතිචාර දැක්වීම සඳහා ආරක්ෂණ සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් පිළියෙළකොට ක්‍රියාවෙහි නැංවිය යුතුය.

ඊ. ප්‍රතිසාධන කාර්යය (Recover Function): ප්‍රතිසාධන කාර්යය මගින්, තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධියක් හේතුවෙන් දුර්වල වූ හෝ බිඳවැටුන ඕනෑම වත්කමක් හෝ සේවාවක් ප්‍රතිෂ්ඨාපනය කිරීමට අවශ්‍ය ක්‍රියාකාරකම් විස්තර වේ. ප්‍රතිසාධන කාර්යයට අනුකූල වීම සඳහා, ආයතනය විසින් ආපදා ප්‍රතිසාධන සැලැස්මක් සකස් කළ යුතු අතර මෙහෙයුම් කාර්යක්ෂමව හා ඵලදායී ලෙස යථා තත්වයට පත් කිරීම සඳහා මෙම සැලැස්ම ක්‍රියාත්මක කළ යුතුය (පරිච්ඡේද අංක 4.6).

4. ප්‍රතිපත්ති සංග්‍රහය

රාජ්‍ය ආයතන සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ප්‍රධාන ප්‍රතිපත්ති අංශ හයකින් සමන්විත වේ. ඒවානම්, (අ) තොරතුරු හා සයිබර් ආරක්ෂණ පාලනයක් ආයතනය තුළ ස්ථාපනය කිරීම, (ආ) වත්කම්, ඒවායේ හිමිකරුවන් සහ භාරකරුවන්, සහ වත්කම් සඳහා වන අවදානම් හඳුනා ගැනීම, (ඇ) වත්කම් ආරක්ෂා කරගැනීම, (ඈ) වත්කම් සම්බන්ධ තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම, (ඉ) ආරක්ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම, සහ (උ) ආපදාවකදී බිඳ වැටුන හෝ අඩපන වූ මෙහෙයුම් ප්‍රතිසාධනය වේ. ඉහත දැක්වූ අංශ හයට අදාළව රාජ්‍ය ආයතන අනුකූල විය යුතු ප්‍රතිපත්තීන් එක් එක් අංශය යටතේ පෙළගස්වා ඇත.

4.1. තොරතුරු සහ සයිබර් ආරක්ෂණ පාලනය

මෙම පරිච්ඡේදය මගින් ආයතනයේ තොරතුරු සුරක්ෂිතතාව මෙහෙයවීම සහ පාලනය කිරීම සඳහා යාන්ත්‍රණයක් යෝජනා කරන අතර ආයතනය තුළ තොරතුරු ආරක්ෂණ ක්‍රියාකාරකම්වල නිසි කළමනාකරණයක් සහතික කිරීම සඳහා අවශ්‍ය නායකත්වය සහ වගවීම සම්බන්ධයෙන් මෙහි සඳහන් වේ. තවද, ආයතනයේ මෙහෙවර හා දැක්ම සාක්ෂාත් කර ගැනීම සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරකම් සක්‍රීය ලෙස දායක කර ගැනීමේ අවශ්‍යතාවය, වගවියයුතු නිලධාරීන්ගේ ධාරිතා සංවර්ධනයේ අවශ්‍යතාවය, ක්‍රමවත් තොරතුරු හා සයිබර් ආරක්ෂණ සැලසුම් සැකසීමේ සහ මෙම ප්‍රතිපත්තිය සඳහා රාජ්‍ය ආයතන අනුගත වීමේ වැදගත්කම මෙහි තවදුරටත් සඳහන් වේ.

මේ අනුව පහත දක්වා ඇති ප්‍රතිපත්තිමය කරනා සඳහා රාජ්‍ය ආයතන අනුකූල වීම අපේක්ෂා කෙරේ.

4.1.1. නායකත්වය පිළිබඳ ප්‍රතිපත්තිය

ආයතන ප්‍රධානියා විසින් ආයතනයේ තොරතුරු ආරක්ෂණ ක්‍රියාකාරකම් සඳහා නායකත්වය සැපයිය යුතු අතර, ආයතනයේ තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමේ පරම වගකීම සහ වගවීමද දැරිය යුතු වේ.

ආයතන ප්‍රධානියා විසින් ආයතනයේ මෙම තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සඳහා මූලිකත්වය ගෙන කටයුතු කළ යුතු අතර, ආයතනයේ දැක්ම සහ මෙහෙවර සාක්ෂාත් කර ගැනීම සඳහා අවශ්‍ය වන තොරතුරු ආරක්ෂණ ඉලක්ක සැකසීමත්, තොරතුරු ආරක්ෂක ක්‍රියාකාරකම් සඳහා අවශ්‍ය සම්පත් සැපයීමත් සිදු කළ යුතුය.

තවද ආයතනයේ පරිගණක පරිශීලකයන්, මෙම ප්‍රතිපත්තියට අනුගත වෙමින් ඔවුන් භාවිතා කරන තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සඳහා සක්‍රීයව දායකත්වය සපයන තොරතුරු ආරක්ෂණ සංස්කෘතියක් ආයතනය තුළ නිර්මාණය කිරීම සඳහා ද ආයතන ප්‍රධානියා විසින් අවශ්‍ය නායකත්වය සැපයිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.2. ආරක්ෂණ ආයතනික ව්‍යුහය පිළිබඳ ප්‍රතිපත්තිය

රාජ්‍ය ආයතනය තුළ තොරතුරු හා සයිබර් ආරක්ෂණ ආයතනික ව්‍යුහයක් ස්ථාපිත කළ යුතුය. එලදායී ආයතනික තොරතුරු ආරක්ෂණ ව්‍යුහයක් තුළ (අ) තොරතුරු ආරක්ෂණ නිලධාරී, (ආ) ප්‍රධාන නව්‍යකරණ නිලධාරී සහ (ඇ) (ප්‍රධාන) අභ්‍යන්තර විගණක වැනි තනතුරු ඇතුළත් විය යුතුය. ආයතනයේ තොරතුරු ආරක්ෂණ ක්‍රියාකාරකම් තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුව ක්‍රියාත්මක කිරීම, මෙහෙයවීම සහ කළමනාකරණය කිරීම සඳහාත් ආයතනයේ තොරතුරු සහ තොරතුරු ආරක්ෂණ වත්කම් සයිබර් ප්‍රහාරයන්ගෙන් ආරක්ෂා කර ගැනීම සඳහාත් මෙම ව්‍යුහාත්මක වගකීම් දරන නිලධාරීන් අවශ්‍ය වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

(අ) තොරතුරු ආරක්ෂණ නිලධාරීගේ කාර්යභාරය පිළිබඳ ප්‍රතිපත්තිය

ආයතන ප්‍රධානියා විසින් රාජ්‍ය ආයතනය සඳහා තොරතුරු ආරක්ෂණ නිලධාරියකු පත් කළ යුතුය. එම නිලධාරියා, ආයතන ප්‍රධානියාගේ අනුදැනුම සහ මගපෙන්වීම යටතේ, ආයතනයේ තොරතුරු ආරක්ෂණ අරමුණු ස්ථාපිත කිරීම, තොරතුරු ආරක්ෂණ අවදානම් කළමනාකරණය කිරීම සහ ආයතනයේ තොරතුරු තාක්ෂණ වත්කම් ප්‍රමාණවත් ලෙස ආරක්ෂා කර ඇති බව සහතික කිරීම සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම යන වගකීම් දරන ජ්‍යෙෂ්ඨ මට්ටමේ විධායක නිලධාරියකු විය යුතුය.

රාජ්‍ය ආයතනය තුළ තොරතුරු ආරක්ෂණ නිලධාරීගේ කාර්යභාරය තොරතුරු තාක්ෂණ විෂය පථයෙන් ස්වායක්ත විය යුතු අතර, තොරතුරු ආරක්ෂණයට අදාළ ක්‍රියාකාරකම් සම්බන්ධයෙන් ආයතන ප්‍රධානියා වෙත සෘජුවම වාර්තා කළ යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

(ආ) ප්‍රධාන නව්‍යකරණ නිලධාරීගේ කාර්යභාරය පිළිබඳ ප්‍රතිපත්තිය

ප්‍රධාන නව්‍යකරණ නිලධාරි හෝ තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියා ආයතනයේ තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට අවශ්‍ය ක්‍රියාමාර්ග ගැනීමට සහ ආයතනයේ පරිපාලන කටයුතු අඛණ්ඩව පවත්වාගෙන යාම සහතික කිරීමට අවශ්‍ය තොරතුරු ආරක්ෂණ පුහුණුව ලබාදී නිසි වගකීම් පැවරිය යුතුය.

සටහන: තොරතුරු ආරක්ෂණ නිලධාරියකු ආයතනය තුළ පත්කර නොමැති අවස්ථාවකදී, තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියා ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරියා ලෙස කටයුතු කිරීමට බල ගැන්විය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

(ඇ) (ප්‍රධාන) අභ්‍යන්තර විගණකගේ කාර්යභාරය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ තොරතුරු ආරක්ෂණ විගණන ආරම්භ කිරීම සහ අධීක්ෂණය කිරීම, තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ආයතනය තුළ ක්‍රියාත්මක කිරීමේ ප්‍රගතිය තක්සේරු කිරීම, සහ තොරතුරු ආරක්ෂාව හා සම්බන්ධ කටයුතු වලදී විගණන හා කළමනාකරණ කමිටුවට (Audit and Management Committee) වාර්තා කිරීම යන වගකීම් ආයතනයේ අභ්‍යන්තර විගණක නිලධාරියා (හෝ ප්‍රධාන අභ්‍යන්තර විගණක නිලධාරියා) වෙත පැවරේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.3. තොරතුරු ආරක්ෂණ කමිටුව පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමට අදාළ ක්‍රියාකාරකම් සඳහා උපාය මාර්ගික උපදෙස් සැපයීම සඳහා ආයතනය තොරතුරු ආරක්ෂණ කමිටුවක් පිහිටුවිය යුතුය. ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේදී තොරතුරු ආරක්ෂණ නිලධාරියා විසින් සිදු කරනු ලබන සියලුම තොරතුරු ආරක්ෂණ පාලනයන්, ක්‍රියාකාරී සැලසුම්, තොරතුරු තාක්ෂණ වත්කම් වර්ගීකරණයට අදාළ

ක්‍රමවේද, සිද්ධීන්ට ප්‍රතිචාර දැක්වීමේ සැලසුම් සහ ආපදා ප්‍රතිසාධන සැලසුම් ඇතුළු අනෙකුත් ක්‍රියාකාරකම් සමාලෝචනය කිරීම සහ අනුමත කිරීම සඳහා මෙම කමිටුව වගකිව යුතුය. ආයතන ප්‍රධානියා කමිටුවේ මුලසුන දැරිය යුතු අතර එම කමිටුව තොරතුරු ආරක්ෂණ නිලධාරී, ප්‍රධාන නව්‍යකරණ නිලධාරී, (ප්‍රධාන) අභ්‍යන්තර විගණක නිලධාරී සහ වත්කම් හිමියන්ගෙන් සමන්විත විය යුතුය. වත්කම් හිමිකරුවන් පිළිබඳ ප්‍රතිපත්තිය අංක 4.2.3 යටතේ දක්වා ඇත.

අනුකූලතාව: සියලුම *රාජ්‍ය* ආයතන සඳහා අදාළ වේ.

4.1.4. අවදානම් කළමනාකරණ කමිටුව පිළිබඳ ප්‍රතිපත්තිය

ආයතනය තුළ අවදානම් කළමනාකරණ කමිටුවක් පිහිටුවිය යුතුය. මෙම කමිටුව ආයතන ප්‍රධානී වෙත සෘජුවම වාර්තා කරන ස්වාධීන කමිටුවක් විය යුතු අතර, තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සම්බන්ධයෙන් ආයතනයේ අවදානම් කළමනාකරණය අධීක්ෂණය කිරීමේ වගකීම දැරිය යුතු වේ.

මෙම කමිටුව ආයතනයේ තොරතුරු තාක්ෂණ වත්කම් සම්බන්ධයෙන් වන අවදානම් හඳුනාගෙන ඒවා නිසි ඇගයීමට ලක් කළ යුතු අතර, එම හඳුනාගත් අවදානම් අවම කිරීම සඳහා අවශ්‍ය ක්‍රියාමාර්ග ගැනීමට තොරතුරු ආරක්ෂණ කමිටුව වෙත සුදුසු ක්‍රමවේද යෝජනා කළ යුතුය. මෙම කමිටුවට ආයතනයේ අංශ ප්‍රධානීන්, තොරතුරු තාක්ෂණ වත්කම් හිමිකරුවන් සහ තොරතුරු ආරක්ෂණ නිලධාරී ඇතුළත් විය යුතුය. ආයතනයේ නියෝජ්‍ය ප්‍රධානියා මෙම කමිටුවේ සභාපතිවරයා විය යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.1.5. පරිශීලකයන්ගේ වගකීම් පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු ආරක්ෂණය ආයතනයේ සෑම කෙනෙකුගේම පොදු වගකීමකි. සියලුම තොරතුරු තාක්ෂණ පරිශීලකයින් ඔවුනට ප්‍රවේශයට අවසර ඇති තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සම්බන්ධයෙන් වන ආයතනික ප්‍රතිපත්තියකට අනුගතව වගකීමෙන් ක්‍රියාකළ යුතුවේ.

පරිශීලක වගකීම්වලට තොරතුරු, පරිගණක මෙවලම්, ඊමේල්, අන්තර්ජාලය, සමාජ මාධ්‍ය, දුරකථන සහ ෆැක්ස් නිසි ලෙස භාවිත කිරීම ඇතුළත් වන අතර, තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශයේ දක්වා ඇති පරිශීලක වගකීම්, සහ මෙම ප්‍රතිපත්තියේ දක්වා ඇති තොරතුරු සහ සයිබර් ආරක්ෂණ භාවිතයන් මනාව තේරුම් ගෙන පිළිපැදිය යුතුය.

එවැනි වත්කම් අවභාවිතයන් සඳහා ආයතන සංග්‍රහයේ දක්වා ඇති විනය ක්‍රියාමාර්ගවලට සහ පරිගණක අපරාධ පනතේ හෝ වෙනත් අදාළ පනත්වල ඇති නීතිමය ප්‍රතිපාදන යටතේ කටයුතු කරනු ලැබිය හැකිය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.6. ධාරිතා සංවර්ධනය පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු ආරක්ෂණය සම්බන්ධයෙන් වගකිව යුතු සහ වගවිය යුතු නිලධාරීන්ගේ (උදා: තොරතුරු ආරක්ෂණ නිලධාරී, ප්‍රධාන නව්‍යකරණ නිලධාරී, අභ්‍යන්තර විගණක නිලධාරී, වත්කම් හිමිකරුවන්, පරිශීලකයන්) තොරතුරු ආරක්ෂණය පිළිබඳ ධාරිතා සංවර්ධනය කිරීම සඳහා ආයතනය විසින් නිසි පියවර ගත යුතුය. ඒ අනුව අදාළ නිලධාරීන්ට අවශ්‍ය තොරතුරු ආරක්ෂණ දැනුම හා කුසලතා ගොඩනැගීම සඳහා අවශ්‍ය පුහුණුවීම්, අධ්‍යාපනය සහ දැනුවත් කිරීම් නිසි ක්‍රමවේදයකට අනුව සිදු කළ යුතු අතර එවැනි වැඩසටහන් ආයතනයේ වාර්ෂික පුහුණු සැලැස්මට ඇතුළත් කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.7. කාර්ය මණ්ඩලය සඳහා ආරක්ෂක නිෂ්කාශන පරීක්ෂාව පිළිබඳ ප්‍රතිපත්තිය

ඉතා රහසිගත හෝ රහසිගත ලෙස වර්ගීකරණය කර ඇති තොරතුරු සමඟ කටයුතු කරන හෝ තීරණාත්මක ජාතික තොරතුරු

යටිතල පහසුකම්වලට ප්‍රවේශ වන යම් තනතුරකට පත් කරන ලද හෝ ස්ථාන මාරුවක් ලද ඕනෑම අයෙකු එම තනතුර සඳහා පත් කිරීමට හෝ ස්ථාන මාරු කිරීමට පෙර ආරක්ෂක නිෂ්කාශන පරීක්ෂාවකට සහ පසුබිම් පරීක්ෂාවකට ලක් කළ යුතු අතර ඔවුන්ගේ සේවා කාලය තුළ ද වරින් වර ආරක්ෂක නිෂ්කාශන පරීක්ෂණවලට ලක් කළ යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.1.8. උපායමාර්ගික පෙළගැස්වීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය, සිය තොරතුරු ආරක්ෂක ක්‍රියාකාරකම් එහි ආයතනික දැක්ම, මෙහෙවර සහ අරමුණු සමඟ පෙළ ගැස්විය යුතුය. ආයතනය තුළ ක්‍රියාත්මක කරන සියලුම තොරතුරු ආරක්ෂක උපාය මාර්ග, ව්‍යාපෘති සහ ක්‍රියාකාරකම් සැලසුම් කළ යුත්තේ ඒවා ආයතනයේ දැක්ම, මෙහෙවර සහ අරමුණුවලට අනුකූල වන ආකාරයට ය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.9. ක්‍රියාකාරී සැලසුම් සහ ප්‍රතිපාදන පිළිබඳ ප්‍රතිපත්තිය

ආයතනික දැක්ම, මෙහෙවර සහ අරමුණු සාක්ෂාත් කර ගැනීමේදී ආයතනයේ තොරතුරු තාක්ෂණ ආරක්ෂාව සහතික කළ යුතු ආකාරය විදහා දැක්වෙන තොරතුරු ආරක්ෂණ ක්‍රියාකාරී සැලසුම් (දිගු කාලීන, මධ්‍ය කාලීන හා කෙටි කාලීන සැලසුම්) ආයතනය විසින් සකස් කර ක්‍රියාත්මක කළ යුතුය. එම සැලසුම් අවදානම් තක්සේරුවකින් තීරණය කරනු ලබන තොරතුරු ආරක්ෂණ ප්‍රමුඛතා මත පදනම්ව සකස් කළ යුතු අතර ඒවා ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය ප්‍රතිපාදන ද වෙන් කරගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.10. ප්‍රතිපත්ති අනුකූලතාවය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය මෙම ලේඛනයේ විස්තර කර ඇති තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුකූල විය යුතුය. මෙහි අංක 4.1.1 සහ 4.1.2 (අ) හි සඳහන් කර ඇති පරිදි, මෙම ප්‍රතිපත්තියට අනුකූලව ආයතනය කටයුතු කිරීමේ පූර්ණ වගකීම ආයතන ප්‍රධානී සහ තොරතුරු ආරක්ෂණ නිලධාරී විසින් දැරිය යුතුය.

ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුකූල වීමේ කාර්ය සාධන මට්ටම තක්සේරු කිරීම සඳහා වාර්ෂිකව තොරතුරු ආරක්ෂණ සූදානම තක්සේරු කිරීමේ පරීක්ෂණයක් ශ්‍රී ලංකා සර්ට් ආයතනය විසින් සිදු කළ යුතු අතර, එම තක්සේරු පරීක්ෂණය සිදුකිරීම සඳහා පහසුකම් ආයතනය විසින් සැලසිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2. වත්කම්, හිමිකරුවන්, පරිශීලකයන් සහ අවදානම් හඳුනා ගැනීම

ආයතනික වත්කම් සඳහා වන තොරතුරු ආරක්ෂණ අවදානම් ඵලදායී ලෙස කළමනාකරණය කිරීම සඳහා, ආයතන ඔවුන් ක්‍රියාත්මක වන වපසරිය පිළිබඳව මනා අවබෝධයක් ඇති කර ගත යුතු වේ. ඒ අනුව ආයතනයට වටිනාකමක් ඇති වත්කම් (තොරතුරු, පද්ධති ඇතුලු තොරතුරු තාක්ෂණ උපාංග), ඒවායේ හිමිකරුවන්, භාරකරුවන් සහ පරිශීලකයන්, එම වත්කම් ආරක්ෂා කිරීම

සඳහා ඔවුන්ගේ වගකීම්, සහ එම වත්කම් සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ අවදානම් ආයතනය විසින් නිවැරදිව හඳුනා ගත යුතුය. මේ පිළිබඳව ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.

4.2.1. තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් හඳුනා ගැනීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය එහි සියළුම වැදගත් තොරතුරු වත්කම් (information assets) නිවැරදිව හඳුනා ගත යුතුය. තොරතුරු වත්කමක් යනු එහි ආයතනික කාර්යයන් ඉටු කිරීමේදී ආයතනයට වැදගත් සහ වටිනා ඕනෑම තොරතුරකි. තොරතුරු වත්කම් සඳහා උදාහරණ ලෙස වෙළඳ රහස්, ටෙන්ඩර් ලියකියවිලි, විදේශ ගමන් බලපත්‍රයක අඩංගු තොරතුරු, අයවැය පත්‍රිකා සහ සේවකයින්ගේ පෞද්ගලික වාර්තා ඇතුළත් වේ. තොරතුරු වත්කම්, කඩදාසි ලේඛනයක්, ඉලෙක්ට්‍රොනික මාධයෙන් ඇති ලේඛනයක්, ඩිජිටල් දත්ත ගබඩාවක්, මුරපදයක් හෝ සංකේතාංක යතුරක් (encryption key) හෝ වෙනත් ඕනෑම ඩිජිටල් ලිපි ගොනුවක් වැනි විවිධ ස්වරූපවලින් පැවතිය හැකිය.

තවද ආයතනය එහි සියළුම වැදගත් තොරතුරු තාක්ෂණ වත්කම් ද (IT assets) නිවැරදිව හඳුනා ගත යුතුය. තොරතුරු තාක්ෂණ වත්කම් යනු තොරතුරු තාක්ෂණ පරිසරයක් තුළ ඇති මෘදුකාංග (උදා: මෙහෙයුම් පද්ධති, වැටුප් ගෙවීමේ පද්ධති, වෙනත් මෘදුකාංග), දෘඩාංග (උදා: පරිගණක, දෘඩ තැටි, සර්වර් පරිගණක, රවුටර, ගිනිපවුරු), ජාල සහ වෙනත් ඩිජිටල් යටිතල පහසුකම් යනාදිය වේ. වත්කම් (තොරතුරු හා තොරතුරු තාක්ෂණ) හඳුනා ගැනීම සිදු කළ යුත්තේ, එම වත්කම් අනවසර ප්‍රවේශයන්, භාවිතයන්, හෙළිදරව් කිරීම්, බාධා කිරීම්, වෙනස් කිරීම් හෝ විනාශ කිරීම් වැනි ක්‍රියාකාරම්වලින් ආරක්ෂා කර ඒවායේ රහස්‍යභාවය, විශ්වාසනීයභාවය සහ උපයෝජ්‍යතාවය සුරැකීමේ අරමුණෙනි.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2.2. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම පිළිබඳ ප්‍රතිපත්තිය

තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් යනු බිඳ වැටීමකදී හෝ අසාර්ථක වීමකදී ජාතික ආරක්ෂාව, පාලනය, ආර්ථිකය, සෞඛ්‍ය සහ සමාජ යහපැවැත්ම කෙරෙහි ඍණාත්මක බලපෑමක් ඇති කරන තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වේ. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් පවත්වාගෙන යන ආයතන මෙම ප්‍රතිපත්තියේ නිශ්චිතව දක්වා ඇති ආකාරයෙන් එවන් වත්කම් ආරක්ෂා කිරීමට සුදුසු පියවර ගත යුතුය. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම ශ්‍රී ලංකා සර්ට් ආයතනය විසින් සිදු කළ යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන අදාළ වේ.

4.2.3. වත්කම් හිමිකරුවන්, භාරකරුවන් සහ පරිශීලකයන්ගේ වගකීම් පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වත්කම් හිමිකරුවන්, පරිශීලකයන් සහ භාරකරුවන් හඳුනා ගත යුතුය. වත්කම් හිමිකරු යනු, වත්කමක මුළු ජීවන චක්‍රයම පාලනය කිරීමේ වගකීම දරන සහ වත්කමක ආරක්ෂාව පිළිබඳව වගකියන ඉහළ මට්ටමේ විධායක ශ්‍රේණියේ නිලධාරියෙකු හෝ ආයතනයක් වේ. වත්කම් හිමිකරු වත්කම්වලට ඇති අවදානම හඳුනා ගත යුතු අතර වත්කම් ආරක්ෂා කිරීම සඳහා සුදුසු ක්‍රමවේද යෝජනා කළ යුතුය. වත්කමක් ආයතනය තුළ නිල වශයෙන් නිර්මාණය කිරීමේදී, අත්පත් කර ගැනීමේදී හෝ වෙනත් ආයතනයකට මාරු කිරීමේදී වත්කම් හිමිකරු වෙත නිල වශයෙන් අයිතිය පැවරීම අත්‍යවශ්‍ය වේ.

වත්කම් භාරකරු යනු වත්කම් ආරක්ෂා කිරීම සම්බන්ධයෙන් වත්කම් හිමිකරු විසින් අනුමත කරන ලද සුදුසු ආරක්ෂණ ක්‍රමවේද ක්‍රියාත්මක කිරීම සඳහා වගකියනු ලබන නිලධාරියෙකු හෝ ආයතනයක් වේ.

වත්කම් සඳහා වත්කම් ලේඛනයක් සැකසීම, වත්කම් වර්ගීකරණය සහ ආරක්ෂණය, වත්කම් සඳහා ප්‍රවේශ සීමා හඳුන්වා දීම, හෝ වත්කමක්

නිල වශයෙන් ඉවත් කිරීමේදී හෝ විනාශ කිරීමකදී එය නිසි පරිදි සිදු වන්නේදැයි සහතික කිරීම වත්කම හිමිකරුගේ සහ භාරකරුගේ වගකීම් වේ.

ආයතනය සිය වත්කම් භාවිතා කරන පරිශීලකයන් ද හඳුනා ගත යුතු වේ. පරිශීලකයන් යනු රාජකාරීමය කටයුතු සඳහා වත්කම් භාවිතා කරන කාර්ය මණ්ඩලය වේ. වත්කම් හිමිකරුවන් විසින්, තමන් භාරයේ පවතින වත්කම් රාජකාරීමය අවශ්‍යතා සඳහා භාවිතා කළ යුතු පරිශීලකයන් නිවැරදිව හඳුනා ගත යුතු අතර එම වත්කම් සඳහා වන ප්‍රවේශයන් මෙහි අංක 4.3.4 සහ 4.3.5 හි දක්වා ඇති ආකාරයට පාලනය කළ යුතු වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2.4. තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් පවත්වා ගැනීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය විසින් තොරතුරු වත්කම් හඳුනාගෙන තොරතුරු වත්කම් ලේඛනයක (Information Assets Register) සටහන් කළ යුතුය. තොරතුරු වත්කම් ලේඛනය යනු ආයතනයක් සතු තොරතුරු වත්කම් පිළිබඳ විධිමත් ඉන්වෙන්ටරියකි. ආයතනයක් අවම වශයෙන් තොරතුරු වත්කම් ලේඛනයේ, වත්කමේ නම, වත්කමේ හිමිකරු සහ භාරකරු, වර්ගීකරණයේ මට්ටම, වර්ගීකරණයට හේතුව, වර්ගීකරණ දිනය, වත්කම් සකසන පරිගණක පද්ධතිය, වත්කම් ගබඩා කරන ස්ථානය, විනාශ කිරීමේ ක්‍රමය, වත්කම නැති වීමකදී, විනාශ වීමකදී හෝ හෙළිදරව් වීමකදී ඇතිවන බලපෑම සහ වත්කමේ වර්ගීකරණය සමාලෝචනය කිරීමේ දිනය සටහන් කළ යුතුය.

ආයතනය සිය තොරතුරු තාක්ෂණ වත්කම් පිළිබඳ විස්තර ද තොරතුරු තාක්ෂණ ලේඛනයක (IT Assets Register) සටහන් කළ යුතුය. අවම වශයෙන්, තොරතුරු තාක්ෂණ වත්කම් ලේඛනයේ වත්කම් වර්ගය (උදා: දෘඩාංග, මෘදුකාංග, සර්වර් පරිගණක), වත්කම පිහිටා ඇති ස්ථානය, එහි මෙහෙයුම් පද්ධතිය, බලපත්‍ර විස්තර, පරිශීලකයන්, අවදානම්, වර්ගීකරණ මට්ටම, ඇස්තමේන්තුගත වටිනාකම යනාදී තොරතුරු සඳහන් කළ යුතුය. තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ලේඛනය නිවැරදි සහ යාවත්කාලීන විය යුතු අතර ඒවා ආයතනයේ අනෙකුත් භාණ්ඩ හා තොග ලේඛන සමග ගැලපිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2.5. අවදානම තක්සේරු කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ වත්කම්වලට ඇති අවදානම් සහ එමගින් වන බලපෑම තීරණය කිරීම සඳහා විධිමත් තක්සේරුවක් සිදු කළ යුතුය. අවදානම් තක්සේරුවක පරමාර්ථය වනුයේ වත්කම් සඳහා ඇති අවදානම් හඳුනා ගැනීමත් එම අවදානම් අවම කිරීම සඳහා ගත යුතු ආරක්ෂක පියවරයන් මොනවාද යන්න තීරණය කිරීමත් ය. අවදානම් තක්සේරුව මත පදනම්ව ආයතනය තුළ අවදානම් ශ්‍රේණි ගත කළ යුතු අතර එම අවදානම් ලේඛනයක (Risk Register) විධිමත්ව සටහන් කළ යුතුය.

ආයතනය විසින් අංක 4.3 හි සඳහන් ප්‍රතිපත්තිමය කරුණු සැලකිල්ලට ගනිමින් අවදානම් ලේඛනයේ සටහන් කර ඇති අවදානම් සඳහා සුදුසු ආරක්ෂක පියවර ගත යුතුය.

අවදානම් තක්සේරුව ආයතනයේ අවදානම් කළමනාකරණ කමිටුව විසින් සිදු කළ යුතුය. එවන් අවදානම් තක්සේරුවක් සිදුකිරීම සඳහා ආයතනය තුළ සුදුසු හැකියාවක් නොමැති අවස්ථාවක, සුදුසුකම් ලත් පළපුරුදු සමාගමක සේවය ලබාගත හැකිය. මේ සඳහා ශ්‍රී ලංකා සර්ට් ආයතනය අදාල ආයතනයට අවශ්‍ය සහයෝගය ලබාදිය යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.2.6. වත්කම් වර්ගීකරණය කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වත්කම් වර්ගීකරණය කළ යුතුය. වත්කම් වර්ගීකරණයේ පරමාර්ථය වනුයේ ආයතනයට එම වත්කමේ ඇති වටිනාකමට සහ

එහි සංවේදීතාවයට අනුව සුදුසු මට්ටමේ ආරක්ෂාවක් ලැබෙන බව සහතික කිරීමයි.

තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් වර්ගීකරණය පිළිගත් මාර්ගෝපදේශවලට අනුව සිදු කළ යුතු අතර තොරතුරු වත්කම් වර්ගීකරණය "ඉතා රහසිගත" (Secret), "රහසිගත" (Confidential), "සීමිත හුවමාරුව" (Limited Sharing), "පොදු" (Public) සහ "වර්ගීකරණය නොකළ" (Unclassified) ලෙස වර්ග කළ යුතුය.

තොරතුරු තාක්ෂණ වත්කම් "ඉතා තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම්" (Very Critical), "තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම්" (Critical), "තීරණාත්මක නොවන තොරතුරු තාක්ෂණ වත්කම්" (Non-Critical) සහ "වර්ගීකරණය නොකළ තොරතුරු තාක්ෂණ වත්කම්" (Unclassified) ලෙස මට්ටම් හතරකට වර්ග කළ යුතුය.

වත්කම් වර්ගීකරණය පිළිබඳ ක්‍රමවේදයක් තොරතුරු සහ සයිබර් ආරක්ෂණ මාර්ගෝපදේශයෙහි දක්වා ඇත. (මෙහි අංක 2.2.(ඇ) හි දක්වා ඇති යොමුව හා බැඳේ).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3. වත්කම් ආරක්ෂා කිරීම

හඳුනාගත් වත්කම් සඳහා ඇති විය හැකි තොරතුරු ආරක්ෂණ සිදුවීමක බලපෑම වැළැක්වීම හෝ සීමා කිරීම සඳහා සුදුසු ආරක්ෂණ ක්‍රමවේද ආයතනය විසින් ක්‍රියාත්මක කළ යුතුය. එසේ යොදනු ලබන ක්‍රමවේදයන්, එක් එක් වත්කමට අදාළ වර්ගීකරණය මත පදනම් විය යුතුය.

මෙම ප්‍රතිපත්තියට අනුකූලව කටයුතු කිරීම සඳහා, ආයතනය විසින් වත්කම් වෙත සිදුවන ප්‍රවේශයන් පාලනය කිරීම, දත්ත සුරක්ෂිත කිරීම සඳහා සුදුසු ක්‍රමවේද භාවිතා කිරීම, සංචරණය වන හා නිශ්චල දත්තවල ආරක්ෂණය සඳහා වන ප්‍රමිතීන්ට අනුගත වීම, වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතා කිරීම, සයිබර් ආරක්ෂණ සිදුවීම්වලට ඔරොත්තුදීමේ හැකියාව සහතික කිරීම සඳහා අවශ්‍ය වෙනත් තාක්ෂණික ක්‍රමවේද භාවිතා කිරීම ඇතුළු ක්‍රියාකාරකම් සිදුකළ යුතුය. වත්කම් ආරක්ෂා කරගැනීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්ති පහත දැක්වේ.

4.3.1. නිශ්චලව පවතින දත්ත ආරක්ෂා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය ඔවුන් සතුව ඇති නිශ්චලව පවතින දත්ත (තොරතුරු වත්කම්) ආරක්ෂා කිරීමට කටයුතු කළ යුතුය. නිශ්චලව පවතින දත්ත යනු උපාංගයෙන් උපාංගයට හෝ ජාලයකින් ජාලයකට ක්‍රියාකාරීව සංචරණය නොවන නිශ්චලව පවතින දත්ත වේ. උදාහරණ ලෙස පරිගණකයක, මේඝයක, දෘඩ තැටියක ගබඩා කර ඇති දත්ත නිශ්චල දත්ත ලෙස දැක්විය හැකිය.

ආයතනයක් තුළ ඇති "ඉතා රහසිගත" හෝ "රහසිගත" ලෙස වර්ගීකරණය කර ඇති ඕනෑම තොරතුරු වත්කමක් ගබඩා කිරීමට පෙර කේතනය (encrypt) කිරීම අත්‍යවශ්‍ය වේ. තවද නිශ්චලව පවතින දත්ත ආරක්ෂා කිරීමේ වෙනත් ක්‍රම අතරට අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේද හරහා පරිශීලක ප්‍රවේශය පාලනය කිරීම සහ වත්කම් සඳහා භෞතික ආරක්ෂාව සැපයීම ඇතුළු මෙම ප්‍රතිපත්තියේ දක්වා ඇති අනෙකුත් අදාළ ක්‍රමවේද ද ඇතුළත් වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.2. සංචරණය වෙමින් පවතින දත්ත ආරක්ෂා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය විසින් ඔවුන් සතු සංචරණය වන දත්ත ආරක්ෂා කිරීමට කටයුතු කළ යුතුය. සංචරණය වන දත්ත යනු අන්තර්ජාලය හරහා හෝ වෙනත් ජාලයක් හරහා එක් ස්ථානයක සිට තවත් ස්ථානයකට සක්‍රියව ගමන් කරන දත්ත වේ. උදාහරණ ලෙස එක ස්ථානයක් සිට තවත් ස්ථානයක් දක්වා ආයතනයකට අයත් පරිගණක ජාලයක් (වයි-ෆයි ජාලද ඇතුළත්ව) හරහා ගමන් කරන දත්ත සංචරණය වන දත්ත ලෙස දැක්විය හැකිය. සංචරණය වන දත්ත ආරක්ෂා කිරීම සඳහා, ආයතනය විසින් තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශයේ සඳහන් කර ඇති පරිදි, සිය සංවේදී තොරතුරු (“ඉතා රහසිගත” හෝ “රහසිගත” ලෙස වර්ගීකරණය කළ තොරතුරු) සංචරණයට පෙර කේතනය කර, ආරක්ෂිත ක්‍රමවේද භාවිතා කර (HTTPS, TLS, SFTP ආදී) සංචරණය වීමට ඉඩ සැලසිය යුතුය. තවද, වයි-ෆයි ජාල හරහා සංචරණය වන දත්ත ආරක්ෂාව තහවුරු කිරීම සඳහා එම ජාලවල ඇති ආරක්ෂක පරාමිතීන් (security parameters) සක්‍රීය කර ඇති බවට ආයතනය සහතික විය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.3. භෞතික ආරක්ෂාව පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සතු වත්කම්වලට සිදු වන අනවසර ප්‍රවේශයන්, සොරා ගැනීම් හෝ වෙනත් අනවසර අත්පත් කර ගැනීම් වැලැක්වීම සඳහා ආයතනය විසින් එම වත්කම් සඳහා අවශ්‍ය භෞතික ආරක්ෂාව සැපයිය යුතුය.

තොරතුරු වත්කම්වල ආරක්ෂණ අවශ්‍යතා මත පදනම්ව, වත්කම් ගබඩා කිරීම හෝ ඒවා සැකසීම (store or process) සඳහා ආරක්ෂිත ස්ථාන හඳුන්වා දිය යුතුය. “ඉතා රහසිගත” සහ “රහසිගත” ලෙස වර්ගීකරණය කර ඇති තොරතුරු වත්කම් ආරක්ෂිත ස්ථානවල ගබඩා කිරීම හෝ සැකසීම අනිවාර්ය වේ.

තවද, (ඉතා) තීරණාත්මක ලෙස වර්ගීකරණය කරන ලද තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂිත ස්ථානවල ගබඩා කර ක්‍රියාත්මක කළ යුතුය.

භෞතික වශයන් වන ආක්‍රමණයන් සහ අනවසර ප්‍රවේශයන් වැළැක්වීම සඳහා ආයතනයේ ආරක්ෂිත ස්ථානයන් බිත්ති වැනි භෞතික ආවරණයන් (පවුරු), අගුලු දැමිය හැකි දොරවල් සහ ආරක්ෂිත උපක්‍රම කිහිපයකින් සමන්විත බහු-සාධක ප්‍රවේශ පද්ධති (multi-factor entry systems) මගින් ආරක්ෂා කළ යුතු අතර, අඛණ්ඩව ආරක්ෂිත කැමරා මගින් ද නිරීක්ෂණය කළ යුතුය.

ආයතනයේ ආරක්ෂිත ස්ථානයන්ට ගිනිගැනීම්, ජලගැලීම්, ආර්ද්‍රතාවය, විද්‍යුත් චුම්භක ක්ෂේත්‍ර සහ උෂ්ණත්ව වෙනස්වීම්වලින් වන හානි වැළැක්වීම සඳහා අවශ්‍ය ක්‍රියාමාර්ග ගත යුතුය. තවද, තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් වෙත වන පරිශීලක ප්‍රවේශයන් පාලනය කිරීම සඳහා මුරපද, ප්‍රවේශ කාඩ්පත්, රහස් අංක සහ ජෛවමිතික ක්‍රමවේද වැනි තාක්ෂණයන් ආයතනය විසින් භාවිතා කළ යුතුය.

ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වෙත අනවසර ප්‍රවේශයන් ක්‍රමවත්ව පාලනය කිරීම සඳහා අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයක් ක්‍රියාත්මක කිරීම ද අත්‍යවශ්‍ය වේ. (ප්‍රතිපත්ති අංක 4.3.4 හි සඳහන් පරිදි).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.4. අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය, සිය තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ඇති පරිශීලක ප්‍රවේශ පාලනය කළ යුතු වේ.

අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය යනු ආයතනයේ තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සුරක්ෂිතව තබා ගැනීමට එම වත්කම් භාවිතා කරන්නන්ගේ අනන්‍යතාවය තහවුරු කර ඒවා ඔවුනට භාවිතා කිරීමට ඇති අවශ්‍යතාවය මත ප්‍රවේශ වීමේ අවසරය ලබාදීමේ ක්‍රියාවලියකි.

පරිශීලකයින්ට ඔවුනට නියමිත කාර්යයන් ඉටු කිරීමට දැනගත යුතු තොරතුරු සහ භාවිතා කළ යුතු වත්කම් සඳහා පමණක් අවශ්‍ය ප්‍රවේශ අවසරය ලබා දිය යුතුය. මෙම කරුණු පදනම් කරගනිමින්, ආයතනය විසින් සිය භාවිතය පිණිස අනන්‍යතා කළමනාකරණ ක්‍රමවේදයක් නිර්මාණය කර ගත යුතුවේ. ශ්‍රී ලංකා සර්ට් ආයතනය විසින් රාජ්‍ය ආයතන සඳහා අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයක් සකස් කර ඇති අතර එය ආයතනයේ අවශ්‍යතාවය පරිදි ගලපා භාවිතයට ගත හැකිය.

ආයතනය විසින් ක්‍රියාත්මක කරන අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයෙහි ප්‍රමාණවත් බවත් යාවත්කාලීන බවත් ආයතනය සහතික කළ යුතු අතර එවැනි ක්‍රමවේදයක් ආයතනය තුළ ක්‍රියාත්මක වන අවස්ථාවන්හිදී සියලුම ආයතන සේවකයින්ට අමතරව තෙවන පාර්ශවීය සේවා සැපයුම්කරුවන් ද එම අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයට අනුගතව කටයුතු කරන බවට ආයතනය සහතික විය යුතුය.

අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදය උල්ලංඝනය කිරීමකදී අවශ්‍ය පියවර ගැනීම සඳහා තොරතුරු ආරක්ෂණ කමිටුව වෙත වාර්තා කළ යුතු අතර ආයතනය තුළ තොරතුරු ආරක්ෂණ කමිටුවක් පිහිටුවා නොමැති අවස්ථාවකදී එම සිදුවීම ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරියා මගින් ආයතන ප්‍රධානී වෙත වාර්තා කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.5. ශක්තිමත් සත්‍යාපනය පිළිබඳ ප්‍රතිපත්තිය

සත්‍යාපනය යනු පරිශීලකයෙකුගේ අනන්‍යතාවය හඳුනා ගැනීමේ ක්‍රියාවලියයි. සත්‍යාපන ක්‍රියාවලියේදී පරිශීලකයා හඳුනාගැනීම (අනන්‍යතාවය හඳුනා ගැනීම) සහ සාක්ෂි මගින් පරිශීලකයා තහවුරු කරගැනීම (අනන්‍යතාවය සත්‍යාපනය කිරීම) තුළින් ආයතනයේ තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් වෙත ප්‍රවේශය සපයනු ලැබේ.

ප්‍රතිපත්ති අංක 4.3.4 හි සඳහන් ආයතනික අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේදයට අනුකූලව, පරිශීලකයෙකුගේ අනන්‍යතාවය තහවුරු කිරීම සඳහා ආයතනය ශක්තිමත් සත්‍යාපනයක් භාවිතා කළ යුතුය.

පරිශීලක නාමය සහ මුරපද සංයෝජනය සහ බහු සාධක සත්‍යාපනය (multi-factor authentication) භාවිතා කිරීම වැනි ශක්තිමත් ක්‍රමවේද පරිශීලක අනන්‍යතාවය සත්‍යාපනය කිරීම සඳහා නිර්දේශ කෙරේ.

ශක්තිමත් සත්‍යාපන ක්‍රියාවලියක් සහතික කිරීම සඳහා ආයතනය, සිය අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේදය සැකසීමේදී, ශක්තිමත් මුරපද භාවිතය සහ බහු සාධක සත්‍යාපනය පිළිබඳ පහත සඳහන් කරුණු ද ආවරණය කළ යුතුය.

(අ) ශක්තිමත් මුරපද:

- මුරපද අවම වශයෙන් අක්ෂර 8 කින් සමන්විත විය යුතු අතර එය ඉංග්‍රීසි හෝඩියේ කැපිටල් සහ සිම්පල් අකුරු (උදා: a-Z), ඉලක්කම් (0-9) සහ විශේෂ අක්ෂරවලින් (!@$+/) සමන්විත විය යුතුය.
- සාමාන්‍ය පරිශීලකයන්ගේ සියලුම මුරපද දින 90 කට වරක් වෙනස් කළ යුතුය. වරප්‍රසාද සහිත පරිශීලකයන් සඳහා (privileged users) ප්‍රවේශ ලබා දිය යුත්තේ අවශ්‍යතා පදනම මත පමණි.

(ආ) බහු සාධක සත්‍යාපනය:

- ‘‘ඉතා රහසිගත’’ සහ ‘‘රහසිගත’’ තොරතුරු වෙත ප්‍රවේශය ඇති පරිශීලක ගිණුම් සුරක්ෂිත කිරීම සඳහා ආයතනය බහු සාධක සත්‍යාපන ප්‍රවේශය ක්‍රියාත්මක කළ යුතුය.
- බහු සාධක සත්‍යාපන ක්‍රමයක් සැලසුම් කිරීමේදී, ආයතනය, අවම වශයෙන් පරිශීලකයා දන්නා යම් කරුණක් (උදා: පරිශීලක මුරපදය), පරිශීලකයා සන්තකයේ ඇති යමක් (උදා: ටෝකනය, ප්‍රවේශ කාඩ්පත) හෝ ජීවමිතික දත්තයක් (උදා: ඇඟිලි සළකුණු) යන සංයෝජන සැලකිල්ලට ගත යුතුය.

කුමන හේතුවක් මත හෝ ආයතනය හැර යන සේවකයෙකු, තවදුරටත් ආයතනික වත්කම් වෙත ප්‍රවේශ වීම වැළැක්වීම සඳහා, එම සේවකයාට ලබා දී ඇති ගිණුම් සහ වෙනත් සත්‍යාපන දත්ත ආයතනය විසින් වහාම ඉවත් කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.6. දත්ත ස්වෛරීභාවය සහ මේඝගත පරිගණක භාවිතය පිළිබඳ ප්‍රතිපත්තිය

දත්ත ස්වෛරීභාවය (data sovereignty) යනු දත්ත (තොරතුරු වත්කම්) එක්රැස් කිරීම, සැකසීම සහ ගබඩා කිරීම සිදු කරනු ලබන රට තුළ පවතින නීති සහ පාලන ව්‍යුහයන්ට එම ක්‍රියාවන් නෛතිකව බැඳී පවතින බවයි. මෙම සන්දර්භය තුළ රාජ්‍ය ආයතනය, දත්ත එක්රැස් කිරීම, සැකසීම සහ ගබඩා කිරීම සඳහා වෙනත් රටවලින් මේඝගත සේවා (cloud services) ලබා ගන්නා විට එම දත්තවල ස්වෛරීභාවය ගැන අතිශයින් සැලකිලිමත් විය යුතුය.

මේඝගත පරිගණක භාවිතය යනු පරිශීලකයන්ගේ සෘජු කළමනාකරණයකින් තොරව ඉල්ලුම මත දත්ත ගබඩා කිරීම, සැකසීම, යෙදවුම් සංවර්ධන වේදිකා (development platforms) වැනි තොරතුරු සහ සන්නිවේදන තාක්ෂණ සම්පත් ලබා ගැනීමේ හැකියාවයි. වර්තමානයේ බොහෝ ආයතන පිරිවැය ඉතිරිකිරීම් සහ කාර්ය සාධනය වැඩිකිරීමේ අරමුණින් මේඝගත සේවා ලබාගැනීමට යොමු වේ.

නමුත්, දත්ත ස්වෛරීභාවය තහවුරු කිරීම සඳහා මේඝගත සේවා භාවිතා කිරීමේ අවදානම පිළිබඳව ආයතනය ප්‍රවේශම් විය යුතු අතර, විශේෂයෙන් පොදු මේඝගත සේවා (public cloud services) භාවිතා කිරීමේ අවදානම පිළිබඳව වඩාත් සැලකිලිමත් විය යුතු වේ. පොදු මේඝගත සේවා යනු, ඒවා මිලදී ගැනීමට කැමති ඕනෑම කෙනෙකුට ලබා ගත හැකි සේවාවන්ය. මේඝගත සේවා විවිධ රටවල නීතිවලට යටත්ව ක්‍රියාත්මක වන බැවින් ඒවා පාලනය කිරීමේ ඇති දුෂ්කරතා, එහි නිර්මාණාත්මක ව්‍යුහයේ ඇති සීමිත පාරදෘශ්‍යභාවය, මෙහෙයුම් ක්‍රියාවලිවල ඇති සීමිත විනිවිදභාවය, සහ සේවා ගිවිසුම්වල ඇති සැලකිය යුතු නොගැලපීම් මේඝගත සේවාවන් ලබාගැනීමේදී ඇති අවදානම් වේ.

මේඝගත සේවා අවශ්‍යතා සඳහා, ආයතන, ශ්‍රී ලංකා රාජ්‍ය මේඝය (Lanka Government Cloud) මගින් සේවාවන් ලබා ගැනීමට ප්‍රමුඛතාවය ලබා දිය යුතුය. ශ්‍රී ලංකා රාජ්‍ය මේඝය යනු රජයේ මේඝගත සේවා අවශ්‍යතා සපුරාලීම සඳහා පිහිටුවන ලද, තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය යටතේ ක්‍රියාත්මක වන, රජය සතු රාජ්‍ය ආයතන සඳහා පමණක් සීමා වූ මේඝගත සේවාවකි. කෙසේවෙතත්, ආයතනය විසින් ඕනෑම ආකාරයක මේඝගත සේවාවක් ලබා ගැනීමට පෙර නිසි අවදානම් තක්සේරුවක් අනිවාර්යයෙන්ම සිදු කළ යුතු වේ.

තවද, ආයතනයේ දත්ත රැස් කිරීම, ගබඩා කිරීම සහ සැකසීම හෝ මෘදුකාංග සඳහා සත්කාරකත්වය ලබාගැනීම ආදී සියලුම ක්‍රියාකාරකම් ශ්‍රී ලංකාවේ දත්ත ආරක්ෂණයට අදාළව පවතින නීති සහ රෙගුලාසිවලට අනුකූලව සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.7. වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතය සහ සරිමා යාවත්කාලීන කිරීම් පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වලංගු බලපත්‍ර සහිත සහ නිසි පරිදි යාවත්කාලීන කරන ලද මෘදුකාංග භාවිතා කළ යුතුය. මෙයට පද්ධති මෘදුකාංග, උපයෝගිතා වැඩසටහන් සහ යෙදුම් මෘදුකාංග ආදිය ඇතුළත්ය. උදාහරණ ලෙස මෙහෙයුම් පද්ධති, වවන සැකසුම් පැකේජ, දත්ත ගබඩා, වෙබ් බ්‍රවුසර්, ප්‍රති-අනිෂ්ට මෘදුකාංග යානාදිය වලංගු බලපත්‍රයන් සහිතව භාවිතා කළ යුතු අතර ඒවායේ සරිමා (patch updates) යාවත්කාලීන කිරීම ද නිසි පරිදි සිදු කළ යුතුය.

ආයතනය විසින් මෙහෙයුම් පද්ධති සහ අනෙකුත් අදාළ මෘදුකාංග සපයන්නන් විසින් සපයන ලද නවතම සරිමා මගින් යාවත්කාලීන කළ යුතුය. තවද, ආයතන සිය මෘදුකාංගයන්හි ස්වයංක්‍රීය යාවත්කාලීන කිරීම් සක්‍රීය කළ යුතුය.

තවද සැපයුම්කරු විසින් සපයන ලද තීරණාත්මක සරිමා ස්ථාපනය කිරීමට පෙර ඒවා ස්ථාපනය කිරීමෙන් ඇතිවිය හැකි බලපෑම පිළිබඳ නිසි ඇගයීමක් සිදු කළ යුතුය (විශේෂයෙන්ම ඉතා තීරණාත්මක හෝ තීරණාත්මක ලෙස වර්ගීකරණය කර ඇති තොරතුරු තාක්ෂණ වත්කම් සඳහා).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.8. ප්‍රති-අනිෂ්ට මෘදුකාංග භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වලංගු බලපත්‍රයක් සහිත ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කළ යුතුය. ප්‍රති-අනිෂ්ට මෘදුකාංග ඕනෑම තොරතුරු තාක්ෂණ වත්කමකට ප්‍රවේශ වීමේ හැකියාවක් ඇති ස්ථානවල (උදා: පරිගණක හා ඒවා ආශ්‍රිත මෙවලම්, අන්තර්ජාලයට නිරාවරණය වන මුහුණත් සහිත තොරතුරු තාක්ෂණ මෙවලම් ආදිය) සක්‍රීයව පැවතිය යුතුය. තවද එම ප්‍රති-අනිෂ්ට මෘදුකාංග යාවත්කාලීන විය යුතු අතර ඒවා ස්වයංක්‍රීයව යාවත්කාලීන වන ලෙස වින්‍යාස ගත (configure) කළ යුතුය.

වෙබ් අඩවි වෙත පිවිසීමේදී, ඩිජිටල් ලිපිගොනු බාගත කිරීම හෝ විවෘත කිරීමේදී, ඉවත් කළ හැකි දත්ත ගබඩාකරන මෙවලම් (removable storage devices) භාවිතයේදී ඒවා ස්වයංක්‍රීයව පරිලෝකනය (scan) කර අනිෂ්ට මෘදුකාංග හඳුනාගැනීමට හැකි වන පරිදි ප්‍රති-අනිෂ්ට මෘදුකාංග වින්‍යාස ගත කළ යුතුය.

ප්‍රති-අනිෂ්ට මෘදුකාංගවල වින්‍යාසය වෙනස් කිරීම, අස්ථාපනය කිරීම, අක්‍රිය කිරීම හෝ වෙනත් ආකාරයකින් විකෘති කිරීම පරිශීලකයින්ට තහනම් කළ යුතුය.

රාජ්‍ය ආයතනයක් තවත් ආයතනයකට හෝ මහජනතාව වෙත ඉලෙක්ට්‍රොනික මාධ්‍යයෙන් තොරතුරු සන්නිවේදනයේදී ඒවා අනිෂ්ට මෘදුකාංගවලින් තොර බව සහතික කර ගැනීමෙන් අනතුරුව එම සන්නිවේදනයන් සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.9. නිල විද්‍යුත් තැපැල් පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය නිල සන්නිවේදන කටයුතු සඳහා නිල විද්‍යුත් තැපැල් ලිපින පමණක් භාවිතා කළ යුතුය. සේවකයින් සිය පෞද්ගලික සන්නිවේදන කටයුතු සඳහා නිල ඊමේල් ලිපින භාවිතා නොකළ යුතුය.

නිල විද්‍යුත් තැපැල් යනු "gov.lk" යන වසම් නාමය යටතේ රජය විසින් සපයන ලද විද්‍යුත් තැපැල් ලිපින වේ. නිල විද්‍යුත් තැපැල් ගිණුම් ආයතනය සතු නිල වත්කමක් වන අතර ඕනෑම අවස්ථාවක එම ගිණුම්වලට ප්‍රවේශ වීමට, විද්‍යුත් තැපැල් කියවීමට හෝ ගිණුම ඉවත් කිරීමට ආයතනයට අයිතිය ඇත්තේය.

සියලුම විද්‍යුත් තැපැල් ඇමුණුම්, එහි මූලාශ්‍රය හෝ අන්තර්ගතය කුමක් වුවත්, ආයතනයේ පරිගණකයක හෝ පද්ධතියක විවෘත කිරීමට හෝ ගබඩා කිරීමට පෙර වෛරස සහ වෙනත් අනිෂ්ට මෘදුකාංග තිබේදැයි පරිලෝකනය කර බැලිය යුතුය. තවද ආයතන සිය නිල විද්‍යුත් තැපැල් සම්බන්ධයෙන් රජය විසින් කලින් කලට නිකුත් කරනු ලබන රෙගුලාසි සහ මාර්ගෝපදේශයන්ට අනුකූලව කටයුතු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.10. විද්‍යුත් තැපැලෙහි ආරක්ෂාව පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක් ඔවුන්ගේ විද්‍යුත් තැපැල් ගිණුම්වලට අදාළ ආරක්ෂක විශේෂාංග ඇතුළත් කොට වින්‍යාස ගත කළ යුතුය. තොරතුරුවල ආරක්ෂාව සහතික කිරීම සඳහා, විද්‍යුත් තැපැල් සේවාදායක පරිගණකය (email server) දත්ත ආරක්ෂණය සම්බන්ධයෙන් වන නීතිමය විධිවිධානවලට අනුගතව ස්ථාපනය කළ යුතුය.

ආයතනය, විද්‍යුත් තැපැල් පෙරහන් (email filters) සක්‍රීය කිරීම මගින් අනිෂ්ට මෘදුකාංග ඇතුල්කොට ඇති විද්‍යුත් තැපැල් ඉවත්කිරීමද, අයාචිත විද්‍යුත් ලිපි (spam emails) ලැබීම අවම කිරීමට ද ක්‍රියාමාර්ග ගත යුතුය. තවද විද්‍යුත් තැපැල් හරහා සංවේදී

තොරතුරු යැවීමේදී ඒවා අනිවාර්යයෙන්ම කේතනය කර යැවිය යුතුය.

ආයතනයේ විද්‍යුත් තැපැල් ගිණුම් ලංකා රාජ්‍ය ජාලය විසින් සපයනු ලබන අවස්ථාවන්හිදී, එම විද්‍යුත් තැපැල් සේවාව ආරක්ෂිතව වින්‍යාස කර ඇති බව ශ්‍රී ලංකා තොරතුරු තාක්ෂණ නියෝජිතායතනය සහතික විය යුතු අතර, අධීක්ෂණ හෝ නියාමන අවශ්‍යතා සඳහා වරින් වර ආරක්ෂක විගණන වාර්තා ශ්‍රී ලංකා සර්ට් ආයතනයෙන් ලබා ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.11. ඩිජිටල් අත්සන් භාවිතය පිළිබඳ ප්‍රතිපත්තිය

සුදුසු අවස්ථාවලදී, ආයතනය විසින් ඩිජිටල් අත්සන් ක්‍රියාත්මක කළ යුතුය. එමගින්, විද්‍යුත් තැපැල්වල නිරවද්‍යතාවය, තථ්‍යභාවය (authenticity), සහ යවනු ලබන පුද්ගලයා විසින්ම අදාල විද්‍යුත් තැපැල යවන ලද බව තහවුරු හැකි බව සහතික කළ හැකිය (non-repudiation).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.12. පරිමිති ආරක්ෂණ පාලනයන් පිළිබඳ ප්‍රතිපත්තිය

අනිෂ්ට මෘදුකාංග අන්තර්ජාලය හරහා ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම්වලට ප්‍රවේශ වීම වැළැක්වීමට සහ අනෙකුත් සයිබර් ප්‍රහාරවලින් එම වත්කම්වලට ආරක්ෂාව සැපයීමට ආයතනය විසින් ගිනිපවුරු සහ ආක්‍රමණ හඳුනාගැනීමේ හා ආක්‍රමණ වැළක්වීමේ පද්ධති (Intrusion Detection Systems/ Intrusion Prevention Systems) වැනි පරිමිති ආරක්ෂණ ක්‍රමවේද (perimeter security methods) ස්ථාපනය කළ යුතුය.

ආයතනය විසින් ස්ථාපනය කර ඇති පරිමිති ආරක්ෂණ උපාංගවල තර්ජන පිළිබඳ විස්තර ඇතුළත් වන දත්ත ගබඩා (threat databases) නිතිපතා යාවත්කාලීන කිරීම, ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කර ඒවා ස්වයංක්‍රීයව යාවත්කාලීන වීමට සැකසීම, සුදුසු ආරක්ෂක වින්‍යාසයන් යොදාගනිමින් පෙරනිමි සැකසුම් (default settings) යාවත්කාලීන කිරීම, සහ සැපයුම්කරු විසින් නිර්මාණය කරන ලද පරිශීලක ගිණුම් (vendor supplied user accounts) අක්‍රිය කිරීම යනාදී කටයුතු සිදු කළ යුතුය. පරිමිති ආරක්ෂණ මෙවලම් සඳහා සුදුසු අරක්ෂක වින්‍යාස පිළිබඳ විශ්ලේෂණයක් තොරතුරු සහ සයිබර් ආරක්ෂණ මාර්ගෝපදේශයේ දක්වා ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.13. ආරක්ෂිත දුරස්ථ ප්‍රවේශ භාවිතය පිළිබඳ ප්‍රතිපත්තිය

වෙනත් ස්ථානවල සිට (භූගෝලීය වශයෙන් දුරස්ථ ස්ථාන) ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම්වලට වන අනවසර ප්‍රවේශයන් වැළැක්විය යුතුය. ඒ සඳහා දුරස්ථ ක්‍රම හරහා ආයතනයේ අභ්‍යන්තර ජාල වෙත සිදු කෙරෙන ප්‍රවේශ පාලනය කළ යුතුය. දුරස්ථ ප්‍රවේශ ක්‍රම හරහා ආයතනය වෙත බොහෝ තොරතුරු ආරක්ෂණ තර්ජන පැමිණේ. දුරස්ථ ප්‍රවේශය හා සම්බන්ධ ආරක්ෂක අවදානම් ලෙස අන්තර්ජාලය හරහා තොරතුරු සංචරණයේදී අනවසරයෙන් එම දත්ත නිරාවරණය කිරීම, දත්ත වෙත අනවසරයෙන් ප්‍රවේශ වීම, අනවසරයෙන් දත්ත වෙනස් කිරීම සහ වෙනත් අනිෂ්ට මෘදුකාංග ආයතනයේ පද්ධතියට ඇතුළු වී හානි සිදු කිරීම ආදිය දැක්විය හැකිය.

දුරස්ථ ප්‍රවේශයන් නිසා ආයතනයට ඇති වන අවදානම් අවම කිරීම සඳහා, ආයතනය විසින් ආරක්ෂිත තත්‍යසම පෞද්ගලික ජාල (Virtual Private Networks) භාවිතා කිරීම, ආයතනයේ අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ප්‍රතිපත්තිය මත පදනම්ව ආයතනික පද්ධති වෙත ප්‍රවේශ වීමට බලයලත් පරිශීලකයින්ට පමණක් ඉඩ සැලසීම, බහු සාධක සත්‍යාපනය ක්‍රියාත්මක කිරීම සහ විශ්වාසදායී ජාල පමණක් භාවිතා කිරීම ආදී ක්‍රියාමාර්ග ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.14. උපස්ථ උපාය මාර්ග පිළිබඳ ප්‍රතිපත්තිය

ආපදා අවස්ථාවකදී බිඳ වැටුණු හෝ අඩපණ වූ ආයතනයේ එදිනෙදා ක්‍රියාකාරකම් ප්‍රතිස්ථාපනය කිරීම සඳහා අවශ්‍ය දත්ත, ලොග් සටහන්, පද්ධති, මෘදුකාංග, විනාහස විස්තර (configuration details) සහ වෙනත් ඕනෑම තොරතුරක් උපස්ථ කිරීම (backup) සඳහා ආයතනය සතුව ක්‍රමවේදයක් තිබිය යුතුය. මෙම උපායමාර්ගය ආයතනයේ ආපදා ප්‍රතිසාධන සැලැස්මට (Disaster Recovery Plan) අනුකූල විය යුතුය (අංක 4.6.1 හි සඳහන් පරිදි).

ආයතනය විසින් තම උපස්ථ භාවිත කොට ආයතනයේ අඩපණ වූ හෝ බිඳ වැටුණු සේවා නිසි පරිදි ක්‍රියාත්මක කළ හැකි බව අනිවාර්යයෙන්ම තහවුරු කර ගත යුතුය.

උපස්ථ මාධ්‍යයන්හි ගබඩා කර ඇති දත්ත රජයේ නියාමන අවශ්‍යතාවය මත සංරක්ෂණය කළ යුතුය.

උපස්ථ කළ යුතු කාල පරාසය තීරණය කිරීම සඳහා ආයතනය විසින් ප්‍රතිසාධන කාල අරමුණ සහ ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණ (Recovery Time Objective and Recovery Point Objective) ද හඳුන්වා දිය යුතුය.

රැන්සම්වෙයා ඇතුළු ඕනෑම ද්වේශසහගත සයිබර් ප්‍රහාරයකින් සජීවී දත්ත ආරක්ෂා කිරීම සඳහා එම සජීවී දත්ත ඊට අදාළ උපස්ථ දත්ත වලින් සම්පූර්ණයෙන්ම වෙන් කොට තිබිය යුතු යුතුය.

තවද උපස්ථගත කරන ලද දත්ත හා තොරතුරු එහි දත්ත සැකසුම් ස්ථානයෙන් දුරස්ථ ආරක්ෂිත ස්ථානයක ගබඩා කළ යුතුය. උපස්ථකරණය සඳහා සිදු කරන ලද ඕනෑම වෙනස්කමක් හඳුනා ගැනීමට හැකි වන ක්‍රමවේදයක් ද තිබිය යුතුය.

"ඉතා රහසිගත" සහ "රහසිගත" ලෙස වර්ගීකරණය කර ඇති තොරතුරු වත්කම්වල උපස්ථ, වත්කම් ලේඛනයේ දක්වා ඇති ආරක්ෂක අවශ්‍යතාවයන්ට අනුගතව ගබඩා කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.15. රාජ්‍ය ආයතන විසින් සපයන තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂාව පිළිබඳ ප්‍රතිපත්තිය

වර්තමානයේ මහජනතාව සහ බොහෝ රාජ්‍ය සහ රාජ්‍ය නොවන ආයතන රජය විසින් සපයන තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් (ඩිජිටල් යටිතල පහසුම්, ඉ-සේවා, යෙදවුම්) මත පදනම්ව කට යුතු කරනු දැකිය හැකිය. එවන් පසුබිමක් තුළ, ශ්‍රී ලංකා තොරතරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය හෝ වෙනත් රාජ්‍ය ආයතන විසින් නිර්මාණය කරන ලද යෙදවුම් හෝ ඩිජිටල් යටිතල පහසුම්වල ආරක්ෂාව, ඒවායේ විශ්වාසනීයභාවය, අකණ්ඩතාවය, සහ නිරවද්‍යතාවය සහතික කළ යුතු වේ. උදාහරණ ලෙස, ලංකා රාජ්‍ය ජාලය (Lanka Government Network), ලංකා රාජ්‍ය මේඝය, විද්‍යුත් තැපැල් සේවා, ලංකා රාජ්‍ය ගෙවීම් පද්ධතිය (Lanka Government Payment System), කෙටි පණිවුඩ සේවාව, ලේඛන කළමනාකරණ පද්ධති හෝ වෙනත් සේවාවන්වල ආරක්ෂාව අදාල ආයතනය විසින් සහතික කළ යුතුය. මේ සඳහා අවශ්‍ය ආරක්ෂණ සහතිකයන් අදාල ආයතනය විසින් ශ්‍රී ලංකා සර්ට් ආයතනයෙන් හෝ වෙනත් සුදුසුකම් ඇති ආයතනයකින් ලබා ගත යුතුය.

අනුකූලතාව: තොරතරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය සහ *සියලුම* රාජ්‍ය *ආයතන සඳහා අදාළ වේ.*

4.3.16. ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය සහ භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක්, අලුතින් මෘදුකාංග මිලදී ගැනීමේදී හෝ ආයතනය තුළම සිය මෘදුකාංග සංවර්ධනය කිරීමේදී ආරක්ෂාව අනුබද්ධ කරගත් මෘදුකාංග සංවර්ධන ක්‍රමවේදයක් අනුගමනය කළ යුතුය. මෙම ක්‍රමවේදය අනුගමනය කිරීමේදී සම්ප්‍රදායික මෘදුකාංග සංවර්ධන ක්‍රමවේදයට වඩා ඉදිරි පියවරක් ගනිමින් මෘදුකාංගයක සංවර්ධන ජීවන චක්‍රයේ සෑම අදියරකටම තොරතුරු හා සයිබර් ආරක්ෂක කරුණු එක් කිරීම සිදු කරනු ලබයි.

මෘදුකාංග සංවර්ධනය කිරීමේදී (හෝ මෘදුකාංග මිලදී ගැනීමේදී), ආයතනය විසින් ව්‍යාපෘතිය සැලසුම් කිරීමේ (planning) අදියරේ සිටම

මෘදුකාංගයේ ආරක්ෂාව සැලසුම් කිරීමත්, අවදානම් තක්සේරු කිරීමත්, ලංසු ලේඛනවල ආරක්ෂක අවශ්‍යතා පිළිබඳව පැහැදිළිව සඳහන් කිරීමත් සිදු කළ යුතුය. නිර්මාණකරණ (designing) අදියරේදී සංවර්ධනය කළ යුතු මෘදුකාංගයේ යෝජිත ආරක්ෂක නිර්මාණාත්මක ව්‍යුහය සමාලෝචනය කිරීම ද, සංවර්ධනය කරන (development) අදියරේදී ආරක්ෂාව සම්බන්ධයෙන් වන දුර්වලතා (දෝෂ) හඳුනා ගැනීම සඳහා කේතය සමාලෝචනය කිරීමත් කළ යුතුය.

එකී මෘදුකාංගය ක්‍රියාත්මක කිරීමේ (implementation) අදියරේදී එහි වෙනත් ආරක්ෂක දුර්වලතා හඳුනා ගැනීම සඳහා ආරක්ෂණ විගණනයක් සිදු කිරීමත් කළ යුතුය. අවසාන වශයෙන්, පද්ධතිය ආයතනයෙන් ඉවත් කිරීමේ (decommissioning) අදියරේදී අනවසර පුද්ගලයින්ට එහි දත්ත සහ අනෙකුත් තොරතුරු වත්කම් වෙත ප්‍රවේශ වීමට හෝ නැවත එම දත්ත ප්‍රතිසාධනය කිරීමට නොහැකිවන සේ පද්ධති (හෝ මෘදුකාංග) ආරක්ෂිතව බැහැර කළ යුතුය.

තවද, ආයතනය වෙබ් අඩවි සහ වෙබ් යෙදවුම් සංවර්ධනය කිරීමේදී, ශ්‍රී ලංකා සර්ට් ආයතනය විසින් රාජ්‍ය ආයතන වෙත නිකුත් කර ඇති "වෙබ් අඩවි ආරක්ෂණ මාර්ගෝපදේශය", "වෙබ් යෙදවුම් ආරක්ෂණ මාර්ගෝපදේශය", සහ තාක්ෂණික කරුණු අඩංගු "වෙබ් යෙදවුම් ආරක්ෂාව සඳහා වන තාක්ෂණික මාර්ගෝපදේශය" පිළිපැදිය යුතුය. මෙම මාර්ගෝපදේශයන් ශ්‍රී ලංකා සර්ට් ආයතනයේ https://www.onlinesafety.lk වෙබ් අඩවියෙන් බාගත කළ හැකිය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.17. වත්කම් සුරක්ෂිතව බැහැර කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක්, සිය වත්කමක් තවදුරටත් අවශ්‍ය නොවන විටකදී විධිමත් ක්‍රියා පටිපාටියක් අනුගමනය කරමින් එම වත්කම් ආරක්ෂිතව බැහැර කළ යුතුය. ආයතනය සිය දත්ත ගබඩා මාධ්‍යයන් වන ප්‍රකාශ මාධ්‍ය (ඩිස්ක්), චුම්බක මාධ්‍ය (ටේප් හෝ ඩිස්කට්), තැටි ධාවක, ෆ්ලෑෂ් ගබඩා උපාංග සහ ලේඛන (කඩදාසි ලේඛන හෝ ඡායාරූප මාධ්‍ය) යනාදිය ආරක්ෂිතව බැහැර කිරීමට කටයුතු කළ යුතුය.

අදාළ ගබඩා මාධ්‍යයේ තවදුරටත් අවශ්‍ය නොවන තොරතුරු තිබේ නම්, එම තොරතුරු ලබා ගැනීම හෝ ප්‍රතිස්ථාපනය වැලැක්වීම සඳහා, ඒවා නැවත ලබාගත නොහැකි ආකාරයෙන් ඉවත් කළ යුතුය. අවම වශයෙන් දත්ත ගබඩා මධ්‍යයේ අංශ පදනම්කරගත් ආකෘතීකරණය කර (sector-based formatting) මාධ්‍යවල ඇති තොරතුරු විනාශ කළ යුතුය.

ගබඩා මාධ්‍යයේ ඇති වත්කම් "ඉතා රහසිගත" හෝ "රහසිගත" ලෙස වර්ගීකරණය කර ඇත්නම්, ඒ සඳහා තොරතුරු ආරක්ෂණ කමිටුව වෙතින් ලබාගත් නිර්දේශ මත බැහැර කිරීමේ ක්‍රියාවලිය ආරම්භ කළ යුතුය.

තවද, දත්ත ගබඩා මධ්‍ය කොටස්වලට කපා දැමීමෙන් හෝ සිදුරු කිරීමෙන් තොරතුරු වත්කම් අඩංගු මාධ්‍ය ස්ථිරවම පාරිසරික ආරක්ෂණ නීති සහ රෙගුලාසිවලට යටත්ව භෞතික වශයෙන් විනාශ කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.18. අභ්‍යන්තර තොරතුරු හා සයිබර් ආරක්ෂණ විගණන ක්‍රියාවලිය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය විසින් තොරතුරු ආරක්ෂණ විගණන වැඩසටහන් ක්‍රියාත්මක කළ යුතු අතර එම විගණනයන් සඳහා, ආයතනය තුළ ස්ථාපනය කර ඇති විවිධ තොරතුරු ආරක්ෂණ ක්‍රමවේදවල ප්‍රමාණාත්මකභාවය, පරිගණක යෙදවුම්වල පවතින ආරක්ෂණ ක්‍රියාමාර්ගයන්, පරිගණක ජාලයන්හි නිර්මාණාත්මක ව්‍යුහයේ ඇති ආරක්ෂාව, ආයතනයේ තොරතුරු ආරක්ෂක අනුකූලතා, අභ්‍යන්තර සහ බාහිර තොරතුරු ආරක්ෂණ දුර්වලතා ආදිය පිළිබඳ වන ඇගයීම් (Vulnerability Assessments) සහ සමාලෝචනයන් ද සැබෑ සයිබර් ප්‍රහාර කෘත්‍රිමව ඇති කරමින් ආයතනයේ තොරතුරු ආරක්ෂණ සූදානම ඇගයීම සඳහා සිදු කරනු ලබන විනිවිදයාමේ පරීක්ෂණයන් (Penetration Tests) ද ඇතුළත් විය යුතුය.

තවද ආයතනයට අදාළ තොරතුරු ආරක්ෂණ සිදුවීමකින් පසු, තොරතුරු හෝ තොරතුරු තාක්ෂණ වත්කම්වලට සිදු කරනු ලැබූ යම් වෙනසකින් පසු, ආයතනය අනුගත විය යුතු සම්මත මාර්ගෝපදේශයන්ට සිදුවන වෙනස් වීමකින් පසු, වෛරස් හෝ අනිෂ්ට මෘදුකාංග පැතිරීමකින් පසු හෝ තොරතුරු ආරක්ෂණ කමිටුව විසින් නිර්දේශ කරනු ලබන අවස්ථාවකදී තොරතුරු ආරක්ෂණ විගණනයන් සිදු කළ යුතුය. ඉහත කරුණු වලින් ස්වායක්තව, ආයතනයේ තොරතුරු ආරක්ෂණ විගණනයන් අවම වශයෙන් වසරකට වරක් හෝ සිදු කිරීම අනිවාර්ය වේ.

ආයතනයේ (ප්‍රධාන) අභ්‍යන්තර විගණක විසින් ඉහත විගණනයන් සම්බන්ධීකරණය කළ යුතු අතර, එක් එක් අමාත්‍යාංශයේ ප්‍රධාන අභ්‍යන්තර විගණක එහි විෂය පථය යටතේ ඇති ආයතනවල තොරතුරු ආරක්ෂණ විගණනයන් සම්බන්ධීකරණය කළ යුතුය.

විගණන වාර්තා මගින් ඉදිරිපත් කරන ලද නිර්දේශ ක්‍රියාත්මක වීම අධීක්ෂණය කිරීම සඳහා ආයතනය විසින් විධිමත් ක්‍රියාවලියක් ස්ථාපිත කිරීම කළ යුතුය. ඒ සඳහා ආයතනයේ (ප්‍රධාන) විගණක නිලධාරී මූලිකත්වය සහ වගකීම ගෙන කටයුතු කළ යුතුය.

තොරතුරු ආරක්ෂණ විගණනයන් ඒ සඳහා සුදුසුකම් ලත් පාර්ශ්වයක් විසින් හෝ ශ්‍රී ලංකා සර්ට් ආයතනය විසින් සිදු කළ යුතුය.

වෙනත් පාර්ශ්වයක් විසින් එම විගණනයන් සිදු කරන්නේ නම්, එහි රහස්‍යභාවය තහවුරු කිරීම සඳහා හෙළිදරව් නොකිරීමේ ගිවිසුමක් අදාළ පාර්ශවය සමඟ ඇති කර ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.19. භාවිතය ආරම්භ කිරීමට පෙර සිදු කරන විගණන පිළිබඳ ප්‍රතිපත්තිය

අභ්‍යන්තර තොරතුරු ආරක්ෂණ විගණන වැඩසටහනට සමගාමීව, ආයතනය ඕනෑම වෙබ් අඩවියක්, වෙබ් යෙදුමක් හෝ පද්ධතියක් නිල වශයෙන් දියත් කිරීමට පෙර අවදානම් තක්සේරු කිරීම් සහ විනිවිද යාමේ පරීක්ෂණ (Vulnerability Assessments and Penetration Tests) සිදු කළ යුතුය.

එම තොරතුරු ආරක්ෂණ විගණනයන් සඳහා ශ්‍රී ලංකා සර්ට් ආයතනයෙහි සේවාව හෝ ශ්‍රී ලංකා සර්ට් ආයතනයේ අනුදැනුම මත තෝරාගනු ලැබූ සුදුසුකම් ලත් වෙනත් පාර්ශවයකගේ සහාය ලබා ගැනීම අවශ්‍ය වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.20. තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂණ ප්‍රතිරෝධය ශක්තිමත් කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂාව දැඩි කිරීමට ඒවා ශක්තිමත් කළ යුතුය (hardening). මෙහෙයුම් පද්ධති, පරිගණක, පරිගණක ජාල සහ ජාල උපාංග, දත්ත ගබඩා සහ තත්‍යසම පෞද්ගලික ජාල යනාදි තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂණ සැකසුම් සක්‍රීය කොට, ඒවායේ ඇති ආරක්ෂණ දුර්වලතා සඳහා විසඳුම් ලබා දී, ඇතිවිය හැකි ප්‍රහාර සඳහා වන ප්‍රවේශ මාර්ග අවහිර කොට එම වත්කම් සයිබර් ප්‍රහාරවලට දක්වන ප්‍රතිරෝධය වැඩි කිරීම සිදුකරනු ලබයි. තොරතුරු තාක්ෂණ වත්කම් ශක්තිමත් කිරීම සඳහා වන උපදෙස් තොරතුරු සහ සයිබර් ආරක්ෂණ මාර්ගෝපදේශයේ දක්වා ඇත.

මෙම තොරතුරු තාක්ෂණ වත්කම් ශක්තිමත් කිරීම සඳහා සුදුසුකම්ලත් පළපුරුදු තොරතුරු ආරක්ෂණ වෘත්තිකයන්ගේ සහාය ලබා ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.21. නිවසේ සිට රාජකාරී කටයුතුවල නිරතවීම් පිළිබඳ ප්‍රතිපත්තිය

නිවසේ සිට (හෝ දුරස්ථව) තොරතුරු තාක්ෂණය භාවිතා කරමින් රාජකාරී ස්ථානවල තොරතුරු තාක්ෂණ වත්කම්වලට ප්‍රවේශ වීමේදී තොරතුරු ආරක්ෂණ තර්ජනවලට ලක්වීමේ සම්භාවිතාවක් පවතී. එබැවින්, කාර්යමණ්ඩල සේවකයින් දුරස්ථව රාජකාරී කටයුතුවල නියැලීමේදී, දැනටමත් රජය විසින් නිකුත් කර ඇති නිවසේ සිට වැඩකිරීමට සම්බන්ධ විධිවිධානවලට අනුකූලව, ශ්‍රී ලංකා සර්ට් ආයතනය විසින් නිකුත්කර ඇති "නිවසේ

සිට වැඩ කිරීම සඳහා වන තොරතුරු ආරක්ෂණ මාර්ගෝපදේශ'' පිළිපැදිය යුතුය.

තවද, තොරතුරු තාක්ෂණ විෂය සම්බන්ධයෙන් කටයුතු කිරීමට අවසරලත් කාර්යමණ්ඩලය ශ්‍රී ලංකා සර්ට් ආයතනය විසින් නිකුත් කර ඇති "පද්ධති පරිපාලකයින් සඳහා නිවසේ සිට වැඩ කිරීමේ මාර්ගෝපදේශය" ට අනුව කටයුතු කළ යුතුය. මෙම මාර්ගෝපදේශයන් ශ්‍රී ලංකා සර්ට් ආයතනයේ www.onlinesafety.lk වෙබ් අඩවියෙන් බාගත කළ හැකිය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.22. රාජකාරී කටයුතු සඳහා තම පෞද්ගලික මෙවලම් භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය සේවකයින්ට නිල රාජකාරී ඉටු කිරීම සඳහා ඔවුන්ගේ පෞද්ගලික ජංගම පරිගණක, ස්මාර්ට් දුරකථන සහ ටැබ්ලට් පරිගණක යනාදී මෙවලම් භාවිතා කිරීමට අවසර ලබා නොදිය යුතුය. කෙසේ වෙතත්, ආයතනයේ තොරතුරු ආරක්ෂණ කමිටුව විසින් තීරණය කරනු ලබන විශේෂිත තත්වයන් යටතේ, තොරතුරු ආරක්ෂණ නිලධාරීගේ අධීක්ෂණය යටතේ නිල රාජකාරී ඉටු කිරීම සඳහා තෝරාගත් සේවකයින්ට ඔවුන්ගේ පුද්ගලික මෙවලම් භාවිතා කිරීමට අවසර දිය හැකිය. එවැනි අවස්ථාවන්හිදී එම මෙවලම් ආයතනය තුළ ක්‍රමවත්ව ලියාපදිංචි කර ඒවා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුගත වන ලෙස ක්‍රියාවේ යෙදවීම අත්‍යවශ්‍ය වේ. එනමුදු, කිසිදු තත්වයක් යටතේ "ඉතා රහසිගත" සහ "රහසිගත" ලෙස වර්ගීකරණය කර ඇති තොරතුරු සැකසීමට හෝ ගබඩා කිරීමට සේවකයින්ගේ පෞද්ගලික මෙවලම් භාවිතා කිරීමට අවසර නොදිය යුතුය.

නිල රාජකාරී ඉටු කිරීම සඳහා සේවකයින්ගේ පෞද්ගලික මෙවලම් භාවිතා කිරීමට අවසර දී ඇතිවිට, ඔවුන්ගේ පරිශීලක ගිණුම් සඳහා සීමිත වරප්‍රසාද ඇති බවටත්, ගිණුම් ශක්තිමත් මුරපද සහ බහු සාධක සත්‍යාපනයෙන් ආරක්ෂා කර ඇති බවටත්, ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කර ඒවායේ ස්වයංක්‍රීය යාවත්කාලීන කිරීම් සක්‍රීය කර ඇති බවටත්, මෙහෙයුම් පද්ධති, උපයෝගිතා මෘදුකාංග සහ භාවිතා කරන අනෙකුත් යෙදුම් මෘදුකාංග වලංගු බලපත් සහිත බවට සහ ඒවා යාවත්කාලීන කර ඇති බවටත් ආයතනය සහතික විය යුතුය.

වෝහාරික පරීක්ෂණයක් සිදු වන අවස්ථාවකදී, රාජකාරී කටයුතු සඳහා භාවිත වන පෞද්ගලික උපාංගවල ඇති පුද්ගලික සහ ආයතනික තොරතුරු විමර්ශනය කිරීමට හෝ පරීක්ෂණ කටයුතු සඳහා එම මෙවලම් රඳවා තබා ගැනීමට සහ නීතිමය අවශ්‍යතා මත රාජ්‍ය ආයතන හෝ පාර්ශවයන් වෙත නිකුත් කිරීමට ආයතනයට අයිතිය ඇත.

සිය පෞද්ගලික මෙවලම්වල ආරක්ෂාව මෙවලම් හිමිකරුගේ වගකීමක් විය යුතුය. උපාංගය භාවිතා කිරීම හේතුවෙන් පෞද්ගලික දත්ත නැතිවීම ඇතුළුව මෙවලම්වලට සිදුවන හානියක් හෝ අස්ථානගත වීමක් සඳහා ආයතනය වගකිව යුතු නොවේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.23. අනාරක්ෂිත ජාල භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ කාර්ය මණ්ඩලය සිය රාජකාරී විද්‍යුත් තැපැල් ගිණුම්වලට හෝ අනෙකුත් කාර්යාලීය තොරතුරු තාක්ෂණ මෘදුකාංග වෙත ප්‍රවේශ වීම සඳහා විශ්වාසදායී නොවන සහ අනාරක්ෂිත වයි-ෆයි ජාල (උදා: ආපනශාලා, හෝටල්, බස් නැවතුම් පොළවල ස්ථාන ගත කර ඇති) හෝ පොදුවේ පරිහරණය කරන පරිගණක, පොදු අන්තර්ජාල සේවා සපයන මධ්‍යස්ථාන සහ වෙනත් එවැනි මෙවලම් භාවිතයෙන් වැළකිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.24. වත්කම් සැපයුම්කරුවන් කළමනාකරණය පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සංවර්ධනය කිරීම සහ කළමනාකරණය කිරීම සඳහා බාහිර පාර්ශ්වයන් (දෘඩාංග, මෘදුකාංග, ජාල, සත්කාරක සහ කළමනාකරණ සේවා ආදිය සපයන්නන්) සම්බන්ධ වන විට සුදුසු ආරක්ෂිත පියවර ආයතනය විසින් ගත යුතුය.

සැපයුම්කරුවන් කළමනාකරණය කිරීමේදී, ආයතනය අවම වශයෙන් පහත සඳහන් කරුණු සැලකිල්ලට ගත යුතුය. එනම් (අ) උපස්ථ, ගබඩා කිරීම, ප්‍රතිසාධනය සහ හදිසි විධිවිධාන, ආරක්ෂක විනාශ කිරීම්, තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ප්‍රවේශවීම ඇතුළු කටයුතු සඳහා ගිවිසුම්ගත පාර්ශවයේ වගකීම් සහ බැඳීම් හඳුනා ගැනීම, (ආ) මෙම ප්‍රතිපත්තියේ අඩංගු කරුණු සහ රජය විසින් හඳුන්වා දී ඇති අනෙකුත් තොරතුරු ආරක්ෂණ ප්‍රමිතීන්ට අනුගතව කටයුතු කිරීම, (ඇ) ගිවිසුමට අදාළ පාර්ශවවල ක්‍රියාවලීන් සහ පාලනයන් විගණනය කිරීමට ආයතනයට ඇති අයිතිය, සහ (ඈ) ගිවිසුම්ගත නියමයන් සහ කොන්දේසිවලට පාර්ශවකරුවන් අනුකූල නොවීම් අධීක්ෂණය සහ වාර්තා කිරීම් ආදිය වේ.

ගිවිසුම්ගත පාර්ශ්වයන් සමඟ ගනුදෙනු කළමනාකරණය කිරීමේ වගකීම ආයතනය ප්‍රධානියා විසින් තීරණය කරන ලද පරිදි තොරතුරු තාක්ෂණ වත්කමෙහි හිමිකරුවන්ට, වෙනත් නම් කරන ලද නිලධාරියෙකුට හෝ ආයතනයකට පැවරිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.25. වෙනස්වීම් කළමනාකරණය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම්වලට අදාළ වන සියලු වෙනස්කම් කළමනාකරණය කළ යුතුය. නිසිලෙස කළමනාකරණය නොකරන ලද වෙනස්කම්, ආයතනයේ තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට අවදානම් ඇති කරන අතරම එහි මෙහෙයුම්වලට ද බාධා ඇති කළ හැකිය. උදාහරණ ලෙස, නිසි පාලනයකින් තොරවූ ස්ථාපනයන් (හෝ අස්ථාපනය කිරීම්), ඇතුළත් කිරීම්, ඉවත් කිරීම් සහ පද්ධති වෙනස් කිරීම්, තොරතුරුවල රහස්‍යභාවය, නිරවද්‍යතාවය සහ උපයෝජ්‍යතාවය වැනි කරුණු කෙරෙහි ඍණාත්මක වශයෙන් බලපෑම් ඇති කළ හැකිය.

තවද, එවන් වෙනස්කම් තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂක දුර්වලතාවයන් ඇති කළ හැකි අතරම, එම වත්කම් අනිසි පුද්ගලයන්ගේ ග්‍රහණයට හසුවීම ද සිදුවිය හැකිය. එබැවින්, තොරතුරු තාක්ෂණ වත්කම් සඳහා වන සමස්ත ආරක්ෂක අවදානම අවම කිරීම සඳහා තොරතුරු ආරක්ෂණ කමිටුව විසින් විධිමත් වෙනස්කම් කළමනාකරණ ක්‍රියාවලියක් ක්‍රියාත්මක කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.4. ආරක්ෂණයට බලපාන සිදුවීම් හඳුනා ගැනීම

ආයතනය විසින් තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම් ක්ෂණිකව හඳුනා ගැනීම සඳහා සුදුසු ක්‍රියාමාර්ග ගත යුතුය. මේ සඳහා, කිසියම් තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීමක්, තොරතුරු තාක්ෂණ වත්කම්වල හඳුනා ගන්නා ලද දුර්වලතා පිළිබඳ, හෝ තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තීන්ට අදාල කරුණු කඩ කිරීමක් පිළිබඳව තොරතුරු ආරක්ෂණය සම්බන්ධයෙන් කටයුතු කරන නිලධාරීන්ට වාර්තා කරන ලෙස ආයතනය විසින් කාර්ය මණ්ඩලයට උපදෙස් ලබා දිය යුතුය. තවද, ආයතනය, තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධීන් හඳුනා ගැනීම සඳහා ලොග් සටහන් විශ්ලේෂණය කිරීම සහ වෙනත් තර්ජන හඳුනාගත හැකි අඛණ්ඩ අධීක්ෂණ විසඳුම් පද්ධතීන් හඳුන්වාදිය යුතු වේ.

තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම් අනාවරණය කර ගැනීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.

4.4.1. ආරක්ෂණ සිදුවීම් වාර්තා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ තොරතුරු සහ සයිබර් ආරක්ෂණය සම්බන්ධයෙන් වන කිසියම් සැක කටයුතු ක්‍රියාකාරකමක් හෝ උල්ලංඝණය කිරීමේ සිදුවීමක් සිදු වූ වහාම එය තොරතුරු ආරක්ෂණ නිලධාරී වෙත වාර්තා කරන ලෙස කාර්ය මණ්ඩලයට පැහැදිලිව උපදෙස් දිය යුතුය. මෙබඳු ආරක්ෂණ කඩකිරීම්වලට උදාහරණ ලෙස, ආයතනයේ පරිගණක ජාලයට, සන්නිවේදන හෝ පරිගණක පද්ධතිවලට අනවසරයෙන් ප්‍රවේශ වීම, පරිගණක පද්ධතිය තුළ යම් වෛරසයක් හඳුනා ගැනීම, ආයතනය මගින් තහනම් කර ඇති කිසියම් අනවසර මෙවලමක් ආයතනය තුළ හඳුනා ගැනීම, අනවසර පරිශීලකයන් විසින් කිසියම් ලිපි ගොනුවක් විකෘති කිරීම සහ වෙනත් පරිශීලකයෙකු හෝ පාර්ශවකරුවකු විසින් මෙම මාර්ගෝපදේශ හෝ ආරක්ෂක ප්‍රතිපත්ති උල්ලංඝනය කිරීම ආදිය දැක්විය හැකිය.

තවද, තොරතුරු තාක්ෂණ වත්කම්වල පවතින යම් යම් දුර්වලතා වාර්තා කරන ලෙස ද පරිශීලකයන් දැනුවත් කළ යුතුය.

තොරතුරු ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම, අනාවරණය කරගත් තොරතුරු ආරක්ෂණ සිදුවීම් වාර්තා කිරීම සහ ඊට අදාළ සාක්ෂි සංරක්ෂණය කිරීම සම්බන්ධයෙන් කාර්ය මණ්ඩලය සඳහා ප්‍රමාණවත් දැනුවත් කිරීම් සහ පුහුණුවක් ආයතනය විසින් ලබා දිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.4.2. ලොග් සටහන් සමාලෝචනය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ සිදුවන ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම සඳහා එහි පරිගණක පද්ධති සහ ආශ්‍රිත වෙනත් මෙවලම් මගින් ජනනය කරන ලද ලොග් සටහන් (ප්‍රවේශ ලොග් සටහන්, දෝෂ ලොග් සටහන්, සේවාදායක පරිගණක ලොග් සටහන්, විගණන ලොග් සටහන්, ගිනිපවුරු ලොග් සටහන් සහ ප්‍රති-අනිෂ්ට මෘදුකාංග ලොග් සටහන් යනාදිය) ආයතනය විසින් මනාව නඩත්තු කරමින් ඒවා සමාලෝචනය කළ යුතුය.

ආයතනයේ පරිගණක පද්ධති වෙත එල්ල වන ද්වේශසහගත ප්‍රහාර හඳුනා ගැනීමට සහ පද්ධතියේ දෝෂ හෝ ආරක්ෂාව කඩවීම් සඳහා හේතු අනාවරණය කර ගැනීමට ද ආයතනය විසින් ලොග් සටහන් සමාලෝචනය කළ යුතුය.

ලොග් සටහන් විකෘති කිරීම් සහ ඒවා වෙත සිදු කරන අනවසර පිවිසුම්වලින් ආරක්ෂා කළ යුතුය. සංවේදී සහ පෞද්ගලිකව හඳුනාගත හැකි තොරතුරු අඩංගු ලොග් සටහන්, ගබඩා කිරීම සහ විශ්ලේෂණය කිරීමට පෙර ඒවායේ රහස්‍යභාවය ආරක්ෂා කිරීම සඳහා සුදුසු පියවර ගත යුතුය.

ලොග් සටහන්, මාස 12ක් හෝ තොරතුරු තාක්ෂණ කමිටුව විසින් තීරණය කරනු ලබන කාල සීමාවක් සඳහා පවත්වාගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.4.3. ආරක්ෂණයට බලපාන සිදුවීම් අඛණ්ඩව අධීක්ෂණය කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය අනිෂ්ට ක්‍රියාකාරකම් හඳුනාගැනීම සඳහා ජාල, පද්ධති හෝ වෙනත් තොරතුරු තාක්ෂණ වත්කම් අධීක්ෂණය කළ යුතු අතර, ඒ සඳහා අනවසර ඇතුළුවීම් හඳුනාගැනීමේ පද්ධතියක් සහ අනවසර ඇතුළුවීම වැළැක්වීමේ පද්ධතියක් (Intrusion Prevention and Detection Systems) ස්ථාපනය කිරීම මගින් එවන් අනිෂ්ට ක්‍රියාකාරකම්වලට එරෙහිව කටයුතු කළ යුතුය.

තවද, ආයතනය සඳහා ආරක්ෂක තොරතුරු සහ සිදුවීම් කළමනාකරණ (Security Information and Event Management) පද්ධති හඳුන්වා දීම තුළින් සයිබර් ආරක්ෂක අධීක්ෂණය සහ තර්ජන හා සිද්ධි හඳුනාගැනීම් සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.4.4. ආරක්ෂණයට බලපාන සිදුවීම් ශ්‍රී ලංකා සර්ට් ආයතනය වෙත වාර්තා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ තොරතුරු ආරක්ෂණ කමිටුව විසින් තීරණය කරුණු ලබන පරිදි,

තීරණාත්මක තොරතුරු ආරක්ෂණ සිදුවීම් ශ්‍රී ලංකා සර්ට් ආයතනයට වාර්තා කර ඒවා කළමනාකරණය කිරීම සඳහා අවශ්‍ය උපදෙස් සහ තාක්ෂණික සහය ලබාගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.5. ආරක්ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම

තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම්වලට වඩා කාර්යක්ෂම ලෙස ප්‍රතිචාර දැක්වීම සඳහා, ආයතනය විසින් ආරක්ෂණ සිද්ධි සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් සකස් කළ යුතු අතර, යම් සිද්ධියකදී එම සැලැස්ම ක්‍රියාත්මක කළ යුතුය. තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම් සඳහා කාර්යක්ෂම ලෙස ප්‍රතිචාර දැක්වීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.

4.5.1. ආරක්ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සඳහා වන ප්‍රතිපත්තිය

ආයතනයේ වත්කම්වලට එරෙහිව ක්‍රියාත්මක වන තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධියක් හඳුනා ගැනීමට, ප්‍රතිචාර දැක්වීමට, එහි අනිටු ප්‍රතිඵල සීමා කිරීමට සහ එම සිදුවීම නිසා හානියට පත් වත්කම් නැවත ඵලදායී ලෙස යථා තත්වයට පත් කිරීමට අවශ්‍ය උපදෙස් සහ ක්‍රියා පටිපාටියකින් සමන්විත සිදුවීම් සඳහා වන ප්‍රතිචාර සැලැස්මක් (Incidents Response Plan) ආයතනය විසින් සකස් කළ යුතුය.

එම සැලැස්මේ අවම වශයෙන්, සිදුවීම් වාර්තා කිරීමේ ක්‍රියා පටිපාටිය, සිදුවීම් හඳුනාගැනීමේ උපාය මාර්ග, සිදුවීම් විශ්ලේෂණ ක්‍රමවේද සහ එම සිදුවීම්වලින් වන බලපෑම සීමා කිරීමේ ක්‍රමවේද සහ හානි වූ වත්කම් ප්‍රතිසාධනය කිරීමට අවශ්‍ය ක්‍රියාකාරකම් අඩංගු විය යුතුය. තවද, විශේෂයෙන්ම, එම සැලැස්ම ක්‍රියාත්මක කිරීම සඳහා අදාළ කාර්ය මණ්ඩල නිලධාරීන් සතු වගකීම් සහ එම සිදුවීම් පසුවිපරම් කිරීම සඳහා අදාළ ක්‍රමවේද ද ඇතුළත් විය යුතුය.

සිද්ධි ප්‍රතිචාර සැලැස්ම ආයතනය තුළ ක්‍රියාත්මක කර එහි ක්‍රියාකාරිත්වය වරින් වර පරීක්ෂා කළ යුතු අතර එම සැලැස්ම සම්බන්ධයෙන් ආයතනයේ සියලුම කාර්ය මණ්ඩල සාමාජිකයින් දැනුවත් කළ යුතුය.

ආරක්ෂණ සිද්ධි සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් නිර්මාණය කිරීම සඳහා වන ක්‍රමවේදය තොරතුරු සහ සයිබර් ආරක්ෂණ මාර්ගෝපදේශයෙහි ඉදිරිපත් කර ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.5.2. ආරක්ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රීය කිරීම සඳහා වන ප්‍රතිපත්තිය

තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීමක දී, ආයතනික මෙහෙයුම්වලට ඇති බලපෑම අවම කිරීම සහ එම මෙහෙයුම් නැවත යථා තත්වයට පත් කිරීම පිණිස, ආයතනයේ බලයලත් නිලධාරියා විසින් සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රීය කළ යුතුය.

ආයතනය විසින් තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් ලේඛනගත කිරීම සඳහා, සිදුවීම් පිළිබඳ ලේඛනයක් (Incidents Register) පවත්වාගෙන යා යුතුය. සිදුවීම් ලේඛනයේ අවම වශයෙන් පහත සඳහන් තොරතුරු පවත්වා ගත යුතුය. ඒවා නම් සිදුවීම වූ දිනය සහ වේලාව, සිදුවීම වාර්තා කළ සේවකයාගේ නම සහ තනතුර, සිදුවීම පිළිබඳ විස්තරය, බලපෑමේ ස්වභාවය, සිදුවීමෙහි වර්ගීකරණය, සිදුවීමට ප්‍රතිචාර වශයෙන් ගන්නා ලද ක්‍රියාමාර්ග, සිදුවීම භාරව කටයුතු කරන නිලධාරියා, සිදුවීමේ වත්මන් තත්වය යනාදිය වේ.

යම් සිදුවීමක් සඳහා ප්‍රතිචාර දැක්වීම සඳහා ආයතනය ගතයුතු ක්‍රියාමාර්ග තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශයෙහි දක්වා ඇත. ආයතනය විසින් තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීමකදී, විධිමත් චෝභාරික පරීක්ෂණයක් සිදු කිරීමට අවශ්‍ය සාක්ෂි ලෙස භාවිතා කළ හැකි තොරතුරු හඳුනා ගැනීම, රැස් කිරීම සහ සංරක්ෂණය කිරීම සඳහා සුදුසු ක්‍රමවේදයක් භාවිතා කළ යුතුය. චෝභාරික පරීක්ෂණය සිදු කළ යුතු ආකාරය දැක්වෙන ප්‍රතිපත්ති අංක 4.5.3 යටතේ ඉදිරිපත් කර ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ

4.5.3. චෝභාරික පරීක්ෂණ පිළිබඳ ප්‍රතිපත්තිය

චෝභාරික පරීක්ෂණයක් ආයතනය තුළ සිදු කිරීමට අවශ්‍ය වූ විට, ඒ සඳහා විධිමත් ක්‍රියාවලියක් අනුගමනය කළ යුතුය. මෙවන් පරීක්ෂණ සඳහා අවශ්‍ය සාක්ෂි භෞතික ලේඛන, දෘඩ තැටිවල දත්ත, මෙවලම් ලොග්-සටහන්, ආරක්ෂිත කැමරා දර්ශන, විද්‍යුත් තැපැල් පණිවුඩ, හඬපට සහ වෙනත් විද්‍යුත් ලේඛන ආදියෙන් ලබා ගත හැකිය.

ඉලෙක්ට්‍රොනික සාක්ෂි භෞතික ස්වභාවයෙන් නොපැවතීම, පිටපත් කිරීමේ හැකියාව සහ ඒවායේ නෂ්‍යතාවය (volatility) සම්බන්ධයෙන් ගත්විට ඒවා සම්ප්‍රදායික චෝභාරික සාක්ෂිවලට වඩා වෙනස් වන බැවින්, එවැනි සාක්ෂි විශ්ලේෂණය කිරීම සඳහා විශේෂඥ දැනුමක් අත්‍යවශ්‍ය වේ. ආයතනය එවැනි සාක්ෂි විශ්ලේෂණය කිරීම සඳහා ශ්‍රී ලංකා සර්ට් ආයතනය හෝ අදාළ තාක්ෂණික හැකියාවන් සහිත ආයතනයක් මගින් තාක්ෂණික සහාය ලබා ගත යුතුය.

ආයතනය විසින් සිදු කරන චෝභාරික පරීක්ෂණයකදී, සාක්ෂිවල භාරකාර දාමය (chain of custody) පවත්වාගෙන යෑම සඳහා අවම වශයෙන් පහත සඳහන් තොරතුරු ලේඛන ගත කළ යුතුය. ඒවා නම්, සිද්ධිය සහ ඊට අදාළ සාක්ෂි පිළිබඳ විස්තර, සාක්ෂි එකතු කරන ලද දිනය සහ වේලාව, සාක්ෂි ලබාදුන් නිලධාරියාගේ නම සහ තනතුර සහ සාක්ෂි එක් එක් නිලධාරීන්ගේ (හෝ ආයතනවල) භාරකාරීත්වයට පත් වූ අයුරු ආදිය වේ. යම් විමර්ශනයකදී ඉදිරිපත් කළ යුතු භාරකාර දාමය නිසි පරිදි පවත්වාගෙන යාම ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරීගේ වගකීමක් වේ.

දැනට ගෙන ඇති සහ ඉදිරියට ගැනීමට අපේක්ෂිත ක්‍රියාමාර්ග සම්බන්ධයෙන් අවශ්‍ය විය හැකි සියලු සාක්ෂි රඳවා තබා ගැනීමේ සහ සංරක්ෂණය කිරීමේ වගකීම ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරී සතු වේ. සාක්ෂි ලෙස භාවිතා කළ හැකි ලේඛන, ඉලෙක්ට්‍රොනික මාධ්‍යයෙන් ඇති තොරතුරු හෝ ඒවා අඩංගු මෙවලම් නැතිවීම, විනාශ කිරීම හෝ චේතනාත්මකව වෙනස් කිරීම ආදියෙන් වැළක්වීමේ වගකීම් ද මෙයට ඇතුළත් වේ.

චෝභාරික පරීක්ෂණ ක්‍රියාත්මක කිරීමේදී, පෞද්ගලික දත්ත ආරක්ෂණය, පරිගණක අපරාධ, ගෙවීම් මෙවලම් වංචා සහ විද්‍යුත් ගනුදෙනු සම්බන්ධව පවතින නීති හෝ වෙනත් අදාළ නීතිමය රාමුවලට යටත්ව සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.6. මෙහෙයුම් ප්‍රතිසාධනය කිරීම

ආපදාවක් හේතුවෙන් හානියට හෝ බිඳ වැටීමකට ලක් වූ ඕනෑම සේවාවක් ප්‍රතිෂ්ඨාපනය කිරීම සඳහා ඵලදායී ක්‍රියාකාරී සැලැස්මක් ආයතනය විසින් සකස් කර ක්‍රියාවට නැංවිය යුතුය.

තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීමකින් පසුව ආයතනයේ මෙහෙයුම් යථා තත්වයට පත් කිරීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.

4.6.1. ආපදා ප්‍රතිසාධන සැලැස්ම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක් සතුව යම් ආපදාවකදී (හෝ සිදුවීමකදී), බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කිරීම සඳහා සකස් කරන ලද ආපදා ප්‍රතිසාධන සැලැස්මක් (Disaster Recovery Plan) තිබිය යුතුය.

එවන් සැලැස්මක, එම ආපදා අවස්ථාවේදී බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් නැවත යථා තත්වයට පත් කිරීම සඳහා කළ යුතු ක්‍රියාකාරකම් ද එක් එක් නිලධාරියාට අදාළ භූමිකාවන් සහ වගකීම් ද අඩංගු විය යුතුය.

ආපදා ප්‍රතිසාධන සැලැස්මක් සකස් කිරීමේදී, වත්කම් සඳහා වන අවදානම් තක්සේරුවක් සහ හානි පිළිබඳ විශ්ලේෂණයක් සිදු කොට එවන් හානියකදී බිඳ වැටුණු (හෝ අඩපණ වූ) දත්ත ප්‍රතිසාධනට ගත යුතු අවම කාලය සහ වත්කම් ප්‍රතිසාධනය කර මෙහෙයුම් නැවත ආරම්භ කිරීමට ගත යුතු අවම කාලය සලකා බැලිය යුතුය. ආයතනය එහි ආපදා ප්‍රතිසාධන සැලැස්මේ ක්‍රියාකාරීත්වය වරින් වර පරීක්ෂා කර යාවත්කාලීන කිරීම කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.6.2. ආපදා ප්‍රතිසාධන සැලැස්ම සක්‍රීය කිරීම පිළිබඳ ප්‍රතිපත්තිය

යම් ආපදාවකදී, අදාළ බලයලත් නිලධාරියා විසින් ආයතනයේ බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කර ආයතනයේ මෙහෙයුම් නැවත ක්‍රියාත්මක කිරීමට ආපදා ප්‍රතිසාධන සැලැස්ම ක්‍රියාත්මක කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.6.3. තීරණාත්මක ආපදා හෝ සිදුවීම් සන්නිවේදනය පිළිබඳ ප්‍රතිපත්තිය

සංකීර්ණ ආපදාවකදී හෝ ආරක්ෂණයට බලපාන සිදුවීමකදී (උදාහරණ ලෙස තීරණාත්මක ආපදාවක්, සයිබර් ප්‍රහාරයක් නිසා ඇතිවූ සිදුවීමකදී වැනි) ආයතන ප්‍රධානියා විසින් තීරණය කරන පරිදි අදාළ රේඛීය අමාත්‍යාංශය, ශ්‍රී ලංකා සර්ට් ආයතනය, සිදුවීමට අදාළ වින්දිතයන්, ජනමාධ්‍යයන්, සේවාදායකයින් සහ නීතිය ක්‍රියාත්මක කරන බලධාරීන් වැනි අභ්‍යන්තර සහ බාහිර පාර්ශ්ව සමඟ සැලැස්මකට අනුව සුදුසු ලෙස එම අර්බුදය පිළිබඳව සන්නිවේදනය කළ යුතුය. අර්බුදය අදාළ පාර්ශ්වකරුවන් වෙත සන්නිවේදනය කිරීම සඳහා ආයතනය විසින් එහි ජ්‍යෙෂ්ඨ මට්ටමේ වගකිව යුතු නිලධාරියෙකු පත් කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

5. ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු

තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ආයතනය තුළ ක්‍රියාත්මක කිරීම සඳහා පහත දැක්වෙන ප්‍රතිපත්තිමය කරුණු ප්‍රමුඛතා මට්ටමින් ක්‍රියාත්මක කළ යුතු වේ.

ප්‍රතිපත්ති අංශය	**ප්‍රතිපත්ති අංකය**	**ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු**	**සියලුම ආයතන**	***කී. ජා. තො. ය. ප. පවතින ආයතන**
තොරතුරු සහ සයිබර් ආරක්ෂණ පාලනය	4.1.1	තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සඳහා ආයතන ප්‍රධානියා විසින් නායකත්වය සැපයීම.	✓	✓
	4.1.2	තොරතුරු හා සයිබර් ආරක්ෂණ ආයතනික ව්‍යුහයක් ස්ථාපන කිරීම.	✓	✓
	4.1.2 (අ)	තොරතුරු ආරක්ෂණ නිළධාරියකු පත්කර තොරතුරු හා සයිබර් ආරක්ෂණ වගකීම් පැවරීම.		✓
	4.1.2 (ආ)	තොරතුරු ආරක්ෂණ නිළධාරියකු නොමැති අවස්ථාවක දී, ප්‍රධාන නව්‍යකරණ නිලධාරියා වෙත තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට වගකීම් පැවරීම.	✓	
	4.1.2 (ඇ)	තොරතුරු හා සයිබර් ආරක්ෂණ විගණන සම්බන්ධයෙන් කටයුතු කිරීම සඳහා (ප්‍රධාන) අභ්‍යන්තර විගණක වෙත වගකීම් පැවරීම.	✓	✓

	4.1.3	තොරතුරු ආරක්ෂණ කමිටුවක් පත්කිරීම.	✓	✓
	4.1.4	අවදානම් කළමනාකරණ කමිටුවක් පත්කිරීම.		✓
	4.1.5	පරිශීලකයන්ගේ වගකීම් හඳුනාගෙන ඒවා ප්‍රකාශයට පත්කිරීම.	✓	✓
	4.1.6	තොරතුරු හා සයිබර් ආරක්ෂණය සම්බන්ධයෙන් වගකිව යුතු නිලධාරීන්ගේ ධාරිතා සංවර්ධනය කිරීම.	✓	✓
	4.1.7	රහසිගත හෝ ඉතා රහසිගත ලෙස වර්ගීකරණය කර ඇති තොරතුරු හෝ තීරණාත්මක ජාතික යටිතල පහසුකම් භාවිතා කරන කාර්යමණ්ඩලයේ ආරක්ෂණ නිෂ්කාශන සහ පසුබිම් පරීක්ෂාවක් කිරීම.		✓
	4.1.8	තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරකම් එහි ආයතනික දැක්ම, මෙහෙවර සහ අරමුණු සමඟ පෙළ ගැස්වීම.	✓	✓
	4.1.9	තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරී සැලසුම් සකස්කර ක්‍රියාත්මක කිරීම.	✓	✓
වත්කම්, හිමිකරුවන් සහ අවදානම් හඳුනා ගැනීම	4.2.1	තොරතුරු, තොරතුරු තාක්ෂණ වත්කම් හා තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම.	✓	✓
	4.2.3	වත්කම් හිමිකරුවන් සහ භාරකරුවන් හඳුනා ගෙන ඔවුන්ට ඒවා ආරක්ෂා කිරීමට වගකීම් පැවරීම.	✓	✓
	4.2.4	තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් රෙජිස්තර පවත්වාගෙන යාම.	✓	✓
	4.2.5	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සඳහා අවදානම් තක්සේරු කිරීම.		✓
	4.2.6	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් ඒවායේ වටිනාමක සහ සංවේදීතාවය මත වර්ගීකරණය කිරීම.	✓	✓

වත්කම් ආරක්ෂා කිරීම	4.3.1	නිශ්චලව පවතින දත්ත ආරක්ෂා කිරීම.	✓	✓
	4.3.2	සංචරණය වන දත්ත ආරක්ෂා කිරීම.	✓	✓
	4.3.3	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සඳහා වන භෞතික ආරක්ෂාව සහතික කිරීම.	✓	✓
	4.3.4	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ඇති පරිශීලක ප්‍රවේශ පාලනය කිරීම.	✓	✓
	4.3.5	ශක්තිමත් සත්‍යාපනයන් සහතික කිරීම.	✓	✓
	4.3.6	දත්තවල ස්වෛරීභාවය සුදුසු පරිදි සහතික කිරීම.	✓	✓
	4.3.7	වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතා කර ඒවායේ සරිමා යාවත්කාලීන කිරීම.	✓	✓
	4.3.8	ප්‍රති-අනිෂ්ට මෘදුකාංග භාවිතා කිරීම.	✓	✓
	4.3.9	නිල සන්නිවේදන කටයුතු සඳහා නිල විද්‍යුත් තැපැල් භාවිතා කිරීම.	✓	✓
	4.3.10	විද්‍යුත් තැපැල් වල ආරක්ෂාව සහතික කිරීම.	✓	✓
	4.3.11	සුදුසු පරිදි ඩිජිටල් අත්සන් භාවිතා කිරීම.	✓	✓
	4.3.12	පරිමිති ආරක්ෂණ පාලනයන් සිදු කිරීම.	✓	✓
	4.3.13	ආරක්ෂිත දුරස්ථ ප්‍රවේශය ක්‍රමවේද භාවිතා කිරීම.	✓	✓

	4.3.14	උපස්ථ සඳහා උපාය මාර්ගයක් භාවිතා කිරීම.	✓	✓
	4.3.16	ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය හා භාවිතය සහතික කිරීම.	✓	✓
	4.3.17	වත්කම් සුරක්ෂිතව බැහැර කිරීම.	✓	✓
	4.3.18	අභ්‍යන්තර තොරතුරු ආරක්ෂණ විගණන ක්‍රියාවලියක් පවත්වාගෙන යාම.	✓	✓
	4.3.19	ඕනෑම වෙබ් අඩවියක්, වෙබ් යෙදුමක් හෝ පද්ධතියක් නිල වශයෙන් දියත් කිරීමට පෙර අවදානම් තක්සේරු කිරීම් සහ විනිවිද යාමේ පරීක්ෂණ සිදු කිරීම.	✓	✓
	4.3.20	තොරතුරු තාක්ෂණ වත්කම් වල ආරක්ෂණ ප්‍රතිරෝධය ශක්තිමත් කිරීම.	✓	✓
	4.3.21	නිවසේ සිට රාජකාරී කටයුතු වල නිරතවීම සඳහා වන ආරක්ෂණ මාර්ගෝපදේශ අනුගමනය කිරීම.	✓	✓
	4.3.23	අනාරක්ෂිත ජාල භාවිතයෙන් වැළකිය සිටීම	✓	✓
	4.3.24	සැපයුම්කරුවන් කළමනාකරණය කිරීම.	✓	✓
	4.3.25	වෙනස් වීම් කළමනාකරණය කිරීම.	✓	✓
ආරක්ෂණයට බලපාන තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම	4.4.1	ආරක්ෂණ සිදුවීම වාර්තා කරන ලෙස කාර්ය මණ්ඩලයට උපදෙස් ලබාදීම.	✓	✓
	4.4.2	ආරක්ෂණයට බලපාන සිදුවීම් හඳුනා ගැනීම සඳහා ලොග් සටහන් සමාලෝචනය කිරීම.	✓	✓
	4.4.3	ආරක්ෂණයට බලපාන සිදුවීම් අඛණ්ඩව අධීක්ෂණය කරමින් සිදුවීම් හඳුනා ගැනීම.		✓

	4.4.4	ආරක්ෂණයට බලපාන සිදුවීම් ශ්‍රී ලංකා සර්ට් ආයතනය වෙත වාර්තා කිරීම.	✓	✓
ආරක්ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම	4.5.1	සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් සකස් කිරීම.	✓	✓
	4.5.2	සිදුවීමකදී, සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම ක්‍රියාත්මක කිරීම.	✓	✓
	4.5.3	ආරක්ෂණ සිදුවීම් සඳහා වෝහාරික පරීක්ෂණ සිදු කිරීම.	✓	✓
මෙහෙයුම් ප්‍රතිසාධනය කිරීම	4.6.1	අපදා ප්‍රතිසාධනය සැලැස්මක් නිර්මාණය කිරීම.	✓	✓
	4.6.2	අපදා අවස්ථාවකදී අපදා ප්‍රතිසාධනය සැලැස්ම ක්‍රියාත්මක කිරීම.	✓	✓
	4.6.3	තීරණාත්මක ආපදාවක් හෝ සිදුවීමක් සන්නිවේදනය කිරීම සඳහා සැලැස්මක් නිර්මාණය කිරීම.	✓	✓

* ***කී. ජා. තො. ය. ප. පවතින ආයතන:*** *තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් **පවතින** ආයතන*

6. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය අධීක්ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදය

6.1 තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාවට නැංවීමට පෙර ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ සූදානම හඳුනා ගැනීම සඳහා සහ ප්‍රතිපත්තිය ක්‍රියාත්මක කරමින් තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට රාජ්‍ය ආයතන ගෙන ඇති ක්‍රියාමාර්ගවල කාර්යසාධනය අධීක්ෂණය සහ ඇගයීම සඳහා ක්‍රමවේදයක් නිර්මාණය කර ඇත.

6.2 ඒ අනුව ශ්‍රී ලංකා සර්ට් ආයතනය අංක 6.6 හි දක්වා ඇති ප්‍රශ්නාවලියෙහි අඩංගු කරුණු පදනම් කර ගනිමින් ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ සූදානම පිළිබඳ මූලික තක්සේරුවක් ලබා ගන්නා අතර එම තක්සේරුව පදනම් කර ගනිමින් එම ආයතන වල මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය මග පෙන්වීම ලබා දෙනු ඇත.

6.3 ශ්‍රී ලංකා සර්ට් ආයතනය වාර්ෂිකව ආයතනවල තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ කාර්ය සාධනය ඇගයීමට ලක් කරනු ලබන අතර එක් එක් ආයතනය ප්‍රතිපත්තියට අනුගත වී ඇති අයුරු තොරතුරු සහ සයිබර් ආරක්ෂණ දර්ශකයක (Information and Cyber Security Index) ඉදිරිපත් කරනු ඇත. තවද මෙම ඇගයීමේ ප්‍රතිඵල මත පදනම්ව ආයතනයේ සමස්ත තොරතුරු සහ සයිබර් ආරක්ෂණ සූදානම වැඩිදියුණු කිරීමට අවශ්‍ය නිර්දේශ ශ්‍රී ලංකා සර්ට් ආයතනය විසින් ඉදිරිපත් කරනු ඇත.

6.4 ආයතනවල තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ කාර්ය සාධනය හෝ සූදානම ඇගයීමට මෙම ලේඛනයේ අංක 6.6 පරිච්ඡේදයේ සඳහන්ව ඇති ප්‍රශ්න 50 කට ආසන්න සංඛ්‍යාවකින් යුත් ප්‍රශ්නාවලිය භාවිතා කළ යුතු අතර ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරියා, ප්‍රධාන නවීකරණ නිලධාරියා, හෝ තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියා විසින් මෙම ප්‍රශ්නාවලිය සම්පූර්ණ කළ යුතු අතර, එය සෑම වසරකම ඔක්තෝබර් 30 වැනි දිනට හෝ ඊට පෙර ආයතන ප්‍රධානියාගේ අත්සන සහිතව ශ්‍රී ලංකා සර්ට් ආයතනය වෙත යොමු කළ යුතුය.

6.5 පිළිතුරු සපයන නිලධාරියා විසින් අදාළ ප්‍රශ්න සඳහා විස්තරාත්මක ප්‍රතිචාරයක් සැපයීමට අවශ්‍ය විටදී, ඒ සඳහා ප්‍රශ්නාවලිය අවසානයේ ඇති සටහන් තීරුවේ (Remarks) විස්තර සැපයිය හැකිය. තවද, මෙම ප්‍රශ්නාවලියේ භාවිතා වී ඇති පදමාලාව පිළිබඳ පැහැදිලි කිරීම් සඳහා මෙම ප්‍රතිපත්තියේ සඳහන්ව ඇති අර්ථ දැක්වීම (Definitions) භාවිතා කළ හැක.

6.6 ඇගැයීමේ ප්‍රශ්නාවලිය

සියලුම රාජ්‍ය ආයතන සිය දැනුවත්භාවය මත සෑම ප්‍රශ්නයකටම ඔවුන්ගේ ප්‍රතිචාරය දැක්වීම ට අවශ්‍ය වේ.

ප්‍රතිපත්ති යොමුව	**තක්සේරු නිර්ණායක**	**ප්‍රතිපත්ති අංකය**	**ආයතනය අනුගතද?**		**සටහන්**
			ඔව්	**නැත**	
තොරතුරු සහ සයිබර් ආරක්ෂණ පාලනය					
ආරක්ෂණ ආයතනික ව්‍යුහය	1. ආයතනය සඳහා තොරතුරු ආරක්ෂණ නිලධාරියෙකු පත් කර තිබේද?	4.1.2(අ)			
	2. ආයතනය සිය තොරතුරු ආරක්ෂණ නිලධාරියා වෙත තොරතුරු හා සයිබර් ආරක්ෂණ වගකීම් පවරා තිබේද?	4.1.2(අ)			
	3. තොරතුරු ආරක්ෂණ නිලධාරියකු පත් කර නොමැති නම්, ප්‍රධාන නව්‍යකරණ නිලධාරී හෝ තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියාට තොරතුරු ආරක්ෂණ වගකීම් පවරා තිබේද?	4.1.2(ආ)			
	4. ආයතනය සිය (ප්‍රධාන) අභ්‍යන්තර විගණන නිලධාරී වෙත තොරතුරු හා සයිබර් ආරක්ෂණ විගණන වගකීම් පවරා දී තිබේද?	4.1.2(ඇ)			
	5. තොරතුරු හා සයිබර් ආරක්ෂාව පිළිබඳ තීරණ ගැනීමට ආයතනයේ කමිටුවක් පිහිටුවා තිබේද?	4.1.3			
	6. ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ අවදානම් සම්බන්ධයෙන් තීරණ ගැනීම සඳහා අවදානම් කළමනාකරණ කමිටුවක් පිහිටුවා තිබේද?	4.1.4			
පරිශීලකයි-න්ගේ වගකීම්	7. තොරතුරු හා සයිබර් ආරක්ෂාව සම්බන්ධයෙන් වන වගකීම් ඔබ ආයතනයේ කාර්ය මණ්ඩලයට පැහැදිලි කොට දී තිබේද?	4.1.5			
ධාරිතා සංවර්ධනය	8. තොරතුරු හා සයිබර් ආරක්ෂණය සම්බන්ධ වගකීම් දරන නිලධාරීන්ගේ තොරතුරු ආරක්ෂණ හැකියාව වර්ධනය කිරීම සඳහා පුහුණු හා දැනුවත්කිරීම් කර තිබේද?	4.1.6			
පසුබිම් පරීක්ෂාව	9. ඔබේ ආයතනය "ඉතා රහසිගත" හෝ "රහසිගත", තොරතුරු වත්කම් හෝ තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සහිත පද්ධති සම්බන්ධයෙන් කටයුතු කරන නිලධාරීන්ගේ පසුබිම් පරීක්ෂණ සහ ආරක්ෂක නිෂ්කාශන සිදු කර තිබේද?	4.1.7			
උපායමාර්ගික පෙළගැස්වීම	10. ආයතනයේ කාර්යයන්, ප්‍රතිපත්ති, උපාය මාර්ග හෝ ව්‍යාපෘති සැලසුම් කිරීමේදී සහ ක්‍රියාත්මක කිරීමේදී, තොරතුරු හා සයිබර් ආරක්ෂාව සැලකිල්ලට ගෙන තිබේද?	4.1.8			

ක්‍රියාකාරී සැලසුම	11. තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරකම් සඳහා ආයතනය මූල්‍ය ප්‍රතිපාදන වෙන් කර තිබේද?	4.1.9			
	12. ආයතනය එහි තොරතුරු හා සයිබර් ආරක්ෂණ අරමුණු සාක්ෂාත් කර ගැනීම සඳහා වන ව්‍යාපෘති ක්‍රියාකාරී සැලසුම්වලට ඇතුළත් කර තිබේද?	4.1.9			
වත්කම්, භිමිකරුවන්, පරිශීලකයන් සහ අවදානම් හඳුනා ගැනීම					
වත්කම් හඳුනා ගැනීම	13. ආයතනය සතු වටිනාකමක් ඇති තොරතුරු වත්කම් හඳුනාගෙන තිබේද?	4.2.1			
	14. ආයතනය සතු තොරතුරු වත්කම් හා සම්බන්ධ අවදානම තක්සේරු කර තිබේද?	4.2.5			
	15. ආයතනයේ තොරතුරු වත්කම්වල සංවේදීතාව හෝ වෙනත් ක්‍රමවේදයක් මත පදනම්ව තොරතුරු වත්කම් වර්ගීකරණය (classification of information assets) කර තිබේද?	4.2.6			
	16. ආයතනය තොරතුරු වත්කම් (information assets) ලේඛනයක සටහන්කර තිබේද?	4.2.4			
	17. ආයතනය තොරතුරු තාක්ෂණ වත්කම් (IT assets) හඳුනාගෙන තිබේද?	4.2.1			
	18. ආයතනය තොරතුරු තාක්ෂණ වත්කම්, ලේඛනයක ලේඛනගත කර තිබේද?	4.2.4			
	19. ආයතනය තොරතුරු තාක්ෂණ වත්කම් ඒවායේ තීරණාත්මකභාවය (criticality) මත වර්ගීකරණය කර තිබේද?	4.2.6			
	20. ආයතනයේ වත්කම්වල හිමිකරුවන් හඳුනාගෙන තිබේද?	4.2.3			
වත්කම් ආරක්ෂා කිරීම					
දත්ත කේතනය	21. ගබඩා කිරීමට පෙර ආයතනයේ සංවේදී තොරතුරු කේතනය (encrypt) කෙරේද?	4.3.1			
	22. ආයතනයේ සංවේදී තොරතුරු පරිගණක ජාල සහ වෙනත් වැනලයන් හරහා ගමන් කිරීමට පෙර කේතනය කෙරේද?	4.3.2			
භෞතික ආරක්ෂාව	23. ආයතනයේ සංවේදී තොරතුරු සකසන්නේ හෝ ගබඩා කරන්නේ භෞතික වශයෙන් ආරක්ෂිත ස්ථානවල ද?	4.3.3			
	24. ගිනි ගැනීම්, ජල ගැලීම්, ආර්ද්‍රතාව වෙනස් වීම් සහ උෂ්ණත්ව වෙනස් වීම් වැනි තත්වයන්ගෙන් ආයතනයේ ආරක්ෂිත ස්ථාන ආරක්ෂා කිරීමට සුදුසු පියවර ගෙන තිබේද?	4.3.3			

	25. ආයතනයේ ආරක්ෂිත ස්ථානවලට අනවසර ඇතුළුවීම් වැලැක්වීමට ක්‍රමවේද සකසා තිබේද?	4.3.3			
අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය	26. ආයතනයේ අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයක් (Identity Management and Access Control) තිබේද?	4.3.4			
	27. ආයතනයේ ශක්තිමත් සත්‍යාපන (strong authentication) ක්‍රමවේද භාවිතා කරන්නේද?	4.3.5			
දත්ත ස්වෛරීභාවය	28. ආයතනය සිය දත්ත වල ස්වෛරීභාවය (Data Sovereignty) සැලකිල්ලට ගෙන තිබේද?	4.3.6			
	29. මේඝගත සේවා ලබා ගැනීමට පෙර ආයතනය එහි අවදානම සැලකිල්ලට ගෙන තිබේද?	4.3.6			
වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතය සහ සරිමා යාවත්කාලීන කිරීම	30. ආයතනය වලංගු බලපත්‍ර සහිත පරිගණක මෙහෙයුම් පද්ධති පමණක් භාවිතා කරන්නේද?	4.3.7			
	31. ආයතනයේ පරිගණක මෙහෙයුම් පද්ධති සැපයුම්කරු විසින් සපයන ලද නවතම සරිමා මගින් යාවත්කාලීන කර තිබේද?	4.3.7			
	32. සැපයුම්කරු විසින් සපයන ලද තීරණාත්මක සරිමා ස්ථාපනය කිරීමට පෙර නිසි ඇගයීමකට භාජනය කරන්නේද?	4.3.7			
ප්‍රති අනිෂ්ට මෘදුකාංග	33. ආයතනය සියලුම පරිගණක සහ අදාළ උපාංගවල වලංගු බලපත්‍රයක් සහිත ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කර තිබේද?	4.3.8			
විද්‍යුත් තැපැල්	34. ආයතනයේ නිල සන්නිවේදන කටයුතු සඳහා පුද්ගලික විද්‍යුත් තැපැල් භාවිතය වැලැක්වීමට අවශ්‍ය ක්‍රියාමාර්ගයන් ගෙන තිබේද?	4.3.9			
	35. විද්‍යුත් තැපැල් ලිපිවල අමුණා ඇති අනිෂ්ට මෘදුකාංග හඳුනා ගෙන ඒවා ඉවත් කිරීමට ආයතනයේ විද්‍යුත් තැපැල් පෙරහන් සක්‍රීය කොට තිබේද ?	4.3.10			
	36. ආයතනය විද්‍යුත් තැපැල මගින් සංවේදී තොරතුරු හුවමාරු කරන විට කේතනය භාවිතා කරයිද?	4.3.10			
පරිමිති ආරක්ෂණ පාලනයන්	37. ආයතනයේ ගිනිපවුරක් ස්ථාපනය කර තිබේද?	4.3.12			
ආරක්ෂිත දුරස්ථ ප්‍රවේශය	38. ආයතනය දුරස්ථ ප්‍රවේශය සඳහා ආරක්ෂිත තත්‍යසම පුද්ගලික ජාල (virtual private networks) භාවිතා කරන්නේද?	4.3.13			

	39. ආයතනයේ දුරස්ථව සම්බන්ධ වන සියලුම පරිශීලකයින් ආරක්ෂිත තත්‍යසම පුද්ගලික ජාල භාවිතා කරන්නේද?	4.3.13			
උපස්ථ උපාය මාර්ග	40. ආයතනය දත්ත උපස්ථ (backup) කරන්නේද?	4.3.14			
	41. ආයතනය සිය උපස්ථ ගබඩා කර ඇත්තේ දත්ත සැකසුම් ස්ථානයෙන් භෞතිකව දුරස්ථ, ගිනිගැනීම් ආදියෙන් ආරක්ෂිත ස්ථානයකද?	4.3.14			
වත්කම් සුරක්ෂිතව බැහැර කිරීම	42. සංවේදී තොරතුරු අඩංගු දත්ත ගබඩා මාධ්‍ය බැහැර කිරීමට ඔබ ආයතනය පහත සඳහන් කිසිවක් අනුගමනය කරන්නේද? (ඉරා දැමීම, සිදුරු කිරීම, භෞතිකව හානි කිරීම යනාදිය)	4.3.17			
අභ්‍යන්තර තොරතුරු ආරක්ෂණ විගණන වැඩසටහන	43. ආයතනය සතුව අභ්‍යන්තර තොරතුරු හා සයිබර් ආරක්ෂණ විගණන වැඩසටහනක් තිබේද?	4.3.18			
	44. ආයතනය ඕනෑම වෙබ් අඩවියක්, වෙබ් යෙදුමක් හෝ පද්ධතියක් නිල වශයෙන් දියත් කිරීමට පෙර ශ්‍රී ලංකා සර්ට් ආයතනය මගින් අවදානම් තක්සේරු කිරීම සහ විනිවිදයාමේ පරීක්ෂණ සිදු කරන්නේද?	4.3.19			
	45. ආයතනයේ පරිගණක ජාල සඳහා අවදානම් තක්සේරු කිරීම සහ විනිවිදයාමේ පරීක්ෂණ සිදු කර තිබේද?	4.3.19			
නිවසේ සිට රාජකාරී කටයුතුවල නියතවීම	46. රජය විසින් නිකුත්කරන ලද උපදෙස්වලට අනුකූලව ශ්‍රී ලංකා සර්ට් ආයතනය විසින් නිකුත් කරන ලද නිවසේ සිට වැඩ කිරීම සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශ ඔබ ආයතනය පිළිපදින්නේද?	4.3.21			
රාජකාරී කටයුතු සඳහා තම පෞද්ගලික මෙවලම් භාවිතය	47. රාජකාරී කටයුතු සඳහා පෞද්ගලික මෙවලම් භාවිතා කිරීමට පෙර ඒවා ලියාපදිංචි කිරීමට ආයතනය විධිමත් ක්‍රියා පටිපාටියක් අනුගමනය කරන්නේද?	4.3.22			
	48. ආයතනය රාජකාරී කටයුතු සඳහා පෞද්ගලික මෙවලම් භාවිතා කරන විට, ඒවායේ සංවේදී දත්ත සැකසීමට හෝ ගබඩා කිරීමට ඉඩ දෙන්නේද?	4.3.22			
තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම					
ආරක්ෂණ සිදුවීම් වාර්තා කිරීම	49. තොරතුරු සහ සයිබර් ආරක්ෂණය සම්බන්ධයෙන් කිසියම් සැක කටයුතු ක්‍රියාකාරකමක්, සම්බන්ධතාවක්, සොරකමක්, වෛරසයක්, අවදානමක්, අනවසර ප්‍රවේශයක්, ලිපිගොනු විකෘති කිරීම හෝ මෙම ප්‍රතිපත්තිය උල්ලංඝණය කිරීමක් ආයතනයේ තොරතුරු ආරක්ෂාව	4.4.1			

	භාර නිලධාරියට වාර්තා කරන ලෙස කාර්ය මණ්ඩලයට උපදෙස් දී තිබේද?				
	50. ආයතනය තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් ශ්‍රී ලංකා සර්ට් ආයතනය වෙත හෝ වෙනත් අදාල ආයතනයකට වාර්තා කර තිබේද?	4.4.4			
ආරක්ෂණ සිදුවීම්වලට ප්‍රතිචාර දැක්වීම					
ආරක්ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සහ එය ක්‍රියාත්මක කිරීම	51. ආරක්ෂණයට අහිතකර ලෙස බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් (Incidents Response Plan) තිබේද?	4.5.1			
	52. තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීමක දී, ආයතනය සිය මෙහෙයුම්වලට ඇති බලපෑම අවම කිරීම සහ එම මෙහෙයුම් නැවත යථා තත්වයට පත් කිරීම පිණිස, සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රීය කරන්නේද?	4.5.2			
මෙහෙයුම් යථා තත්වයට පත් කිරීම					
ආපදා ප්‍රතිසාධන සැලැස්ම සහ එය ක්‍රියාත්මක කිරීම	53. යම් ආපදාවකදී (හෝ සිදුවීමකදී), බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කිරීම සඳහා සකස් කරන ලද ආපදා ප්‍රතිසාධන සැලැස්මක් (Disaster Recovery Plan) ආයතනයට තිබේද?	4.6.1			
	54. යම් ආපදාවකදී (හෝ සිදුවීමකදී), බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කිරීම සඳහා ආයතනය, සිය ආපදා ප්‍රතිසාධන සැලැස්ම ක්‍රියාත්මක කරන්නේද?	4.6.2			

අර්ථ දැක්වීම

ප්‍රති-අනිෂ්ට මෘදුකාංග (Anti-malware)	ප්‍රති-අනිෂ්ට මෘදුකාංග යනු අනිෂ්ට මෘදුකාංග හඳුනා ගැනීමට හෝ එම මෘදුකාංග පරිගණක පද්ධති හෝ ඉලෙක්ට්‍රොනික උපාංගවලට ආසාදනය වීම වැළැක්වීමට නිර්මාණය කර ඇති මෘදුකාංගයකි. අනිෂ්ට මෘදුකාංග (malware) යනු පරිගණකයකට, සේවාදායකයක පරිගණකයකට හෝ පරිගණක ජාලයකට (උදා: වෛරස්, වර්ම්, රැන්සම්වෙයා) හානි කිරීමේ අරමුණින් නිර්මාණය කර ඇති ඕනෑම ආකාරයක මෘදුකාංගයකි.
වත්කම් වර්ගීකරණය (Assets Classification)	වත්කම් වර්ගීකරණය යනු ආයතනයට වටිනාකමක් ඇති වත්කම් ඒවායේ සංවේදීතා මට්ටම සහ වටිනාකම මත පදනම්ව වර්ගීකරණය කිරීමේ ක්‍රියාවලියයි. මෙහි මූලික පරමාර්ථය වන්නේ ආයතනයට එම වත්කමේ ඇති වටිනාකමට අනුකූලව සුදුසු මට්ටමේ ආරක්ෂාවක් ලබා දීම සහතික කිරීමයි. මේ ආකාරයට තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වර්ගීකරණය කළ හැකිය.
වත්කම් භාරකරු (Assets Custodian)	තොරතුරු වත්කම් හිමිකරු විසින් අනුමත කරන ලද ආරක්ෂක අවශ්‍යතාවලට අනුව වත්කමේ ජීවන චක්‍රය පුරා තොරතුරු වත්කමක් ආරක්ෂා කිරීමේ වගකීම ඇති නිලධාරියෙකු හෝ ආයතනයක් වේ.
වත්කම් හිමිකරු (Assets Owner)	වත්කම් හිමිකරු යනු වත්කම්වල දෛනික කළමනාකරණය සඳහා වගකිව යුතු විධායක මට්ටමේ නිළධාරියකු වේ. වත්කම් හිමිකරු විසින් අදාළ වත්කමෙහි මුළු ජීවන චක්‍රයම පාලනය කරනු ලබන අතර වත්කම්වලට ඇති අවදානම හඳුනා ගෙන ඒවා ආරක්ෂා කිරීම සඳහා සුදුසු ආරක්ෂණ ක්‍රමවේදයන් යෝජනා කළ යුතුය.
තොරතුරුවල උපයෝජ්‍යතාවය (Availability of Information)	උපයෝජ්‍යතාවය යනු තොරතුරු අවසරලත් පුද්ගලයන් සඳහා අවශ්‍ය ඕනෑම අවස්ථාවකදී ප්‍රවේශ වීම සහ භාවිත කිරීමේ හැකියාව තහවුරු කිරීමයි.
තොරතුරු වල රහස්‍යභාවය (Confidentiality of Information)	රහස්‍යභාවය යනු අනවසර පුද්ගලයන්ට සහ ආයතනවලට තොරතුරු හෙලි නොකරන බවට තහවුරු කිරීමයි.
සංවේදී තොරතුරු වත්කම් (Sensitive Information Assets)	සංවේදී තොරතුරු වත්කම් යනු අස්ථානගත වීමක්, වෙනස් කිරීමක්, අවභාවිතයක්, අනවසර හෙළිදරව් කිරීමක් හෝ බිඳ වැටීමක් නිසා ආයතනයකට හෝ පුද්ගලයකුට අහිතකර බලපෑමක් ඇති කළ හැකි තොරතුරු වේ. මේවා “ඉතා රහසිගත” (Secret), “රහසිගත” (Confidential) සහ “සීමිත හුවමාරුව” (Limited Sharing) ලෙස වර්ගීකරණය කරනු ඇත.
තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම් (Critical IT Assets)	තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම් යනු අනවසර ඇතුල්වීමක්, අවභාවිතයක් හෝ බිඳ වැටීමක් නිසා එහි දත්තවලට, ආයතනයට, හෝ පුද්ගලයකුට අහිතකර බලපෑමක් ඇති කළ හැකි පද්ධති වේ. මේවා “ඉතා තීරණාත්මක” (Very Critical) සහ “තීරණාත්මක” (Critical) තොරතුරු තාක්ෂණ වත්කම් ලෙස වර්ගීකරණය කළ හැකිය. මෙම පද්ධති සඳහා ඉහළ මට්ටමේ ආරක්ෂාවක් අවශ්‍ය වන අතර ඒවා පහත අර්ථ දක්වා ඇති තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් යන ආකාරයෙන් ද පැවතිය හැකිය.
තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් (Critical National Information Infrastructure)	තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් යනු බිඳ වැටීමකදී හෝ අසාර්ථක වීමකදී ජාතික ආරක්ෂාව, පාලනය, ආර්ථිකය, සෞඛ්‍ය සහ සමාජ යහපැවැත්ම කෙරෙහි ඍණාත්මක බලපෑමක් ඇති කරන තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වේ.
ඩිජිටල් අත්සන් (Digital Signatures)	ඩිජිටල් අත්සන් යනු ඩිජිටල් පණිවිඩ හෝ ලේඛනවල සත්‍යතාව තහවුරු කිරීම සඳහා යොදා ගැනෙන තාක්ෂණයකි. එය යවන්නාගේ සත්‍යතාව (අනන්‍යතාවය), පණිවිඩ නිරවද්‍යතාවය (අනවසර වෙනස් කිරීම්) සහ

	ප්‍රතික්ෂේප කිරීම (යවන්නාට පසුව ලේඛනය ජනනය කිරීම ප්‍රතික්ෂේප කළ නොහැක) සපයයි.
සංකේතනය (Encryption)	සංකේතනය යනු පණිවිඩයක් ආරක්ෂිත-කේත සහිත පෙළකට පරිවර්තනය කිරීමේ ක්‍රියාවලියයි, එය විකේතනය හරහා නැවත පරිවර්තනය නොකර තේරුම් ගත නොහැක.
රාජ්‍ය ආයතන (Government Organizations)	රාජ්‍ය ආයතන යනු 2016 අංක 12 දරන තොරතුරු දැනගැනීමේ අයිතිය පිළිබඳ පනතේ අර්ථ දක්වා ඇති පොදු අධිකාරීන්ය.
ආරක්ෂක පාලන (Information Security Controls)	ආරක්ෂක පාලන යනු තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ආරක්ෂක අවදානම් වළක්වා ගැනීම, හඳුනා ගැනීම, ප්‍රතික්‍රියා කිරීම හෝ අවම කිරීම සඳහා වන ආරක්ෂක ක්‍රියාකාරකම් වේ. මෙවන් පාලනයන්, තොරතුරු වත්කම් ආරක්ෂා කිරීම සඳහා ස්ථාපනය කර ඇති තාක්ෂණයන්, ප්‍රතිපත්ති, ක්‍රියා පටිපාටි හෝ වෙනත් ක්‍රමවේද වේ.
තොරතුරු ආරක්ෂක නිලධාරි (Information Security Officer)	තොරතුරු ආරක්ෂණ නිලධාරියා යනු තොරතුරු වත්කම් ප්‍රමාණවත් ලෙස ආරක්ෂා කිරීම සහතික කිරීම සඳහා සංවිධාන අරමුණු, උපාය මාර්ග සහ ක්‍රියාකාරී සැලසුම් ස්ථාපිත කිරීම සහ පවත්වාගෙන යාම සඳහා වගකිව යුතු ජ්‍යෙෂ්ඨ මට්ටමේ නිලධාරියකි.
තොරතුරු ආරක්ෂණ කමිටුව (Information Security Committee)	ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේදී, තොරතුරු ආරක්ෂණ නිළධාරී විසින් සිදු කරනු ලබන සියලුම තොරතුරු ආරක්ෂණ පාලන, ක්‍රියාකාරී සැලසුම්, වත්කම් වර්ගීකරණ යෝජනා ක්‍රම, සිද්ධි ප්‍රතිචාර සැලසුම් සහ ආපදා ප්‍රතිසාධන සැලසුම් සහ අනෙකුත් ක්‍රියාකාරකම් සමාලෝචනය කිරීම සහ අනුමත කිරීම සඳහා මෙම කමිටුව වගකිව යුතුය.
ආරක්ෂක තොරතුරු සහ සිදුවීම් කළමනාකරණ පද්ධති (Security Information and Event Management Systems)	ආරක්ෂක තොරතුරු සහ සිදුවීම් කළමනාකරණ පද්ධති යනු ලොග් සටහන් වලින් එකතු කරන දත්ත විශ්ලේෂණය කර, ආරක්ෂක තර්ජන සහ සිදුවීම් තත්‍ය කාලීනව හඳුනාගෙන ඒවාට නිසි ක්‍රියාමාර්ග ගැනීම සඳහා පද්ධති පරිපාලකයන් වෙත දැනුම්දීම සඳහා නිර්මාණය කර ඇති පද්ධතිවේ.
තොරතුරු හා සයිබර් ආරක්ෂාව (Information and Cyber Security)	තොරතුරු හා සයිබර් ආරක්ෂාව යනු තොරතුරු වල රහස්‍යභාවය, නිරවද්‍යතාවය සහ උපයෝජ්‍යතාවය සහතික කිරීම සඳහා එම තොරතුරු වත්කම් වෙත අනවසරයෙන් වන ප්‍රවේශ වීම්, භාවිත කිරීම්, වෙනස් කිරීම්, හෝ විනාශ කිරීම් වලින් තොරතුරු වත්කම් ආරක්ෂා කිරීමයි. මේ යටතේ තොරතුරු වත්කම් අඩංගු හෝ භාවිතා වන තොරතුරු තාක්ෂණ මෙවලම් පුද්ගලයන් විසින් ද්වේශසහගතව සයිබර් තාක්ෂණය හෝ වෙනත් ක්‍රමවේදයන් භාවිතා කොට සිදු කරන හානිදායී ක්‍රියා වලින් ආරක්ෂා කර ගැනීම හෝ ජල ගැලීම්, ගිනි ගැනීම් වැනි වෙනත් ස්වභාවික විපත් මගින් සිදු වන හානි වලින් ආරක්ෂා කර ගැනීමත් ඇතුළත් වේ.
තොරතුරු වත්කම් (Information Assets)	තොරතුරු වත්කම් යනු ආයතනයට වටිනාකමක් ඇති තොරතුරු හෝ දත්ත වේ. විද්‍යුත් ආකෘතියකින් ලබා ගත හැකි ලේඛන, දත්ත සමුදා වාර්තා මෙන්ම කඩදාසි ආකෘතියෙන් ලබා ගත හැකි ලේඛන මෙයට ඇතුළත් වේ. තොරතුරු වත්කම් සඳහා උදාහරණ: වචන ගොනුව, රූප, දත්ත ගබඩාවක සේවකයින්ගේ පුද්ගලික වාර්තාව.
තොරතුරු තාක්ෂණ වත්කම් (IT Assets)	තොරතුරු තාක්ෂණ වත්කම් යනු ආයතනයට වටිනාකමක් ඇති ඕනෑම තොරතුරු තාක්ෂණ උපකරණ, තොරතුරු පද්ධතිය, මෘදුකාංග, ගබඩා මාධ්‍ය වේ. තොරතුරු තාක්ෂණ වත්කම් සඳහා උදාහරණ වන්නේ පරිගණක, සේවාදායක පරිගණක, රවුටර, දෘඪ තැටි, ජාල, මෘදුකාංග, තොරතුරු පද්ධති සහ එහි සංරචක වේ.
ආක්‍රමණ හඳුනාගැනීමේ පද්ධති හා ආක්‍රමණය වැළැක්වීමේ පද්ධති (Intrusion	ආක්‍රමණ හඳුනාගැනීමේ පද්ධති (Intrusion Detection Systems) යනු, සයිබර් ප්‍රහාර හඳුනා ගැනීම සඳහා ජාල විශ්ලේෂණය කරන මෙවලම් වේ. ආක්‍රමණය වැළැක්වීමේ පද්ධති (Intrusion

Detection and Prevention Systems)	Prevention Systems) යනු සයිබර් ප්‍රහාර හඳුනා ගැනීම සඳහා ජාල විශ්ලේෂණයකර ඒ මත පදනම්ව සයිබර් ප්‍රහාර වලක්වනු ලබන මෙවලම් වේ.
තොරතුරුවල නිරවද්‍යතාවය (Integrity of Information)	නිරවද්‍යතාවය යනු නුසුදුසු වෙනස් කිරීම්වලට එරෙහිව තොරතුරු ආරක්ෂා කිරීමයි. මෙමගින් තොරතුරු එහි මුල් ස්වරූපයෙන් පවතින බව සහතික කරයි.
නිල විද්‍යුත් තැපෑල (Official Email)	නිල විද්‍යුත් තැපෑල යනු "gov.lk" යන වසම් නාමය සහිත රජය විසින් සපයන ලද විද්‍යුත් තැපැල් ගිණුම් වේ.
පෞද්ගලික මේඝය (Private Cloud)	තෝරාගත් පරිශීලකයින් සඳහා පමණක් අන්තර්ජාලය හරහා හෝ පුද්ගලික අභ්‍යන්තර ජාලයක් හරහා ලබා දෙන සේවාවන්. උදා. ලංකා රාජ්‍ය මේඝය.
පොදු මේඝය (Public Cloud)	මේඝගත සේවා යනු ඒවා මිලදී ගැනීමට කැමති ඕනෑම කෙනෙකුට ලබා ගත හැකි සේවා වේ.
ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණ (Recovery Point Objective: RPO)	යනු ආයතනය කොපමණ වාරයක් උපස්ථ ගත යුතුද යන්න පිළිබඳ මිනුමක් වන අතර, එය ප්‍රතිසාධන දත්ත යාවත්කාලීන කරන්නේ කෙසේද යන්න පිළිබඳ ඇඟවීමක් ලබා දෙයි. එය දත්ත ප්‍රතිසාධනය කිරීමට පිළිගත හැකි මුල්ම කාලය (earliest possible time) පෙන්නුම් කරයි. උදාහරණයක් ලෙස, උපස්ථ අතර ව්‍යසනයක් සිදුවුවහොත්, ආයතනය විනාඩි 2 ක දත්ත හෝ පැය 2 ක දත්ත හෝ සම්පූර්ණ දිනයක දත්ත අහිමි කර ගත හැකිද යන්න පිළිබඳ මිනුමක් වේ.
ප්‍රතිසාධන කාල අරමුණ (Recovery Time Objective: RTO)	ප්‍රතිසාධන කාල අරමුණ යනු ආයතනයකට දරාගත හැකි බිඳවැටීම් කාලයයි.
පද්ධති ශක්තිමත් කිරීම (Systems Hardening)	පද්ධති ශක්තිමත් කිරීම යනු තොරතුරු තාක්ෂණ අවදානම සහ අනවසර පුද්ගලයන්ට නතුවීමේ හැකියාව අවම කිරීම සඳහා පෙරනිමි වින්‍යාසය සහ සැකසුම් වෙනස් කිරීම මගින් පද්ධතියක් සුරක්ෂිත කිරීමේ ක්‍රියාවලියයි.
තත්‍යසම පෞද්ගලික ජාල (Virtual Private Network)	තත්‍යසම පෞද්ගලික ජාල යනු අන්තර්ජාලය හරහා දත්ත සන්නිවේදනය කිරීම සඳහා සංකේතාත්මක වැනලයක් භාවිතා කිරීමෙන් ආරක්ෂිත සම්බන්ධතාවයක් ස්ථාපිත කිරීමයි.

භාවිත ලේඛන

1. තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශය. ශ්‍රී ලංකා සර්ට් ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.

2. අවම තොරතුරු ආරක්ෂණ ප්‍රමිතීන්. ශ්‍රී ලංකා සර්ට් ආයතනය විසින් 2021 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.

3. ශ්‍රී ලංකාවේ තොරතුරු සහ සයිබර් ආරක්ෂණ උපායමාර්ගය (2019:2023). ශ්‍රී ලංකා සර්ට් ආයතනය විසින් 2019 දී ප්‍රකාශයට පත් කරන ලදී. මෙය https://cert.gov.lk /documents/NCSStrategy.pdf යන වෙබ් අඩවියෙන් බාගත කළ හැක.

4. සයිබර් ආරක්ෂණ රාමුව. එක්සත් ජනපද ජාතික ප්‍රමිති සහ තාක්ෂණ ආයතනය විසින් ප්‍රකාශයට පත් කරන ලදී. මෙය ලේඛනය https://www.nist.gov/ cyberframework/online-learning/five-functions යන වෙබ් ලිපිනය මගින් බාගත කළ හැක.

5. නිවසේ සිට වැඩ කිරීම සඳහා තොරතුරු ආරක්ෂණ මාර්ගෝපදේශ. ශ්‍රී ලංකා සර්ට් විසින් ප්‍රකාශනය කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් ලිපිනය මගින් බාගත කළ හැක.

6. රාජ්‍ය ආයතන සඳහා සම්පාදිත වෙබ් අඩවි ආරක්ෂක මාර්ගෝපදේශය. ශ්‍රී ලංකා සර්ට් ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.

7. රාජ්‍ය ආයතන සඳහා සම්පාදිත වෙබ් යෙදවුම් ආරක්ෂණ මාර්ගෝපදේශය. ශ්‍රී ලංකා සර්ට් ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.

8. වෙබ් යෙදවුම් ආරක්ෂාව සඳහා සම්පාදිත තාක්ෂණික මාර්ගෝපදේශය. ශ්‍රී ලංකා සර්ට් ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.

9. ජාත්‍යන්තර ප්‍රමිති සංවිධානය: 27002 (2013) : තොරතුරු තාක්ෂණය – ආරක්ෂක ශිල්පීය ක්‍රම - තොරතුරු ආරක්ෂණ කළමනාකරණ පද්ධති – අවශ්‍යතා. මෙය https://www. iso.org/ යන වෙබ් ලිපිනය මගින් බාගත කළ හැක.