මුදල් මණ්ඩලය

ශ්‍රී ලංකා මහ බැංකුව

2022 ජනවාරි 28 — මුදල් ව්‍යාපාර පනත යටතේ නිකුත් කරන විධාන — 2022 අංක 01

තාක්ෂණික අවදානම් කළමනාකරණය සහ ඔරොත්තු දීමේ හැකියාව

1. නෛතික ප්‍රතිපාදන

1.1 2011 අංක 42 දරන මුදල් ව්‍යාපාර පනතේ 12 වන වගන්තිය මගින් පැවරී ඇති බලතල ප්‍රකාරව, ශ්‍රී ලංකා මහ බැංකුවේ මුදල් මණ්ඩලය විසින් බලපත්‍රලාභී මුදල් සමාගම්වල තාක්ෂණික අවදානම් කළමනාකරණය සහ ඔරොත්තු දීමේ හැකියාව පිළිබඳව මෙම විධානයන් නිකුත් කරනු ලබයි.

2. විධානවල අරමුණු

2.1 නවීන තාක්ෂණය ප්‍රතිග්‍රහණය කිරීම සහ නියෝජිතයන් හා තෙවන පාර්ශව වෙත ලබා දෙන තාක්ෂණ සේවා ඉහළ නැංවීමත් සමඟ, බලපත්‍රලාභී මුදල් සමාගම් තාක්ෂණික අවදානමට ලක් වන අතර එය අවදානම් කළමනාකරණයට ඒකාබද්ධ කළ යුතු වේ. මෙම විධානයන් මගින් බලපත්‍රලාභී මුදල් සමාගම් සඳහා තාක්ෂණික අවදානම් කළමනාකරණය සහ ඔරොත්තු දීමේ හැකියාව පිළිබඳ අවම නියාමන අවශ්‍යතා පිහිටු වීමට අරමුණු කෙරේ.

3. අදාළත්වය

3.1 මෙම රාමුවේ අවශ්‍යතා, නියෝජිතයන් සහ තෙවන පාර්ශව සේවා සපයන්නන් විසින් ක්‍රියාත්මක කරනු ලබන මෙහෙයුම් ඇතුළුව බලපත්‍රලාභී මුදල් සමාගම්වල සමස්ත මෙහෙයුම්වලට අදාළ විය යුතුය.

3.2 බලපත්‍රලාභී මුදල් සමාගමක් මෙම විධානයන් ක්‍රියාත්මක කරන ප්‍රමාණය සහ මට්ටම, භාවිත කරන තාක්ෂණයන්ගේ අවදානම් මට්ටම සහ සංකීර්ණත්වය සමඟ සමාන විය යුතු අතර, ඒවා නියමිත පරිදි අධ්‍යක්ෂ මණ්ඩලය විසින් අවම නියාමන අවශ්‍යතා වලින් ඔබ්බට ගොස් නිශ්චය කරනු ලැබිය යුතුය.

3.3 මෙම විධානයන්හි විධිවිධාන, 10 වන විධානයෙහි අන්තර්කාලීන විධිවිධානවලට යටත්ව, 2023.01.01 දින සිට බලපැවැත්විය යුතුය.

4. තාක්ෂණික අවදානම් යහපාලනය සහ අධීක්ෂණය

4.1 **අධ්‍යක්ෂ මණ්ඩලයේ කාර්යභාරය**

අ) තාක්ෂණය, ව්‍යාපාර ක්‍රමෝපාය සහ අවම නියාමන අවශ්‍යතා මගින් එල්ල කරනු ලබන විභව අවදානම්වලට ගැළපෙන පරිදි තොරතුරු තාක්ෂණ සහ සයිබර් ආරක්ෂණ ක්‍රමෝපායයන් සම්පාදනය කිරීම අධ්‍යක්ෂ මණ්ඩලයේ වගකීම වේ.

ආ) මැනවින් ලේඛනය කරන ලද තොරතුරු ආරක්ෂණ ප්‍රතිපත්තියක්, නිසි මණ්ඩල අධීක්ෂණයක් සහිතව පූර්ණ සහ සවිමත් අවදානම් කළමනාකරණ රාමුවක්, ප්‍රමාණවත් තාක්ෂණික සම්පත්, විෂය පිළිබඳ දැනුවත්භාවයක් ගොඩනැංවීම සඳහා ආයතනික සැකසුමක් සහ ස්වාධීන විගණනයක් ඇතුළු අධ්‍යක්ෂ මණ්ඩලය විසින් අනුමත කරනු ලබන ප්‍රතිපත්ති මගින් තොරතුරු තාක්ෂණ සහ සයිබර් ආරක්ෂණ ක්‍රමෝපාය සමන්විත විය යුතුය.

ඇ) වලාකුළු සේවාවන් (Cloud Services) සහ මූල්‍ය තාක්ෂණය (Fin Tech) භාවිතයෙන් පැන නගින අවදානම් ඇතුළුව බලපත්‍රලාභී මුදල් සමාගම් වෙත එල්ල විය හැකි තොරතුරු තාක්ෂණ සහ සයිබර් අවදානම් සැලකිල්ලට ගනිමින් තෙවන පාර්ශවයන් සහ නියෝජිතයන් සමඟ ඇති ගිවිසුම් ඇගයීමට ලක් කළ යුතුය.

ඈ) බලපත්‍රලාභී මුදල් සමාගම්වල තොරතුරු ආරක්ෂාව සහ තාක්ෂණමය ඔරොත්තු දීමේ හැකියාව සඳහා වගකීම දරන අධ්‍යක්ෂ මණ්ඩල මට්ටමේ තොරතුරු ආරක්ෂණ කමිටුවක් පිහිටුවීම සඳහා බලපත්‍රලාභී මුදල් සමාගම් දිරිමත් කෙරේ.

ඉ) තාක්ෂණික අවදානම් කළමනාකරණය සහ ඔරොත්තු දීමේ හැකියාව විධානය තුළ නියාමන අවශ්‍යතා සාර්ථකව ක්‍රියාත්මක කිරීම තහවුරු කිරීම සඳහා අධ්‍යක්ෂ මණ්ඩලය විසින් ප්‍රමාණවත් අධීක්ෂණ ක්‍රියාමාර්ග ගනු ලැබිය යුතුය.

4.2 **තාක්ෂණික අවදානම් කළමනාකරණය**

අ) තාක්ෂණික අවදානම් කළමනාකරණයේ අවධානය පුළුල් වශයෙන් හඳුනා ගැනීම, ආරක්ෂාව, අනාවරණය, ප්‍රතිචාර දැක්වීම සහ ප්‍රතිසාධනය යන කාර්යයන් කෙරෙහි යොමු විය යුතුය. තාක්ෂණික අවදානම් කළමනාකරණය මඟින් පාලනයන් හි ප්‍රමාණවත් බව, සඵලතාවය සහ යෝග්‍යතාවය ඇගයීමට ලක් කිරීමත් නිරන්තර කාල විරාමයන් තුළ අධීක්ෂණය කරමින් නිරීක්ෂණය වන ඕනෑම ප්‍රධාන අනනුකූලතාවයන් සම්බන්ධව අධ්‍යක්ෂ මණ්ඩලය දැනුවත් කිරීමත් කළ යුතුය.

ආ) පහත කාර්යයන් සමඟ තාක්ෂණික අවදානම් කළමනාකරණ රාමුවක් පිහිටු විය යුතුය.

i. අවදානම හඳුනා ගැනීම
නියෝජිතයන් හෝ තෙවන පාර්ශ්වීය සේවා සපයන්නන් විසින් පවත්වා ගෙන යනු ලබන හෝ සහාය ලබා දෙනු ලබන තොරතුරු පද්ධති ඇතුළුව, තොරතුරු තාක්ෂණ පරිසරයට අදාළ වන තර්ජන සහ අවදානම් තත්ත්වයන් හඳුනා ගැනීම.

ii. අවදානම් තක්සේරුකරණය
සමස්ත ව්‍යාපාරය සහ මෙහෙයුම් මත තොරතුරු තාක්ෂණ තර්ජන සහ අවදානම් තත්ත්වයන් ඇතිවීමේ සම්භාවිතාව හා ඒවාගේ විභව බලපෑම්/ප්‍රතිඵල පිළිබඳව විශ්ලේෂණයක් සිදු කිරීම. අවදානම් සිද්ධි ඇතිවීමේ සම්භාවිතාව සහ එහි බලපෑම, මැනීම සහ තීරණය කිරීම සඳහා නිර්ණායකයක් පිහිටු වීම.

iii. අවදානම් සඳහා පිළියම් යෙදීම
තොරතුරු තාක්ෂණ පද්ධතිවල තීරණාත්මක බව සහ අවදානමට ඔරොත්තු දීමේ මට්ටම සමඟ අනුකූල වන අවදානම් අවම කිරීමේ සහ පාලන ක්‍රියාමාර්ග සංවර්ධනය කිරීම සහ ක්‍රියාත්මක කිරීම. අවදානම් අවම කිරීමේ ක්‍රියාමාර්ග යෙදීමෙන් අනතුරුව අවදානම් පිළිගත හැකි මට්ටමකට අවම වී තිබේද යන වග තක්සේරු කිරීම.

iv. අවදානම් අධීක්ෂණය, සමාලෝචනය සහ වාර්තාකරණය
හඳුනාගත් අවදානම්වලට එරෙහිව තොරතුරු තාක්ෂණ පාලනවල සැලැස්ම සහ මෙහෙයුම් ඵලදායීතාවය තක්සේරු කිරීම සහ අධීක්ෂණය සඳහා ක්‍රියාවලියක් පිහිටු වීම.

4.3 **ජ්‍යෙෂ්ඨ කළමනාකාරීත්වයේ කාර්යභාරය**

අ) සඵලදායී අධීක්ෂණය, වාර්තාකරණය, උත්සන්න වීමේ ක්‍රියාමාර්ගවල සහය ඇති හා අනුමත කරන ලද අවදානම් ඔරොත්තු දීමකට අනුකූල නිශ්චිත ප්‍රතිපත්ති සහ ක්‍රියාපටිපාටිවලට අධ්‍යක්ෂ මණ්ඩලය විසින් අනුමත කරන ලද තාක්ෂණ අවදානම් කළමනාකරණ රාමුව ක්‍රියාත්මක කිරීම සහ ඕනෑම අහිතකර ප්‍රවණතාවක් පිළිබඳව අධ්‍යක්ෂ මණ්ඩලය වෙත දැනුම් දීම.

ආ) මාණ්ඩලික මට්ටමේ තොරතුරු ආරක්ෂණ කමිටුව සඳහා සහාය ලබා දීමට සහ තාක්ෂණය ප්‍රතිග්‍රහණය කිරීම, තොරතුරු ආරක්ෂාව, සයිබර් ආරක්ෂාව, බාහිරින් සේවා සපයා ගැනීම සහ සංකේන්ද්‍රනය පිළිබඳ ගැටලුවලට පිළියම් යෙදීම සඳහා ප්‍රධාන විධායක නිලධාරියා විසින් ප්‍රධානත්වය දරනු ලබන කළමනාකාරීත්ව මට්ටමේ තොරතුරු ආරක්ෂණ කමිටුවක් බලපත්‍රලාභී මුදල් සමාගම් සතු විය යුතුය. කළමනාකාරීත්ව මට්ටමේ තොරතුරු ආරක්ෂණ කමිටුවක කාර්යභාරයන් සහ වගකීම් ඇමුණුම - 1 හි දක්වා ඇත.

ඇ) ආයතනය තුළ සහ බාහිර සේවා සපයන තෙවන පාර්ශ්වීය නියෝජිත ආයතන තුළ සයිබර් සනීපාරක්ෂාව අඛණ්ඩව පවත්වා ගෙන යනු ලබන බවට තහවුරු කිරීම. කාර්යමණ්ඩලය සහ අනෙකුත් සම්බන්ධිත පාර්ශ්වයන් විසින් සිදු කරනු ලබන භූමිකාව මත පදනම්ව දැනුවත් කිරීමේ වැඩසටහන් කලින් කලට පැවැත්විය යුතු වේ.

ඈ) විවිධ තොරතුරු ආරක්ෂණ ප්‍රමිතීන්/ රාමුවල පැහැදිලිව දක්වා ඇති පරිදි භෞතික පිවිසුම (physical access), තාර්කික පිවිසුම (logical access), විපර්යාස කළමනාකරණය (change management), පරිමා කළමනාකරණය (patch management) සහ වින්‍යාස කළමනාකරණය (configuration management), යහ පරිචයන්ට (best practices) අදාළ නිසි පාලන මාර්ගයන් පිහිටුවීම සහ එවැනි පාලනයන් තොරතුරු පද්ධතිවල සමස්ත ජීවන චක්‍රය සඳහා සලකා බැලිය යුතු වේ.

ඉ) තොරතුරු ආරක්ෂණ පාලන මාර්ගවල කාර්යක්ෂමතාව සහ අදාළත්වය කලින් කලට සමාලෝචනය කිරීම හා ප්‍රමුඛතාව මත අවශ්‍ය පිළියම් ක්‍රියාමාර්ග ගැනීම.

4.4 **ප්‍රධාන තොරතුරු ආරක්ෂක නිලධාරියා**

අ) බලපත්‍රලාභී මුදල් සමාගම් විසින් තොරතුරු ආරක්ෂක අවශ්‍යතාවන්ට නායකත්වය සැපයීමට ප්‍රධාන තොරතුරු ආරක්ෂක නිලධාරියෙකු පත් කළ යුතුය. ප්‍රධාන තොරතුරු ආරක්ෂණ නිලධාරියෙකුගේ ප්‍රධාන වගකීම් පහත පරිදි වේ:

i. තොරතුරු ආරක්ෂණ ක්‍රමෝපාය සංවර්ධනය කිරීම, කළමනාකරණය සහ ක්‍රියාත්මක කිරීම.

ii. තොරතුරු ආරක්ෂණ ක්‍රියාමාර්ග අඛණ්ඩව අධීක්ෂණය හා ඇගයීම.

iii. තොරතුරු ආරක්ෂණ විගණන සහ අවදානම් ඇස්තමේන්තු සිදු කිරීම.

iv. තොරතුරු ආරක්ෂණ රෙගුලාසිවලට අනුකූලව ආයතනය පවත්වා ගෙන යෑම.

v. ව්‍යාපාර අඛණ්ඩතා සැලසුම් සංවර්ධනය කිරීම සහ පවත්වා ගෙන යෑම.

vi. තොරතුරු ආරක්ෂණ අවදානම් සහ ක්‍රමෝපායන්ට අදාළව පුහුණුකරණය සහ දැනුවත් කිරීම.

vii. තොරතුරු ආරක්ෂණ අයවැයන් කළමනාකරණය; සහ

viii. තොරතුරු ආරක්ෂණය පිළිබඳව අධ්‍යක්ෂ මණ්ඩලය වෙත වාර්තා කිරීම.

ආ) ප්‍රධාන තොරතුරු ආරක්ෂක නිලධාරියා ජ්‍යෙෂ්ඨ කළමනාකරණ කණ්ඩායමේ විධායක නිලධාරියෙකු විය යුතුය.

ඇ) තොරතුරු ආරක්ෂණ නිලධාරියා විසින් ප්‍රධාන විධායක නිලධාරියා වෙත වාර්තා කළ යුතුය, නැතහොත් වාර්තාකරණ ධූරාවලියක් අවසානයේ ප්‍රධාන විධායක නිලධාරියා සිටින සුදුසු වාර්තාකරණ ධූරාවලියක් තිබිය යුතුය.

ඈ) තොරතුරු ආරක්ෂණ කටයුතු බාධාවකින් තොරව ක්‍රියාත්මක කිරීම සඳහා තොරතුරු ආරක්ෂණ නිලධාරියා බලපත්‍රලාභී මුදල් සමාගමෙහි අවදානම් කළමනාකරණ සහ තොරතුරු තාක්ෂණ කාර්යයන් සමඟ සම්බන්ධීකරණය විය යුතුය.

ඉ) බලපත්‍රලාභී මුදල් සමාගම් විසින් මුහුණ දෙනු ලබන තාක්ෂණික සහ තොරතුරු ආරක්ෂණ අවදානම්වල විශාලත්වයට ඒ සඳහා ම වෙන් වූ ප්‍රධාන තොරතුරු ආරක්ෂණ නිලධාරියෙකු අවශ්‍ය නොවන බවට අධ්‍යක්ෂ මණ්ඩලය විසින් නිශ්චිතව දක්වන්නේ නම්, බලපත්‍රලාභී මුදල් සමාගම් විසින් ප්‍රධාන තොරතුරු ආරක්ෂණ නිලධාරියෙකු ලෙස තම අනෙකුත් රාජකාරීන් හා සමගාමීව කටයුතු කිරීම සඳහා එම බලපත්‍රලාභී මුදල් සමාගමෙහි කළමනාකාරීත්ව කණ්ඩායමෙන් විධායක නිලධාරියෙකු පත් කළ යුතුය. කෙසේ වෙතත්, එවැනි නිලධාරියෙකු ප්‍රධාන තොරතුරු නිලධාරියා, ප්‍රධාන අභ්‍යන්තර විගණක, ප්‍රධාන අවදානම් නිලධාරියා හෝ අනුකූලතා නිලධාරියා වැනි ධූරයන් ඇතුළුව ඔහුගේ වගකීම් සමඟ පරස්පර වන කිසිදු කාර්යයක් ඉටු නොකළ යුතුය.

4.5 **අභ්‍යන්තර විගණනය**

බලපත්‍රලාභී මුදල් සමාගම් විසින් අභ්‍යන්තර විගණනයක් තුළින් මෙම විධානයන්හි අවශ්‍යතා සමඟ අනුකූල වීම අවම වශයෙන් වාර්ෂිකව තහවුරු කළ යුතුය.

5. තොරතුරු සහ තොරතුරු පද්ධතිවල ආරක්ෂාව

5.1 **පාරිභෝගික දත්ත සාධාරණව සහ සදාචාරාත්මකව භාවිත කිරීම**

අ) පාරිභෝගිකයන් විසින් තම දත්ත බලපත්‍රලාභී මුදල් සමාගම් භාවිත කරනු ඇතැයි සාධාරණාත්මකව අපේක්ෂා කරන ආකාරයෙන් පමණක් එම පාරිභෝගික දත්ත භාවිත කරනු ඇති බවට බලපත්‍රලාභී මුදල් සමාගම් විසින් තහවුරු කළ යුතුය.

ආ) අධ්‍යක්ෂ මණ්ඩලය විසින් සෑම කලක දී ම පාරිභෝගික දත්ත සාධාරණව සහ සදාචාරාත්මකව භාවිත කරන බව තහවුරු කිරීමට ඵලදායී ප්‍රතිපත්ති සහ ක්‍රියාමාර්ග ක්‍රියාත්මක කළ යුතුය. තවද, නෛතික අවශ්‍යතාවන් හැරුණු කොට, බලපත්‍රලාභී මුදල් සමාගම් විසින් එවැනි දත්ත අනාවරණය නොකළ යුතුය.

ඇ) බලපත්‍රලාභී මුදල් සමාගම්වල මෙහෙයුම්වලට අදාළව පවතින පරිදි, පාරිභෝගික දත්ත සාධාරණව සහ සදාචාරාත්මක භාවිත කිරීම පිළිබඳ අපේක්ෂාවන් ගෙන් බැඳී පවතින සහ එම රෙගුලාසිවලට ම ඔවුන් යටත් වන බැවින්, මූල්‍ය තාක්ෂණය (Fin Tech) ඇතුළුව, බාහිර සේවා සපයන විකුණුම්කරුවන්ගෙන් ද එම අනුකූලතාව ඉටු වන බවට බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතුය.

5.2 **තොරතුරු වර්ගීකරණය සහ ලේබල්කරණය**

අ) අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ නිර්දේශ මත පදනම්ව අධ්‍යක්ෂ මණ්ඩලය විසින් අනුමත කරන ලද තොරතුරු වර්ගීකරණ ප්‍රතිපත්තියක් බලපත්‍රලාභී මුදල් සමාගම් සතු විය යුතුය.

ආ) ඉලෙක්ට්‍රොනිකමය වශයෙන් පවත්වා ගෙන යනු ලබන සියලුම දත්ත, තොරතුරු ආරක්ෂණ මට්ටම මත පදනම්ව වර්ග කළ යුතු අතර, තොරතුරු වර්ගීකරණ ප්‍රතිපත්තියට අනුව නියම කර ඇති වර්ගීකරණයට අනුව ලේබල් කළ යුතුය.

5.3 **තීරණාත්මක තොරතුරු පද්ධති හඳුනා ගැනීම**

අ) තීරණාත්මක තොරතුරු පද්ධතියක් යනු බලපත්‍රලාභී මුදල් සමාගමේ ඉතා වැදගත් කටයුතු හෝ ගෙවීම් සේවා සැපයීමට සහාය ලබා දෙන ඕනෑම තොරතුරු පද්ධතියක් වන අතර මෙම පද්ධතියේ සිදු වන ඇණ හිටීමකින් මූල්‍ය ආයතනය විසින් තම ගනුදෙනුකරුවන්ට හෝ ප්‍රතිපාර්ශ්වයන්ට සපයනු ලබන මූල්‍යමය සේවාවන්, ව්‍යාපාර මෙහෙයුම්, මූල්‍ය තත්ත්වය, කීර්තිනාමය හෝ අදාළ නීති සහ නියාමන අවශ්‍යතා සමඟ අනුකූල වීම කෙරෙහි සැලකිය යුතු ලෙස හානි සිදු කළ හැකිය.

ආ) තීරණාත්මක තොරතුරු පද්ධතීන් ලෙස ගනුදෙනු සැකසුම් පද්ධති, සාමාන්‍ය ලෙජර පද්ධති, ගෙවීම් සහ පියවීම් පද්ධති, බෙදාහැරීමේ මාර්ග, මුදල් විශුද්ධිකරණය (AML) වැළැක්වීමට හා/ඔබේ ගනුදෙනුකරු හඳුනා ගැනීමේ ක්‍රියාමාර්ග (KYC) සහ මුදල් ව්‍යාපාර බාධාවකින් තොරව පවත්වා ගෙන යෑම තහවුරු කිරීමට අවශ්‍ය වන වෙනත් ඕනෑම පද්ධතියක් හඳුනා ගන්නා නමුත් එකී පද්ධතීන්වලට පමණක්ම තීරණාත්මක තොරතුරු පද්ධතීන් සීමා නොවේ. ඉහතින් බැහැර කරනු ලබන ඕනෑම තොරතුරු පද්ධතියක් අභ්‍යන්තරිකව පිහිටුවන ලද ප්‍රතිපත්තියක් මත පදනම් විය යුතුය. එවැනි සියලු බැහැර කිරීම් අවම වශයෙන් සෑම දෙවසරකට වරක් සමාලෝචනය කළ යුතුය.

ඇ) අධ්‍යක්ෂ මණ්ඩලය විසින් අධ්‍යක්ෂ මණ්ඩල විසින් ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ නිර්දේශයන් මත තීරණාත්මක තොරතුරු පද්ධතිවල නිර්වචනයට ඇතුළත් වන තොරතුරු පද්ධති හඳුනා ගත යුතුය.

5.4 **පරිශීලක ප්‍රවේශ (User Access) කළමනාකරණය**

අ) පාරිභෝගික දත්ත වෙත නිරාවරණය වී තිබෙන තොරතුරු පද්ධති සහ තීරණාත්මක තොරතුරු පද්ධතිවලට පරිශීලක පිවිසුම් පාලනය අදාළ වනු ඇත.

ආ) අධ්‍යක්ෂ මණ්ඩලය විසින් ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ උපදෙස් ඇතිව පාරිභෝගික නොවන රහස්‍ය දත්තවලට නිරාවරණය වන තීරණාත්මක නොවන තොරතුරු පද්ධති සඳහා තීරණාත්මක තොරතුරු පද්ධති හා සමාන පරිශීලක පිවිසුම් පාලන අවශ්‍යතා යෙදවීමේ අවශ්‍යතාව පිළිබඳව තීරණය කළ යුතුය.

ආ) බලපත්‍රලාභී මුදල් සමාගම් විසින් වරප්‍රසාදිත (Privileged) පරිශීලකයන් ඇතුළුව සියලු පරිශීලකයන් කළමනාකරණය කිරීම සඳහා තොරතුරු තාක්ෂණ අංශයේ සම්මත පරිශීලක ප්‍රවේශයක් සහ අනන්‍යතා කළමනාකරණ පද්ධතියක් (පද්ධති) ක්‍රියාත්මක කළ යුතුය.

ඇ) තොරතුරු තාක්ෂණ අංශයේ සම්මත පරිශීලක පිවිසුමක සහ අනන්‍යතා කළමනාකරණ පද්ධතියක් (පද්ධතීන්) සාධ්‍ය හෝ උචිත නොවන අවස්ථාවක දී, අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ නිර්දේශය මත අධ්‍යක්ෂ මණ්ඩලයේ අනුමැතියට යටත්ව පවතින ඕනෑම තොරතුරු පද්ධතියක් සඳහා බලපත්‍රලාභී මුදල් සමාගම් විසින් නිසි පාලනයක් ක්‍රියාත්මක කරමින් විකල්ප පාලන භාවිත කළ යුතුය.

ඉ) වරප්‍රසාදිත පරිශීලක පිවිසුම "තිබිය යුතුය යන අවශ්‍යතාව" මත පමණක් පදනම්ව සැලසිය යුතු අතර, පිවිසුමේ ඉහළම මට්ටම එවැනි පිවිසුමක් අවශ්‍ය වූ විටක දී පමණක් සීමිත කාලයක් සඳහා පමණක් සැලසිය යුතුය. මෙම ගිණුම්වල කටයුතු සටහන් කළ යුතු අතර, බලපත්‍රලාභී මුදල් සමාගමෙහි සිදු කර ගෙන යමින් පවතින අධීක්ෂණයෙහි කොටසක් ලෙස ඒවා සමාලෝචනය කළ යුතුය.

ඊ) බලපත්‍රලාභී මුදල් සමාගම් විසින් පරිශීලක පිවිසුම් සමාලෝචන පහත වාර ගණනින් සිදු කළ යුතුය.

i. තීරණාත්මක තොරතුරු පද්ධති සඳහා අවම වශයෙන් මාසික පදනමක් මත.

ii. පාරිභෝගික දත්ත සහ පාරිභෝගික නොවන රහස්‍ය දත්තවලට නිරාවරණය වූ තීරණාත්මක නොවන තොරතුරු පද්ධති සඳහා අවම වශයෙන් කාර්තුමය පදනමක් මත.

iii. අනෙකුත් සියලු තොරතුරු පද්ධති සඳහා අවම වශයෙන් වාර්ෂික පදනමක් මත.

iv. සම්බන්ධිත ගිණුම්වල (Linked Accounts) මෙහෙයුම් උපදෙස්වලට අනුකූලව සුදුසු ක්‍රමවේදයක් භාවිත කරමින්, විද්‍යුත් බෙදාහැරීමේ මාර්ග ඇතුළුව බලපත්‍රලාභී මුදල් සමාගමෙහි ඕනෑම තොරතුරු පද්ධතියක් භාවිත කිරීම සඳහා ලියාපදිංචි වූ පාරිභෝගිකයන් සහ ඔවුන්ගේ බලයලත් නියෝජිතයන් සඳහා අවම වශයෙන් අර්ධ වාර්ෂික පදනමක් මත.

උ) බලපත්‍රලාභී මුදල් සමාගම් තොරතුරු ආරක්ෂණ කමිටුව විසින් අනුමත කරන ලද පරිදි පරිශීලක පිවිසුම් වරප්‍රසාද සමාලෝචන පැවැත්වීම සඳහා නිසි ක්‍රමවේදයන් අනුගමනය කළ යුතුය.

ඌ) පරිශීලක පිවිසුම් වරප්‍රසාද සමාලෝචනයන් සිදු කරන විට දී, බලපත්‍රලාභී මුදල් සමාගම් විසින් තෙවන පාර්ශ්ව සේවා සපයන්නන් වැනි අභ්‍යන්තර සහ බාහිර පරිශීලකයන් හඳුනා ගැනීම, සත්‍යාපනය (authentication) සහ අවසර දීම (authorization) සමාලෝචනය කිරීමට සුදුසු යාන්ත්‍රණයක් ක්‍රියාත්මක කළ යුතුය.

5.5 **පරිගණක ආරක්ෂාව සහ පරිශීලක කටයුතු සටහන් (User Activity Log) කළමනාකරණය**

අ) තීරණාත්මක තොරතුරු පද්ධති සහ පාරිභෝගික දත්ත තොරතුරු පද්ධතිවල පරිගණක ආරක්ෂාව සහ පරිශීලක කටයුතු සටහන් කිරීම කළමනාකරණය සඳහා බලපත්‍රලාභී මුදල් සමාගම් විසින් සටහන් කළමනාකරණ ප්‍රතිපත්තියක් ක්‍රියාත්මක කළ යුතුය. එවැනි ප්‍රතිපත්තියක් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුවක අභිමතය පරිදි අනෙකුත් තොරතුරු පද්ධති දක්වා පුළුල් කළ හැකිය.

ආ) අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ නිර්දේශයන් මත පදනම්ව අධ්‍යක්ෂ මණ්ඩලය විසින් මෙම ප්‍රතිපත්තිය අනුමත කරනු ලැබිය යුතුය.

ඇ) පවත්වා ගෙන යා යුතු සටහන් වර්ග (Logs), රඳවා ගැනීමේ කාලය, සමාලෝචනය කිරීමේ වාර ගණන, සමාලෝචනය කිරීමේ ක්‍රමය හා භාවිත කළ යුතු මෙවලම් (Tools), සිද්ධි හඳුනා ගැනීම හා ප්‍රතිචාරය සහ සටහන් ගත කිරීම් පවත්වා ගෙන යෑම සහ සමාලෝචනය සඳහා වන වගකීම් යනාදිය මෙම ප්‍රතිපත්තියට ඇතුළත් විය යුතුය.

ඈ) ආරක්ෂණ මෘදුකාංග, මෙහෙයුම් පද්ධති සහ යෙදවුම් මගින් පරිගණක ආරක්ෂණ සටහන් උත්පාදනය කළ යුතුය. පවත්වා ගෙන යනු ලබන පරිගණක ආරක්ෂාව සහ පරිශීලක කටයුතු සටහන් කිරීම්, තොරතුරු ආරක්ෂණ සිදුවීම් සාර්ථකව හඳුනා ගැනීමට සහ ගවේෂණය කිරීම සඳහා ප්‍රමාණවත් විය යුතුය.

ඉ) වරප්‍රසාදිත පරිශීලකයන්ගේ සටහන් සඳහා ඉහළ අවධානයක් යොමු කළ යුතු අතර, නිසි මෙවලම් සහ උපක්‍රම භාවිත කරමින් ආසන්න තත් කාලීන පදනමක් මත සමාලෝචනය කළ යුතුය.

5.6 **දත්ත සංකේතනය (Data Encryption)**

5.6.1 පාරිභෝගික දත්ත සංකේතනය

අ) සංකේතනය මඟින් පාරිභෝගික දත්ත ආරක්ෂා කළ යුතුය.

ආ) බලපත්‍රලාභී මුදල් සමාගම්, නියෝජිතයන් සහ තෙවන පාර්ශ්වීය සේවා සපයන්නන් සමඟ පවත්වා ගෙන යනු ලබන පාරිභෝගික දත්ත සඳහා සංකේතනය අදාළ විය යුතුය.

ඇ) දත්ත සංකේතනයේ මට්ටම්,

i. ඩේටා ඇට් රෙස්ට් එන්ක්‍රිප්ෂන් (data-at-rest encryption) පාරිභෝගික දත්තයන්, දත්ත සමුදාය (Database) සංකේතනයට හෝ ගොනු මට්ටමේ සංකේතනයට යටත් විය යුතුය.

ii. ඩේටා ඉන් ට්‍රාන්සිට් එන්ක්‍රිප්ෂන් (data-in-transit encryption) පාරිභෝගික දත්තවලින් සමන්විත ගොනුවක් සම්ප්‍රේෂණය කරන ඕනෑම අවස්ථාවකදී, එය ගොනු මට්ටමින් සංකේතනය කර තිබිය යුතුය.

iii. අන්ත ලක්ෂ්‍ය උපාංග සහ වෙන් කළ හැකි මාධ්‍ය සඳහා පූර්ණ සංවාහක සංකේතනය (Full disk encryption for endpoint devices and removable media)

ස්ථිර වශයෙන් හෝ තාවකාලිකව යන දෙආකාරයෙන් එක් ආකාරයකට බලපත්‍රලාභී මුදල් සමාගම්වල ගනුදෙනුකරුවන්ගේ දත්ත තැන්පත් කරන තෙවන පාර්ශ්වීය සේවා සපයන්නන් සහ නියෝජිතයන්ගේ උපාංග ඇතුළුව සියලු අන්ත ලක්ෂ්‍ය උපාංග සහ වෙන් කළ හැකි මාධ්‍ය පූර්ණ සංවාහක සංකේතනයට යටත් විය යුතුය.

ඈ) බලපත්‍රලාභී මුදල් සමාගම් විසින් තොරතුරු තාක්ෂණ අංශයේ සම්මත සංකේතන ක්‍රමයන් භාවිත කළ යුතුය. අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවෙහි නිර්දේශය මත අධ්‍යක්ෂ මණ්ඩලයේ අනුමැතියට යටත්ව එවැනි ක්‍රමයන් තෝරා ගැනීම සිදු කළ යුතුය.

ඉ) තොරතුරු තාක්ෂණ අංශයේ සම්මත සංකේතන ක්‍රම සාධ්‍ය නොවන හෝ සුදුසු නොවන විට දී, බලපත්‍රලාභී මුදල් සමාගම් විසින් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවෙහි අනුමැතියට යටත්ව ගනුදෙනුකරු දත්ත ආරක්ෂා කිරීම සඳහා විකල්ප පාලන භාවිත කළ යුතුය.

5.6.2 පාරිභෝගික නොවන රහස්‍ය දත්ත සංකේතනය

අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව විසින් තීරණය කරනු ලබන පරිදි සංකේතනය මඟින් වළක්වා ගැනීමට හැකියාව තිබූ දත්ත පිටතට පැමිණීම හෝ වෙනත් අහිතකර තොරතුරු ආරක්ෂණ සිදුවීමකට යටත්ව බලපත්‍රලාභී මුදල් සමාගම් වෙත නොසැලකිය හැකි අහිතකර බලපෑමක් පමණක් එල්ල කරන පාරිභෝගික නොවන රහස්‍ය දත්ත වර්ග හැරුණු කොට, පාරිභෝගික නොවන රහස්‍ය දත්තවලට ද සංකේතන අවශ්‍යතා අදාළ විය යුතුය.

5.7 **ආරක්ෂණ මෙහෙයුම් කේන්ද්‍රය**

විද්‍යුත් බෙදා හැරීමේ මාර්ග ලබා දෙන සියලු බලපත්‍රලාභී මුදල් සමාගම් (උදාහරණ: අන්තර්ජාල බැංකුකරණය, ජංගම යෙදවුම්, පාරිභෝගික/ තෙවන පාර්ශ්ව ඒකාබද්ධ වීම් යනාදිය) ඇමුණුම II හි දක්වා ඇති අවම අවශ්‍යතාවලට අනුකූලව ආරක්ෂණ මෙහෙයුම් කේන්ද්‍රයක් ක්‍රියාත්මක කළ යුතුය.

5.8 **දත්ත අහිමි වීම වැළැක්වීම**

අ) බලපත්‍රලාභී මුදල් සමාගම් විසින් දත්ත කාන්දු වීමේ අවදානම අවම කිරීම සඳහා තොරතුරු තාක්ෂණ අංශයේ සම්මත දත්ත හානි වැළැක්වීමේ මෙවලම් ක්‍රියාත්මක කළ යුතුය. අදාළ ක්‍රියා පටිපාටියෙහි විෂය පථය මඟින් සමස්ථ බලපත්‍රලාභී මුදල් සමාගම සහ පාරිභෝගික දත්තවලට නිරාවරණය වන ඕනෑම තෙවන පාර්ශවීය සේවා සපයන්නන් සහ නියෝජිතයන් ආවරණය විය යුතුය.

ආ) තෙවන පාර්ශ්වීය සේවා සපයන්නන් සහ නියෝජිතයන් පිළිබඳව සලකා බැලීමේ දී, බලපත්‍රලාභී මුදල් සමාගම් එම සමාගම් විසින් නිශ්චිතව දක්වන ලද අවම අවශ්‍යතාවලට අනුකූලව දත්ත හානි වැළැක්වීමේ මෙවලම් ක්‍රියාත්මක කිරීම සඳහා ඔවුනට ඉඩ ලබා දෙනු ඇත.

ඈ) තෙවන පාර්ශ්වීය සේවා සපයන්නන් සහ නියෝජිතයන් විසින් ප්‍රමාණවත් දත්ත හානි වැළැක්වීමේ ක්‍රියාමාර්ග නිසි තැන්හි යොදා ගෙන ඇති බව තහවුරු කිරීමට බලපත්‍රලාභී මුදල් සමාගම් විසින් එවැනි ක්‍රියාත්මක කිරීම් පිළිබඳ සමාලෝචනයක් අවම වශයෙන් වාර්ෂිකව සිදු කළ යුතුය.

ඇ) තොරතුරු තාක්ෂණ අංශයේ ප්‍රමිතියෙන් යුත් දත්ත හානි වැළැක්වීමේ මෙවලම් සාධ්‍ය හෝ සුදුසු නොවන විට දී, බලපත්‍රලාභී මුදල් සමාගම් විසින් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවෙහි අනුමැතියට යටත්ව පාරිභෝගික දත්ත ආරක්ෂා කිරීම සඳහා විකල්ප පාලන භාවිත කළ යුතුය.

5.9 **තොරතුරු ආරක්ෂණය සම්බන්ධ සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීම සහ ප්‍රතිසාධනය**

5.9.1 සිද්ධි ප්‍රතිචාර සැලැස්ම

අ) සිද්ධි උත්සන්න වීම, පිළියම් යෙදීම, ප්‍රතිසාධනය සහ අභ්‍යන්තර සහ බාහිර සම්බන්ධිත පාර්ශවයන් සමඟ සන්නිවේදනය සඳහා ගනු ලබන ක්‍රියාමාර්ග ඇතුළුව, අධ්‍යක්ෂ මණ්ඩලය විසින් අනුමත කරන ලද යාවත්කාලීන සිද්ධි ප්‍රතිචාර සැලැස්මක් බලපත්‍රලාභී මුදල් සමාගමක් සතු විය යුතුය.

ආ) සයිබර් ආරක්ෂණ සිද්ධීන් සහ එයට පමණක් සීමා නොවූ සිද්ධීන්ද ඇතුළුව, පොදුවේ හැඳින්වෙන තොරතුරු ආරක්ෂණ සිද්ධි සමඟ ගනුදෙනු කිරීම සඳහා සිද්ධි ප්‍රතිචාර සැලැස්ම තුළ නිශ්චිත ක්‍රියාමාර්ග පැවතිය යුතුය.

5.9.2 සිද්ධි ප්‍රතිචාර සහ ප්‍රතිසාධන පරීක්ෂාව

බලපත්‍රලාභී මුදල් සමාගම්වල සිද්ධි සඳහා ප්‍රතිචාර දැක්වීමට තිබෙන සූදානම තීරණය කිරීම සඳහා හැකිතාක් සැබෑ ජීවිතයට සමීප අවස්ථා භාවිත කරමින් අවම වශයෙන් වාර්ෂිකව සිද්ධි ප්‍රතිචාර සහ ප්‍රතිසාධන හැකියාවන් පරීක්ෂා කළ යුතුය. එවැනි පරීක්ෂණයක ප්‍රතිඵල තොරතුරු ආරක්ෂණ කමිටුව මගින් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව ඔස්සේ අධ්‍යක්ෂ මණ්ඩලය වෙත වාර්තා කළ යුතුය.

5.10 **තොරතුරු ආරක්ෂණ පරීක්ෂණය**

5.10.1 පූර්ව තොරතුරු ආරක්ෂණ පරීක්ෂණය ක්‍රියාත්මක කිරීම

අ) විෂය පථය

i. පාරිභෝගික දත්තවලට නිරාවරණය වූ තොරතුරු පද්ධති සහ තීරණාත්මක තොරතුරු පද්ධති, පූර්ව තොරතුරු ආරක්ෂණ පරීක්ෂාවන්ට යටත් විය යුතුය. පාරිභෝගික දත්තවලට නිරාවරණය වූ ඕනෑම තොරතුරු පද්ධතියක් හෝ ඕනෑම තීරණාත්මක තොරතුරු පද්ධතියක් හෝ අනාගතයේ දී අවදානමට ලක් කළ හැකි වෙනත් ඕනෑම තොරතුරු පද්ධති ද පූර්ව තොරතුරු ආරක්ෂණ පරීක්ෂාවන්ට යටත් විය යුතුය.

ii. අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ නිර්දේශය මත රහස්‍ය පාරිභෝගික නොවන දත්තවලට නිරාවරණය වූ තීරණාත්මක නොවන තොරතුරු පද්ධති පූර්ව තොරතුරු ආරක්ෂණ පරීක්ෂාවට ලක් කිරීමේ අවශ්‍යතාව අධ්‍යක්ෂ මණ්ඩලය විසින් තීරණය කරනු ලැබිය යුතුය.

iii. මූලික ස්ථාපනය ක්‍රියාත්මක කිරීමට පෙර සහ සංශෝධන ක්‍රියාත්මක කිරීමට පෙර පූර්ව තොරතුරු ආරක්ෂණ පරීක්ෂාවන් සිදු කිරීම සිදු කළ යුතුය. අධ්‍යක්ෂ මණ්ඩලය විසින් අනුමත කරන ලද බැහැර කිරීමේ ප්‍රතිපත්තිය (Exclusion Policy) මත පදනම්ව සුළු සංශෝධනයන් පූර්ව තොරතුරු ආරක්ෂණ පරීක්ෂා ක්‍රියාත්මක කිරීමෙන් බැහැර කළ හැකිය. ඕනෑම නිශ්චිත සුළු සංශෝධනයක් බැහැර කිරීමට අවශ්‍ය වන අවස්ථාවක දී, තොරතුරු ආරක්ෂණ කමිටුවෙහි අනුමැතිය ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය වේ.

ආ) යම් ස්ථාපනයක් ක්‍රියාත්මක කිරීමට අදාළව පහත වර්ගවල පූර්ව ක්‍රියාත්මක කිරීමේ පරීක්ෂා පවත්වා ගෙන යා හැකිය:

i. ඕනෑම අනිෂ්ට හෝ සුරක්ෂිත නොවන කේතයක් අනාවරණය කර ගැනීමට ස්ථිතික යෙදවුම් ආරක්ෂණ පරීක්ෂාව (Static Application Security Testing) හෝ මූල කේත සමාලෝචනය (source code reviews).

ii. ප්‍රහාරකයෙකුට ගවේෂණය කළ හැකි යෙදවුම් මට්ටමේ දුර්වලතා අනාවරණය කිරීම සඳහා ගතික යෙදවුම් ආරක්ෂණ පරීක්ෂාව (Dynamic Application Security Testing).

iii. අභ්‍යන්තර දැඩි කිරීම් ප්‍රතිපත්ති සමඟ අනුකූල වීම තහවුරු කිරීම සඳහා පරිගණක සහ ජාලකරණ යටිතල පහසුකම් දැඩි කිරීම් පිළිබඳ තත්ත්ව සහතිකකරණ පරීක්ෂාව (Quality assurance testing), සහ

iv. පරිගණක සහ ජාලකරණ යටිතල පහසුකම් තුළ පවතින අවදානම් සහගත තත්ත්වයන් හඳුනා ගැනීම සඳහා යටිතල පහසුකම් තුළ පවතින අවදානම් සහගත තත්ත්වයන් සඳහා තක්සේරු කිරීම් (Infrastructure vulnerability assessments).

ඇ) තොරතුරු පද්ධති සංවර්ධනය සහ/හෝ ක්‍රියාත්මක කිරීම සඳහා වගකිව යුතු කණ්ඩායමෙන් ස්වාධීන වන කණ්ඩායමක් විසින් පූර්ව ක්‍රියාත්මක කිරීමේ පරීක්ෂණ සිදු කළ යුතුය.

ඈ) 5.10.1 (ආ) ට අනුව පූර්ව ක්‍රියාත්මක කිරීමේ පරීක්ෂණ පැවැත්වීමට නොහැකි නම්, බලපත්‍රලාභී මුදල් සමාගම් විසින් පවතින තොගයෙන් (off the shelf) ගනු ලබන මෘදුකාංග සැපයීමේ දී සුදුසු විකල්ප ආරක්ෂණ ඇගයීම් ක්‍රමවේද අනුගමනය කළ යුතුය.

ඉ) බාහිර විකුණුම්කරුවන් විසින් සපයනු ලබන තොරතුරු පද්ධති සලකා බැලීමේ දී 5.10.1 (ආ)(i) ට විකල්පයක් ලෙස, බලපත්‍රලාභී මුදල් සමාගම සහ තොරතුරු පද්ධති සැපයුම්කරු යන දෙපාර්ශ්වයටම අන්‍යෝන්‍යමය වශයෙන් පිළිගත හැකි, ස්වාධීන තෙවන පාර්ශ්වයක් විසින් සපයනු ලබන සහතිකකරණයක් මත බලපත්‍රලාභී මුදල් සමාගම් විශ්වාසය තැබිය යුතුය.

ඊ) අදාළ පූර්ව ක්‍රියාත්මක කිරීමේ පරීක්ෂණ සම්පූර්ණ කිරීමෙන් අනතුරුව මූල කේතය, නිෂ්පාදන පරිසරයකට මාරු වීමේදී අනිෂ්ට කේතය නික්ෂේපනය නොකෙරෙනු ඇති බවට තහවුරු කිරීම සඳහා බලපත්‍රලාභී මුදල් සමාගම් තොරතුරු තාක්ෂණ අංශයේ සම්මත පාලනයන් ස්ථාපනය කළ යුතුය.

5.10.2 අවදානම් තක්සේරු කිරීම්

අ) තීරණාත්මක තොරතුරු පද්ධති සහ පාරිභෝගික දත්තවලට නිරාවරණය වී පවතින තොරතුරු පද්ධති අවම වශයෙන් අර්ධ වාර්ෂිකව හෝ තොරතුරු තාක්ෂණ යටිතල පහසුකම් සහ පද්ධති සංශෝධනවලට වෙනස්කමක් සිදු කරන විටෙක දී අවදානම් තක්සේරු කිරීම්වලට යටත් විය යුතුය.

ආ) යටිතල පහසුකම් සහ යෙදවුම්වල ඇති වන අවදානම් තත්ත්වයන් යන කරුණු දෙකම කෙරෙහි අවදානම් තක්සේරු කිරීමේ දී අවධානය යොමු කළ යුතුය.

ඇ) අවදානම් තක්සේරු කිරීම් නිෂ්පාදන පරිසරයන් මත සිදු කළ යුතුය.

ඈ) බලපත්‍රලාභී මුදල් සමාගමෙහි අභ්‍යන්තර තොරතුරු ආරක්ෂක නිළධාරීන් හෝ බාහිර විශේෂඥයන් විසින් අවදානම් තක්සේරු කිරීම් සිදු කළ යුතුය.

ඉ) හඳුනාගත් අවදානම් තත්ත්වයන් සඳහා තොරතුරු ආරක්ෂක කමිටුව විසින් අනුමත කරනු ලබන කාල පරිච්ඡේදයක් තුළ දී පිළියම් යෙදිය යුතුය.

5.10.3 විනිවිදුම් පරීක්ෂාව (Penetration Testing)

අ)
i. සැබෑ ලොව ශෛලීය ප්‍රහාරවලට ඔරොත්තු දීමට පරීක්ෂා කළ තොරතුරු පද්ධති සතු හැකියාව;
ii. පරීක්ෂාවට ලක් කළ තොරතුරු පද්ධති සාර්ථකව බිඳ හෙළීම සඳහා ප්‍රහාරකයෙකු සතු විය යුතු සංකීර්ණභාවයෙහි සහ අඛණ්ඩතාවයෙහි අවශ්‍ය වන මට්ටම;
iii. එවැනි ප්‍රහාර හඳුනා ගැනීමට සහ සුදුසු ලෙස ප්‍රතිචාර දැක්වීම සඳහා බලපත්‍රලාභී මුදල් සමාගමෙහි තොරතුරු ආරක්ෂණය, මෙහෙයුම් සහ නායකත්ව කණ්ඩායම්වල හැකියාව;
iv. අනාගතයේ දී එවැනි තර්ජන අවම කර ගැනීම සඳහා අවශ්‍ය වන ඕනෑම වැඩි දියුණු කිරීමක්;

තීරණය කිරීම සඳහා බලපත්‍රලාභී මුදල් සමාගම් විසින් ස්වාධීන බාහිර විශේෂඥයෙකු උපයෝගී කර ගනිමින් විනිවිදුම් පරීක්ෂාව සිදු කළ යුතුය.

ආ) තීරණාත්මක තොරතුරු පද්ධති, පාරිභෝගික දත්ත වෙත නිරාවරණය වූ තොරතුරු පද්ධති සහ බලපත්‍රලාභී මුදල් සමාගම් සමඟ පවතින පාරිභෝගික දත්තවල සුරක්ෂිතාගාර, නියෝජිතයන් සහ තෙවන පාර්ශ්ව සේවා සපයන්නන් අවම වශයෙන් වාර්ෂිකව, ස්වාධීන බාහිර විනිවිදුම් පරීක්ෂා විශේෂඥයෙකු විසින් සිදු කරනු ලබන විනිවිදුම් පරීක්ෂාවලට යටත් විය යුතුය. විනිවිදුම් පරීක්ෂණ පැවැත්වීම පිළිබඳ දක්වන ලද මාර්ගෝපදේශයක් III වන ඇමුණුමෙහි දී ඇත.

ඇ) පරිණත සහ තම ව්‍යාපාර කටයුතුවලට සහාය ලබා දීමට සංකීර්ණ තාක්ෂණයන් සතු බලපත්‍රලාභී මුදල් සමාගම්වලට විනිවිදුම් පරීක්ෂණවල දීර්ඝ කිරීමක් ලෙස රතු කණ්ඩායම් අභ්‍යාසයන් (Red team exercises) මෙහෙයවිය හැකිය. එවැනි රතු කණ්ඩායම් අභ්‍යාසයන් සිදු කළ හැක්කේ කෙසේද යන්න පිළිබඳව පෙන්නුම් කරන මාර්ගෝපදේශයක් ඇමුණුම IV හි දී දක්වා ඇත.

5.11 තොරතුරු ආරක්ෂණ පුහුණුකරණය සහ සහතිකකරණය

5.11.1 අධ්‍යක්ෂ මණ්ඩලය පුහුණුකරණය සහ දැනුවත් කිරීම

අ) බලපත්‍රලාභී මුදල් සමාගම් විසින් පහත අවශ්‍යතාවලට අනුකූලව, අධ්‍යක්ෂ මණ්ඩලය සඳහා තොරතුරු ආරක්ෂණය සහ තාක්ෂණික අවදානම් කළමනාකරණය පිළිබඳව පරිපූර්ණ වාර්ෂික පුහුණුවක් සහ දැනුවත් කිරීමේ වැඩසටහනක් ක්‍රියාත්මක කළ යුතුය.

i. තොරතුරු ආරක්ෂණයේ ප්‍රමාණවත් බව හා සඵලදායීත්වය සහ බලපත්‍රලාභී මුදල් සමාගමේ තාක්ෂණික අවදානම් කළමනාකරණ ප්‍රතිපත්ති සහ ක්‍රියාවලි සම්බන්ධව අධ්‍යක්ෂ මණ්ඩලයට ඵලදායී සාර්ථක අධීක්ෂණයක් ඇති කිරීම එවැනි වැඩසටහනක අරමුණ විය යුතුය.

ii. මෙම නියාමන රාමුවෙහි අවශ්‍යතාවන්ට අනුකූලව අධ්‍යක්ෂ මණ්ඩලයේ සහ අධ්‍යක්ෂ මණ්ඩල කමිටුවල වගකීම් සහ තොරතුරු ආරක්ෂණය සහ තාක්ෂණික අවදානම් කළමනාකරණයට අදාළ වන අනෙකුත් නීති සහ රෙගුලාසි ද එවැනි වැඩසටහන් ඔස්සේ ආවරණය විය යුතුය.

iii. එවැනි පුහුණු කිරීමක්, අවම වශයෙන් වාර්ෂික ව්‍යුහගත පුහුණු කිරීමේ වැඩසටහනක් සහ සෑම වසරක් පාසාම තොරතුරු ආරක්ෂණ සහ තාක්ෂණික අවදානම් කළමනාකරණ විශේෂඥයන් විසින් මෙහෙය වනු ලබන දැනුවත් කිරීමේ සැසි එකක් හෝ ඊට වැඩි ගණනකින් සමන්විත විය යුතුය.

iv. බලපත්‍රලාභී මුදල් සමාගමේ අධ්‍යක්ෂ මණ්ඩල ලේකම් විසින් පුහුණුකරණය සහ දැනුවත් කිරීම සම්බන්ධව ඉහත අවශ්‍යතාවන් සමඟ එම සමාගමේ අධ්‍යක්ෂ මණ්ඩලයෙහි අනුකූල වීම තහවුරු කරනු ලැබිය යුතුය.

5.11.2 කාර්ය මණ්ඩලය සඳහා තොරතුරු ආරක්ෂණ දැනුවත් කිරීමේ පුහුණුව සහ සහතිකකරණ අවශ්‍යතාව

අ) බලපත්‍රලාභී මුදල් සමාගම් විසින් පහත අවශ්‍යතාවන්ට අනුකූලව, තීරණාත්මක තොරතුරු පද්ධති, පාරිභෝගික දත්ත, රහස්‍ය පාරිභෝගික නොවන දත්තවලට නිරාවරණය වූ හෝ අනාගතයේ දී නිරාවරණය විය හැකි, බලපත්‍රලාභී මුදල් සමාගමෙහි කාර්ය මණ්ඩලය, නියෝජිතවරුන් සහ තෙවන පාර්ශ්ව සේවා සපයන්නන් තොරතුරු ආරක්ෂණය පිළිබඳ පුහුණුවක් ලැබූ සහ සහතික ලත් පිරිස් බවට තහවුරු කරනු ලැබිය යුතුය.

i. බලපත්‍රලාභී මුදල් සමාගමෙහි තොරතුරු ආරක්ෂණ ප්‍රතිපත්ති සහ ක්‍රියාමාර්ග මත පදනම්ව තොරතුරු ආරක්ෂණ දැනුවත් කිරීම් පුහුණු කිරීමේ වැඩසටහනක් අවශ්‍ය පුද්ගලයන් විසින් සම්පූර්ණ කළ යුතුය.

ii. 5.11.2 අ (ස) ට අනුව එවැනි වැඩසටහන් පුහුණුව, ලබන්නාගේ තොරතුරු ආරක්ෂණ වගකීම්වලට සරිලන ඒවා විය යුතු අතර, බලපත්‍රලාභී මුදල් සමාගමෙහි තොරතුරු ආරක්ෂණ ප්‍රතිපත්ති යාවත්කාලීන කෙරෙන සෑම අවස්ථාවක දී ම එය ද නිතිපතා යාවත්කාලීන කළ යුතුය.

iii. අවශ්‍ය පුද්ගලයන් විසින් තොරතුරු ආරක්ෂණ දැනුවත් කිරීම් පුහුණු කිරීම පදනම්ව අභ්‍යන්තර සහතිකකරණ පරීක්ෂණයක් අවම වශයෙන් වාර්ෂිකව සම්පූර්ණ කළ යුතුය.

ආ) නියෝජිතයන් සහ තෙවන පාර්ශ්වීය සේවා සපයන්නන් විසින් ප්‍රමාණවත් සහ සැසඳිය හැකි තොරතුරු ආරක්ෂණ දැනුවත් කිරීමේ ක්‍රියාමාර්ග ක්‍රියාත්මක කරනු ලැබ ඇති නම්, අධ්‍යක්ෂ මණ්ඩලය විසින් එවැනි නියෝජිතයන් සහ තෙවන පාර්ශ්වීය සේවා සපයන්නන් 5.11.2 අ (i) හි අවශ්‍යතාවලින් බැහැර කළ යුතුය.

6. තොරතුරු පද්ධතිවල උපයෝජ්‍යතාවය සහ ආපදා ප්‍රතිසාධනය

6.1 **විෂය පථය**

6.2 සිට 6.5 දක්වා නිශ්චිතව දක්වා ඇති අවශ්‍යතා තීරණාත්මක තොරතුරු පද්ධතිවලට අදාළ විය යුතුය.

6.2 **පද්ධති උපයෝජ්‍යතාව (System Availability)**

අ) බලපත්‍රලාභී මුදල් සමාගම් විසින් තීරණාත්මක තොරතුරු පද්ධති සඳහා ඉහළ මට්ටමකින් පද්ධති උපයෝජ්‍යතාවයක් ළඟා කර ගැනීම තහවුරු කළ යුතුය.

ආ) අධ්‍යක්ෂ මණ්ඩලය විසින් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුවෙහි නිර්දේශය මත එක් එක් තීරණාත්මක තොරතුරු පද්ධතිය සඳහා පද්ධති උපයෝජ්‍යතා ඉලක්ක පිහිටු විය යුතුය.

ඇ) තීරණාත්මක තොරතුරු පද්ධති සඳහා පද්ධති උපයෝජ්‍යතා ඉලක්ක අත්පත් කර ගැනීම අධ්‍යක්ෂ මණ්ඩලය විසින් අධීක්ෂණය කරන බවට සහ ඔවුන් වෙත එය වාර්තා කරන බවට අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව තහවුරු කළ යුතුය.

6.3 **ආපදා ප්‍රතිසාධන (Disaster Recovery) සැකැස්ම**

අ) බලපත්‍රලාභී මුදල් සමාගම් විසින් පහත අවම අවශ්‍යතාවන්ට අනුකූලව, අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුවේ නිර්දේශය මත අධ්‍යක්ෂ මණ්ඩලය විසින් තීරණය කරන ලද ප්‍රතිසාධන කාල අරමුණු (Recovery Time Objectives) සහ ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණු (Recovery Point Objectives) සමඟ තීරණාත්මක තොරතුරු පද්ධති සඳහා ආපදා ප්‍රතිසාධන සැකැස්මක් පවතින බවට තහවුරු කළ යුතුය.

i. බලපත්‍රලාභී මුදල් සමාගමෙහි තීරණාත්මක තොරතුරු පද්ධති සඳහා පැය 6කට අඩු ප්‍රතිසාධන කාල අරමුණු; සහ
ii. ශුන්‍ය හෝ ශුන්‍යයට ආසන්න ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණු (එනම්, ආපදාවක දී දත්ත හානියක් සිදු නොවීම)

6.4 **ආපදා ප්‍රතිසාධන සක්‍රීය කිරීම**

අ) අධ්‍යක්ෂ මණ්ඩලය විසින් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුවේ සහ තොරතුරු ආරක්ෂණ කමිටුවෙහි නිර්දේශයන් මත පදනම්ව එක් එක් තීරණාත්මක තොරතුරු පද්ධතිය සඳහා ආපදා ප්‍රතිසාධන සක්‍රීය කිරීමේ ක්‍රියාරම්භකයන් පිහිටුවිය යුතුය.

ආ) එවැනි සක්‍රීය කිරීමේ ක්‍රියාරම්භකයන් මගින් 6.3 හි නිශ්චිතව දක්වා ඇති ප්‍රතිසාධන කාල අරමුණුවලට අනුකූලව ආපදා ප්‍රතිසාධන සැකැස්ම සක්‍රීය කිරීම සඳහා ප්‍රමාණවත් කාලයක් තහවුරු කළ යුතුය.

6.5 **ආපදා ප්‍රතිසාධන පරීක්ෂාව**

අ) අවම වශයෙන් වසරකට එක් දිනයක දී හෝ ආපදා ප්‍රතිසාධන යටිතල පහසුකම් භාවිත කරමින් සියලු තීරණාත්මක තොරතුරු පද්ධති ක්‍රියාත්මක කිරීම මගින් ආපදා ප්‍රතිසාධන ක්‍රියා පිළිවෙල පරීක්ෂාවට ලක් කළ යුතුය.

ආ) 6.5 (අ) ට අනුව ආපදා ප්‍රතිසාධන යටිතල පහසුකම් පරීක්ෂා කිරීමට අමතරව, විවිධ ආපදා තත්ත්වයන් යටතේ අවශ්‍ය ප්‍රතිසාධන කාල අරමුණු සහ ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණු සාක්ෂාත් කර ගැනීම සහ අවශ්‍ය වූ විට නිසි නිවැරදි කිරීමේ ක්‍රියාමාර්ග ගැනීම සඳහා බලපත්‍රලාභී මුදල් සමාගම් සතු හැකියාව තීරණය කිරීමට අධ්‍යක්ෂ මණ්ඩලයට හැකියාව ලබා දීම සඳහා ආපදා ප්‍රතිසාධන අනුකරණවල වාර්ෂික චක්‍රයක් ක්‍රියාත්මක කළ යුතුය.

7. කාර්යමණ්ඩල නිපුණත්ව අවශ්‍යතා

7.1 අ) අවශ්‍ය සුදුසුකම්වලින් සමන්විත සේවකයන් තොරතුරු ආරක්ෂණය, තාක්ෂණික අවදානම් කළමනාකරණය සහ අභ්‍යන්තර විගණන කාර්යයන්වල සේවයෙහි නිරත වී සිටින බවට බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතුය. මීට අමතරව, තෙවන පාර්ශ්වීය සේවා සපයන්නන්ගේ කාර්යමණ්ඩල සාමාජිකයන්ට ද එම එවැනි සුදුසුකම් තිබිය යුතුය. පිළිගත් සුදුසුකම්, ආදාළ භූමිකාවන් සඳහා ආයතන පිළිබඳ මඟපෙන්වීමක් V වන ඇමුණුමෙහි දක්වා ඇත.

ආ) බලපත්‍රලාභී මුදල් සමාගමකට 7.1 (අ) වන වගන්තියෙහි අවශ්‍යතා සමඟ අනුකූල වීමට නොහැකි වන අවස්ථාවේ දී, අධ්‍යක්ෂ මණ්ඩලය විසින් අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවෙහි නිර්දේශයන්ට යටත්ව තොරතුරු ආරක්ෂණය සහ තාක්ෂණික අවදානම් කළමනාකරණයේ සුදුසු අත්දැකීම් සහ කුසලතා සඳහා දක්වන සුදුසුකම් ආදේශ කිරීමට නියම කළ යුතුය.

8. තෙවන පාර්ශ්වීය සේවා සපයන්නන් කළමනාකරණය

8.1 අධ්‍යක්ෂ මණ්ඩලය සහ ජ්‍යෙෂ්ඨ කළමනාකාරීත්වය විසින් තීරණාත්මක තාක්ෂණ කාර්යයන් සහ පද්ධති සඳහා තෙවන පාර්ශ්ව සේවා සපයන්නන් සේවයේ යෙදවීමේ දී ඵලදායී අධීක්ෂණයක් සිදු කිරීම සහ ආශ්‍රිත අවදානම්වලට පිළියම් යෙදීමට කටයුතු කළ යුතුය. ස්වාධීන තක්සේරු ලබා ගැනීම් ඇතුළුව, තෙවන පාර්ශ්වීය සේවා සපයන්නන් යොදා ගැනීම, තාක්ෂණ කාර්යයන් සහ පද්ධතිවල ආරක්ෂාව සහ විශ්වසනීයත්වය සඳහා බලපත්‍රලාභී මුදල් සමාගමෙහි මූලික වගවීම් සහ වගකීම් කිසිදු ආකාරයකින් අවම කිරීම හෝ පැහැර හැරීම සිදු නොකරයි.

8.2 තෙවන පාර්ශ්ව සේවා සපයන්නෙකු විසින් සිදු කරනු ලබන ඕනෑම පාරිභෝගික දත්තවල රහස්‍යභාවය උල්ලංඝනය කිරීමක් සඳහා අධ්‍යක්ෂ මණ්ඩලය වගකිය යුතුය.

8.3 **තෙවන පාර්ශ්ව සේවා සපයන්නන් ඇගයීම**

අ) බලපත්‍රලාභී මුදල් සමාගම් තෙවන පාර්ශ්ව සේවා සපයන්නන් සේවයට පත් කර ගැනීමට පෙර, ඔවුන්ගේ නිපුණත්වය, පද්ධති යටිතල පහසුකම් සහ මූල්‍ය ශක්‍යතාවය පිළිබඳ නිසි යථායෝගීතා පරීක්ෂණයක් සිදු කළ යුතුය.

ආ) මීට අමතරව, පහත නිශ්චිත අවදානම් කළමනාකරණය කිරීමේ දී තෙවන පාර්ශ්ව සේවා සපයන්නන්ගේ හැකියාවන් සම්බන්ධව ඇගයීමක් සිදු කළ යුතුය.

i. ගනුදෙනුකාර සහ ප්‍රතිපාර්ශවවල තොරතුරු අනවසර ලෙස හෙළිදරව් කිරීම ඇතුළුව දත්ත කාන්දු වීම්.
ii. ධාරිතා කාර්යසාධනය ඇතුළුව සේවාවලට බාධා වීම්.
iii. සැකසුම් දෝෂ.
iv. භෞතික ආරක්ෂණ උල්ලංඝනය කිරීම්.
v. සයිබර් තර්ජන.
vi. ප්‍රධාන පුද්ගලයන් මත අධික ලෙස යැපීම.
vii. මූල්‍ය ආයතනය හෝ එහි ගනුදෙනුකරුවන්ට අදාළ රහස්‍ය තොරතුරු සම්ප්‍රේෂණය කිරීම, සකස් කිරීම හෝ ගබඩා කිරීමේ දී සිදු කරන ලද අනිසි පරිහරණය කිරීම්.
viii. සංකේන්ද්‍රණ අවදානම.

ඇ) තෙවන පාර්ශ්වීය සේවා සපයන්නන් විසින් 8.3 (ආ) හි ඉස්මතු කර ඇති අවදානම් පිළිබිඹු කරන අවස්ථාවක දී, එවැනි අවදානම් අවම කිරීම සඳහා නිසි ක්‍රියාමාර්ග ගනු ලබන බවට බලපත්‍රලාභී මුදල් සමාගම විසින් තහවුරු කළ යුතුය.

8.4 **සේවා සැපයීමේ ගිවිසුම්**

අ) සේවා සපයන තෙවන පාර්ශවයක් සමඟ කටයුතු කිරීමේ දී සේවා සැපයීමේ ගිවිසුමකට එළඹීම සඳහා බලපත්‍රලාභී මුදල් සමාගම් කටයුතු කළ යුතු වේ. අවම වශයෙන්, සේවා සැපයීමේ ගිවිසුමක පහත සඳහන් කරුණු අඩංගු විය යුතු වේ.

i. ශ්‍රී ලංකා මහ බැංකුව හෝ බලපත්‍රලාභී මුදල් සමාගමක කිසියම් කටයුත්තක් හෝ ආයතනයක් අධීක්ෂණය කිරීම සඳහා බලපත්‍රලාභී මුදල් සමාගම විසින් පත් කරනු ලැබූ ඕනෑම පාර්ශවයක් සඳහා ප්‍රවේශ අයිතිය. කළමනාකරණ තොරතුරු සහ සියලුම උපදේශන සහ තීරණ ගැනීමේ ක්‍රියාවලියේ සටහන් ඇතුළත්ව බලපත්‍රලාභී මුදල් සමාගමේ ඕනෑම වාර්තාවක්, ලිපි ගොනුවක් හෝ දත්ත සඳහා ප්‍රවේශ වීම මෙහි ඇතුළත් විය යුතුය.

ii. සේවා සපයන තෙවන පාර්ශවය සහ බලපත්‍රලාභී මුදල් සමාගම වෙත සපයනු ලබන සේවාවන් හා සම්බන්ධ සේවා සපයන තෙවන පාර්ශවයේ කාර්ය මණ්ඩලය පරීක්ෂා කිරීම සඳහා ශ්‍රී ලංකා මහ බැංකුව සතු අයිතිය.

iii. බලපත්‍රලාභී මුදල් සමාගම වෙත සපයනු ලබන සේවාවන් සම්බන්ධයෙන් අධ්‍යක්ෂවරයා විසින් ඉල්ලුම් කරනු ලබන කිසියම් තොරතුරක් හෝ දත්ත ලබා දීම සඳහා සේවා සපයන තෙවන පාර්ශවය කටයුතු කළ යුතු බව.

iv. බලපත්‍රලාභී මුදල් සමාගම වෙත සපයනු ලබන සේවාවන් සම්බන්ධයෙන් කිසියම් තොරතුරක් හෝ දත්ත ඉල්ලුම් කර ලබා ගැනීම සඳහා ශ්‍රී ලංකා අධිකරණය සතු අයිතිය.

v. පාරිභෝගික දත්ත සාධාරණව සහ බලපත්‍රලාභී මුදල් සමාගම විසින් දත්ත හුවමාරු කර ගනු ලැබූ අරමුණ සඳහා පමණක් භාවිත කිරීම, සේවා සපයන තෙවන පාර්ශවය තහවුරු කළ යුතු වේ.

vi. සේවා සපයන තෙවන පාර්ශවය සතුව ඇති සියලුම පාරිභෝගික දත්ත සහ රහස්‍ය පාරිභෝගික නොවන දත්ත, ගිවිසුම් කාල සීමාව අවසානයේ දී පෙර නිශ්චය කරන ලද කාලයක් තුළ සම්පූර්ණයෙන් මකා ඉවත් කළ යුතුය.

vii. මෙම විධානයන්ගේ සඳහන් අභ්‍යන්තර විගණන අවශ්‍යතා සහ තොරතුරු ආරක්ෂණය පරීක්ෂා කිරීමේ අවශ්‍යතා සඳහා සේවා සපයන තෙවන පාර්ශව පහසුකම් සැලසිය යුතු වේ.

viii. සැලකිය යුතු කාලයකට පූර්වයෙන් බලපත්‍රලාභී මුදල් සමාගම වෙත පෙර දැනුම් දීමක් කිරීම සඳහා සේවා සපයන්නා සහ උප-කොන්ත්‍රාත්කරුවන්ට අවශ්‍යතා.

ix. සේවා සපයන්නා විසින් අදාළ නීති යටතේ රහස්‍ය විධිවිධාන සමඟ අනුකූල වන බවට ලිඛිත එකඟතාවයක් පැවතීම. සේවා සපයන්නාගේ කටයුතු අවසන් වූ පසුව ද ගිවිසුමේ නිශ්චය කරන ලද රහස්‍යභාවය සඳහා වන ප්‍රතිපාදන හා බැඳී පවතින බව සේවා සැපයීමේ ගිවිසුමේ තවදුරටත් පැහැදිලිව සඳහන් කළ යුතු වේ.

x. ආපදාවකින් පසු යථා තත්ත්වයට පත් කිරීම සඳහා සැලසුම් සහ උපස්ථා (backup) හැකියාව.

xi. බාධාවකින් තොරව සේවා සැපයීම සඳහා තෙවන පාර්ශවය විසින් යොමු කරන ලද කාර්ය මණ්ඩලය කැපවීමෙන් කටයුතු කිරීම තහවුරු කිරීම සහ කිසියම් වෙනසක් වේ නම්, ඒ පිළිබඳව ප්‍රමාණවත් කාල සීමාවක් තුළ දැනුම් දීම.

xii. සේවා සපයන තෙවන පාර්ශවය විසින් පාරිභෝගිකයන්ගේ දත්තවල රහස්‍යභාවය උල්ලංඝනය කර ඇත්නම්, ඒ සඳහා වන්දි ලබා දීමේ යාන්ත්‍රණය සහ නිවැරදි කිරීමේ ක්‍රියාපටිපාටිය.

xiii. තීරණාත්මක පද්ධති සඳහා පිවිසීමට ඇති හැකියාව.

xiv. සේවා සපයන්නා සේවයෙන් ඉවත් වුවහොත් හෝ සේවය අත්හිටුවහොත් හෝ ව්‍යාපාර කටයුතු අඛණ්ඩව සිදු කරගෙන යාම තහවුරු කිරීම සඳහා වන සැලසුම් සකස් කිරීම.

ආ) තෙවන පාර්ශවීය සේවා සපයන්නන් හා එළඹී ඇති ගිවිසුමේ ස්වභාවය සහ සංකීර්ණත්වය හේතුවෙන් සේවා සැපයීමේ ගිවිසුමේ ඉහත 8.4 (අ) හි දක්වා ඇති කොන්දෙසි ඇතුළත් කිරීමට බලපත්‍රලාභී මුදල් සමාගම අපොහොසත් වන අවස්ථාවකදී, එවැනි කොන්දේසි සේවා සැපයීමේ ගිවිසුමෙන් ඉවත් කිරීම, අධ්‍යක්ෂ මණ්ඩල ඒකාබද්ධ අවදානම් කළමනාකරණ කමිටුව සහ තොරතුරු ආරක්ෂණ කමිටුවේ නිර්දේශ මත අධ්‍යක්ෂ මණ්ඩලය විසින් සම්මත කළ යුතුය.

8.5 සපයනු ලබන සේවාවන් සම්බන්ධයෙන් නවතම ආරක්ෂක සහ තාක්ෂණික දියුණුවන් සැලකිල්ලට ගනිමින් තෙවන පාර්ශවයන් සමග සේවා සැපයීමේ ගිවිසුම් කාලීනව සමාලෝචනය කිරීමට ඇති හැකියාව බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතු වේ.

8.6 මෙම විධානයන්ගේ නියම කර ඇති සියලුම අදාළ නියාමන අවශ්‍යතා සමග තෙවන පාර්ශවීය සේවා සපයන්නන් අනුකූල වන බවට බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතු වේ.

8.7 තෙවන පාර්ශවීය සේවා සපයන්නන් භාරයේ ඇති දත්ත කාලීනව නැවත ලබා ගැනීමට හැකි බව බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතු වේ. සයිබර් අවකාශයේ සිදුවන ගැටලුවක දී බලපත්‍රලාභී මුදල් සමාගම වෙත කඩිනමින් දැනුම් දීම්, බලපත්‍රලාභී මුදල් සමාගම සහ අනිකුත් නියාමන ආයතන වෙත කාලෝචිත යාවත්කාලීන කිරීම සඳහා පහසුකම් සැලසීම සඳහා තෙවන පාර්ශවීය සේවා සපයන්නන් හා පැහැදිලිව නිර්වචනය කරන ලද සැලසුම් සකස් කර තිබෙන බවට බලපත්‍රලාභි මුදල් සමාගම් තහවුරු කළ යුතු වේ.

8.8 තෙවන පාර්ශවීය සේවා සපයන්නන් විසින් බලපත්‍රලාභී මුදල් සමාගම්හී දත්ත ගබඩා කිරීමේ දී එම දත්ත අවම වශයෙන් තාර්කික අයුරින් අනෙකුත් සේවාදායකයන්ගේ දත්තවලින් වෙන් කර ඇති බවට බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතු වේ. බලයලත් පරිශීලකයන් වෙත සපයා ඇති ප්‍රවේශයන් සම්බන්ධයෙන් නිසි පාලනයන් සහ කලින් කලට සමාලෝචනයන් කළ යුතුය.

8.9 තෙවන පාර්ශවීය සේවා සපයන්නන් විසින් ඔවුන්ගේ සේවාව සැපයීමට අසමත් වූ අවස්ථාවක දී හෝ කාර්ය සාධනය සතුටුදායී නොවන අවස්ථාවක දී නිසි අයුරින් එම කාර්යයෙන් ඉවත් වීම සඳහා සේවා සපයන තෙවන පාර්ශව විසින් පවත්වාගෙන යන තීරණාත්මක පද්ධති ශක්තිමත්ව යථා තත්ත්වයට පත් කිරීම සහ නැවත ආරම්භ කිරීමේ හැකියාව, බලපත්‍රලාභී මුදල් සමාගම් තහවුරු කළ යුතුය.

9. වලාකුළු සේවාවන් (Cloud Services)

9.1 වලාකුළු සේවාවන්ට අනන්‍ය වූ අන්තර්ජාලය හරහා බහු විධි තැනැත්තන් සමග සම්පත් සහ සේවා හුවමාරු කර ගැනීම සැලකිල්ලට ගනිමින් වලාකුළු සේවාවන් ප්‍රතිග්‍රහණය කිරීමේ අන්තර්ගත අවදානම බලපත්‍රලාභී මුදල් සමාගම් පැහැදිලිව අවබෝධ කළ ගත යුතුය.

9.2 **විස්තීරණ අවදානම් තක්සේරුකරණය**

අ) වලාකුළු සේවාවන් ප්‍රතිග්‍රහණය කිරීමට පෙර බලපත්‍රලාභී මුදල් සමාගම් විසින් අවදානම් තක්සේරු කිරීමක් සිදු කළ යුතුය. පහත සඳහන් කරුණු හා සම්බන්ධ අවදානම් ආමන්ත්‍රණය කිරීම සඳහා මෙම තක්සේරුවෙන් කටයුතු කළ යුතුය.

i. යෙදවීම් ආකෘතියේ සංකීර්ණත්වය.
ii. පවතින පද්ධති, වලාකුළු සේවාව වෙත සංක්‍රමණය කිරීම.
iii. වලාකුළු සේවාව සඳහා යටිතල පහසුකම් පවතින ස්ථානය.
iv. බහු විධි තැනැත්තන් සඳහා සේවා සැපයීම සහ දත්ත අන්තර් හුවමාරු වීමේ හැකියාව.
v. සේවා සපයන්නා මත යැපීමට සිදුවීම (Vendor lock-in) සහ යෙදවුම් සුවහනීයතාවය (application portability) හෝ අන්තර් ක්‍රියාකාරීත්වය (Interoperability).
vi. ඉහළ මට්ටමේ දත්ත සහ තාක්ෂණික පද්ධති ආරක්ෂණයක් තහවුරු කිරීම සඳහා වලාකුළු සේවාවන්ගේ යටිතල පහසුකම්හි ආරක්ෂක සැකසුම් අභිරුචිකරණය කිරීමට ඇති හැකියාව.
vii. වලාකුළු සේවා සපයන්නන් හරහා සයිබර් ප්‍රහාරයන්ට නිරාවරණය වීම.
viii. සේවය අවසන් කිරීමෙන් පසුව මූල්‍ය ආයතනයේ දත්ත ආරක්ෂා කිරීමට ඇති හැකියාව ඇතුළුව වලාකුළු සේවා සපයන්නෙකුගේ සේවය අවසන් කිරීම.
ix. සේවා සපයන්නාගේ වගකීම්, සීමා සහ බැඳීම් වෙන් කර දැක්වීම.
x. අඛණ්ඩ පදනමක් මත වලාකුළු සේවා පහසුකම් සම්බන්ධයෙන් නියාමන අවශ්‍යතා සහ ජාත්‍යන්තර ප්‍රමිතීන් සපුරාලීමට ඇති හැකියාව.

ආ) ඉහත 9.2 (අ) හි මතු කර දක්වා ඇති අවදානම් වලාකුළු සේවා සපයන්නා විසින් පෙන්නුම් කරනු ලබන අවස්ථාවක දී, එවැනි අවදානම් අවම කර ගැනීම සඳහා අවශ්‍ය පියවර නිසි අයුරින් ක්‍රියාත්මක කිරීමට බලපත්‍රලාභී මුදල් සමාගම් කටයුතු කළ යුතුය.

9.3 පහත සඳහන් කරුණු ප්‍රමාණවත් ලෙස ආමන්ත්‍රණය සඳහා තෝරාගත් වලාකුළු ආකෘතිය කෙතරම් දුරකට කටයුතු කරන්නේ දැයි බලපත්‍රලාභී මුදල් සමාගම් තක්සේරු කළ යුතුය.

අ) භූගෝලීය බලපෑම්වලින් වියුක්ත බව (Geographical redundancy)

ආ) අඛණ්ඩව ක්‍රියාත්මක වීමේ හැකියාව (High availability)

ඇ) පරිමාණීකෘතබව (Scalability)

ඈ) සුවහබව (Portability)

ඉ) අන්තර් ක්‍රියාකාරීත්වය (Interoperability)

ඊ) සිදු විය හැකි අන්තර්ජාල දෝෂ වලින් ආරක්ෂා වීම සඳහා සුදුසු විකල්ප අන්තර්ජාල ප්‍රවේශ ඇතුළුව ශක්තිමත්ව යථා තත්ත්වයට පත්වීම සහ නැවත ආරම්භ කිරීමේ හැකියාව

9.4 අවම වශයෙන්, පහත සඳහන් ක්ෂේත්‍රයන් ඇතුළුව වලාකුළු සේවා සපයන්නන් ස්වාධීන, ජාත්‍යන්තර වශයෙන් පිළිගත් සහතිකයක් ලබා ඇති දැයි බලපත්‍රලාභී මුදල් සමාගම් තක්සේරු කළ යුතුය.

අ) පරිශීලක දත්ත සංකේතනය (encryption) සහ විකේතනය (decryption) කිරීම සඳහා භාවිත කළ හැකි ක්‍රිප්ටෝග්‍රැපික් මොඩියුල (cryptographic modules) ඇතුළුව තොරතුරු ආරක්ෂණ කළමනාකරණ රාමුව.

ආ) භාවිත වන, ගබඩා කර ඇති සහ සංක්‍රාන්ති තත්ත්වයේ ඇති ගෙවීම් ගනුදෙනු දත්ත ඇතුළුව පාරිභෝගිකයා සහ ප්‍රති-පාර්ශවය හෝ හිමිකාර වාණිජ තොරතුරු ආරක්ෂා කිරීම සඳහා වලාකුළු සේවාවට විශේෂිත ආරක්ෂක පාලනයන්.

9.5 කිසියම් වලාකුළු සේවාවක් භාවිත කිරීමට පෙර බලපත්‍රලාභී මුදල් සමාගම් විසින් තීරණාත්මක සහ තීරණාත්මක නොවන පද්ධති වෙන වෙනම හඳුනා ගැනීමට කටයුතු කළ යුතුය. ප්‍රතිග්‍රහණය කිරීමට පෙර 9.2 පරිච්ඡේදයේ දක්වා ඇති අවදානම් තක්සේරු කිරීම ලේඛනගත කර අධ්‍යක්ෂවරයාට දැනුම් දිය යුතුය.

9.6 වලාකුළු සේවාවන් භාවිත කිරීමේ දී පාරිභෝගික, ප්‍රති-පාර්ශව තොරතුරු සහ හිමිකාරීත්ව වාණිජ දත්ත අනවසර හෙළිදරව් වීම් සහ අනවසර ප්‍රවේශයන්ගෙන් ආරක්ෂා වීම සඳහා සුදුසු ආරක්ෂණ ක්‍රියාමාර්ග ක්‍රියාත්මක කිරීමට බලපත්‍රලාභී මුදල් සමාගම් කටයුතු කළ යුතුය. ක්‍රිප්ටෝග්‍රැපික් යතුරු (cryptographic keys) කළමනාකරණය ඇතුළුව පාරිභෝගික හා ප්‍රතිපාර්ශව තොරතුරු හිමිකාරීත්වය වාණිජ දත්ත සහ අන්තර්ජාලය තුළින් සපයන සේවාවල හිමිකාරීත්වය, පාලනය සහ කළමනාකරණය, රඳවා ගැනීම මෙයට ඇතුළත් වේ.

10.අන්තර්කාලීන ප්‍රතිපාදන

10.1 මෙම විධානයට අදාළ අන්තර්කාලීන ප්‍රතිපාදන පහත දක්වා ඇති වගුව 1 පරිදි විය යුතුය.

වගුව 1: අනුකූල වීම සඳහා කාලරාමුව

යොමුව	අවශ්‍යතාව	අනුකූල විය යුතු දිනය
4.3 (ආ)	විධායක මට්ටමේ තොරතුරු ආරක්ෂණ කමිටුව	2023.07.01
4.4	ප්‍රධාන තොරතුරු ආරක්ෂක නිලධාරී පත්කිරීම	2025.01.01
5.2	තොරතුරු වර්ගීකරණය සහ ලේබල්කරණය	2023.07.01
5.3	තීරණාත්මක තොරතුරු පද්ධති හඳුනා ගැනීම	2023.07.01
5.4	පරිශීලක ප්‍රවේශ කළමනාකරණය	2024.01.01
5.5	පරිගණක ආරක්ෂණ සහ පරිශීලක කටයුතු සටහන් කළමනාකරණය	2024.01.01
5.6	දත්ත සංකේතනය	2024.01.0
5.7	ආරක්ෂණ මෙහෙයුම් කේන්ද්‍රය	2026.01.01
5.8	දත්ත අහිමි වීම වැලැක්වීම	2024.01.01
5.9	තොරතුරු ආරක්ෂණය සම්බන්ධ සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීම සහ ප්‍රතිසාධනය	2024.01.01
 5.10.2 5.10.3	තොරතුරු ආරක්ෂණය පරීක්ෂා කිරීම අ) අවදානම් තක්සේරු කිරීම ආ) විනිවිදුම් පරීක්ෂාව	 2024.01.01 2024.01.01
 5.11.1 5.11.2	තොරතුරු ආරක්ෂණ පුහුණුව සහ සහතික කිරීම අ) අධ්‍යක්ෂ මණ්ඩලය පුහුණු කිරීම සහ දැනුම්වත් කිරීම ආ) කාර්ය මණ්ඩලය සඳහා තොරතුරු ආරක්ෂණ දැනුවත් කිරීමේ පුහුණුව සහ සහතිකකරණය	 2023.07.01 2023.07.01
6.2	පද්ධතිය උපයෝජ්‍යතාවය	2023.07.01
6.3/6.4/6.5	ආපදා ප්‍රතිසාධනය	2023.07.01

11. නිර්වචන

11.1 මෙම විධානයන්ගේ අරමුණු සඳහා පහත නිර්වචන අදාළ වේ.

අ) නියෝජිතයා - නියෝජිතයෙකු හෝ උප-නියෝජිතයෙකු යනු අධ්‍යක්ෂ මණ්ඩලය විසින් අනුමත කරන ලද අභ්‍යන්තර ප්‍රතිපත්තිවලට අනුකූලව, බලපත්‍රලාභී මුදල් සමාගම වෙනුවෙන් සීමිත මූල්‍ය ව්‍යාපාර කටයුතු සැලසීම සඳහා බලපත්‍රලාභී මුදල් සමාගම විසින් තෝරා පත් කර ගන්නා ලද ආයතනයක් හෝ පුද්ගලයෙකු වේ.

ආ) රහසා පාරිභෝගික නොවන දත්ත - බලපත්‍රලාභී මුදල් සමාගමේ මූල්‍ය ගනුදෙනු, අධ්‍යක්ෂ මණ්ඩලය සහ කළමනාකාරීත්වය වෙත ඉදිරිපත් කිරීම්, සංවේදී සේවක දත්ත සහ බලපත්‍රලාභී මුදල් සමාගම විසින් තීරණය කරනු ලබන වෙනත් ඕනෑම දත්තයක් ඇතුළුව, ද්වේශසහගත ලෙස භාවිත කළහොත් හෝ අනවසරයෙන් මුදා හැරියහොත් සැලකිය යුතු මූල්‍ය හෝ කීර්ති නාමය අහිමි වීමක් සිදු විය හැකි සහ පාරිභෝගික දත්ත යන නිර්වචනය යටතට නොගැනෙන ඕනෑම පොදු නොවන දත්තයක් මේ යටතට අයත් වේ.

ඇ) පාරිභෝගික දත්ත - අතීත, වර්තමාන හෝ භව්‍ය පාරිභෝගිකයෙකුට අදාළ ප්‍රසිද්ධ නොවන දත්ත මේ යටතට අයත් වේ. කෙසේ වුවද, හඳුනා ගැනීම අපහසු කළ පාරිභෝගික දත්ත, පාරිභෝගික දත්ත යටතට ගැනීම සිදු නොකළ යුතු වේ.

ඈ) හඳුනා ගැනීම අපහසු කළ පාරිභෝගික දත්ත - දත්ත මූලිකව අදාළ වූ පාරිභෝගිකයා හඳුනා ගැනීම සඳහා තනිව, හෝ වෙනත් කිසියම් දත්ත සමඟ ඒකාබද්ධව භාවිත කළ නොහැකි වන ලෙස සිතාමතා වෙනස් කරන ලද පාරිභෝගික දත්ත වේ.

ඉ) අධ්‍යක්ෂවරයා - බැංකු නොවන මූල්‍ය ආයතන අධීක්ෂණ දෙපාර්තමේන්තුවේ අධ්‍යක්ෂවරයා වේ.

ඊ) පොදු දත්ත - කිසිඳු සීමාවකින් තොරව භාවිත කිරීම සහ නැවත පළ කිරීම සඳහා සැම දෙනාහට නොමිලේ ලබාගත හැකි දත්ත.

උ) සේවා සපයන්නා - මුදල් ව්‍යාපාර පනත යටතේ නිකුත් කරන ලද 2018 අංක 07 දරන ව්‍යාපාර මෙහෙයුම් කටයුතු සම්බන්ධව බාහිර සේවා ලබා ගැනීම විධානය හෝ එහි සංශෝධන අනුව බලපත්‍රලාභී මුදල් සමාගම් විසින් බාහිර සේවා ලබා ගැනීමේ ගිවිසුමකට යොමු වී ඇති සේවා සපයන්නෙකු.

ඌ) ජ්‍යෙෂ්ඨ කළමනාකාරීත්වය - මුදල් ව්‍යාපාර පනත යටතේ නිකුත් කරන ලද 2021 අංක 06 දරන ප්‍රධාන වගකිව යුතු පුද්ගලයන්ගේ යෝග්‍යතාවය තක්සේරු කිරීම විධානය හෝ එහි සංශෝධන යටතේ දක්වා ඇති නිර්වචනය අනුකූල විය යුතුය.

නිවාඩ් අජිත් ලෙස්ලි කබ්රාල්
මුදල් මණ්ඩලයේ සභාපති සහ
ශ්‍රී ලංකා මහ බැංකුවේ අධිපති