කෙටුම්පත් අංක 1.3

රාජ්‍ය තොරතුරු වර්ගීකරණ ප්‍රතිපත්තිය

ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය

සැප්තැම්බර් 2022

පටුන

1 හැඳින්වීම

තොරතුරු යනු, එහි පැවැත්ම පුරාවටම, සුරක්ෂිතව තබාගත යුතු අත්‍යවශ්‍ය සම්පතකි.

එනමුත්, යම් ආයතනයක් සතුව පවතින සෑම තොරතුරක්ම එක හා සමාන වටිනාකමකින් යුක්ත නොවන අතරම එකම මට්ටමක ආරක්ෂණයක් ද අවශ්‍ය නොවේ. තොරතුරු ආරක්ෂණයේදී තොරතුරු වර්ගීකරණය යනු යම් ආයතනයකට ඔවුන් සතු තොරතුරු වල පැවැත්ම, විශ්වාසනීයත්වය සහ රහස්‍යභාවය පිළිබඳ තිබෙන අවදානම්සහගත තත්ත්වයන් සැලකිල්ලට ගනිමින් එම තොරතුරු සඳහා කිනම් මට්ටමක ආරක්ෂණයක් අවශ්‍යදැයි තීරණය කිරීමට ඒවායෙහි සංවේදීභාවය නිර්ණය කිරීම සඳහා වන ක්‍රියාවලියකි.

ඒ අනුව යම් රාජ්‍ය ආයතනයකට පෙර නිර්ණය කරනලද සංවේදීභාවයේ මට්ටම අවධානයට ගනිමින් තම නෛතික වගකීම් වලට අනුකූල වීමට, මූල්‍යමය අවදානම් සහ කීර්තිය පිළිබඳ අවදානම් මගහැරීමට, තම සේවා සැපයීම සම්බන්ධ අරමුණු අත්පත් කරගැනීමට සහ රාජ්‍ය සේවය පිළිබඳ පුරවැසියන්ගේත් ව්‍යාපාරයන්ගේත් විශ්වාසය ඉහළ මට්ටමකට ගෙන ඒමට අවශ්‍ය පියවර ගතහැක.

1.1 රාජ්‍ය සංවිධානයක තොරතුරු වත්කම් සම්බන්ධ බලපෑමේ මට්ටම්

බලපෑමේ මට්ටම මගින් තොරතුරු වල ආරක්ෂණය උල්ලංඝණය වීමෙන් යම් ආයතනයකට, එහි සේවාදායකයන්ට සහ අනෙකුත් ආයතන වලට ඇතිවිය හැකි ප්‍රතිවිපාක වල වැදගත්කම පෙන්නුම් කරයි.

මෙම ප්‍රතිවිපාක පහත සඳහන් කරුණු සම්බන්ධව තිබෙන ආයතනික නොහැකියාවන් මගින් ඇතිවිය හැක.

- එහි කටයුතු සාර්ථකව ඉෂ්ට කිරීම.
- නීති, රෙගුලාසි සහ ගිවිසුම් සම්බන්ධ බැඳීම් වලට අනුකූලවීම.
- ආයතනයේ සහ රජයේ ප්‍රතිරූපය ආරක්ෂා කර ගැනීම.
- ලබාදෙන සේවාවන් පිළිබඳව ගනුදෙනුකරුවන්ගේ සහ හවුල්කරුවන්ගේ විශ්වාසය පවත්වාගැනීම සහ වැඩිදියුණු කරගැනීම.
- පුරවැසියන් සහ ඔවුන්ගේ පෞද්ගලික ජීවිතය සම්බන්ධ තොරතුරු සුරක්ෂිත කිරීම වෙනුවෙන් පුරවැසියන්ගේ මූලික අයතිවාසිකම් වලට ගරු කිරීම.
- තම ව්‍යාපාර වල පැවැත්ම සහ තරහකාරී වාසිය සම්බන්ධව ව්‍යාපාර ආයතන මගින් ලබාදෙන ලද රහසිගත තොරතුරු වල ආරක්ෂණයට ගරු කිරීම.
- තම සේවාවන් මත යැපෙන තුන්වන පාර්ශවයේ ආයතන සඳහා දායකත්වය සැපයීම.

රාජ්‍ය ආයතන වලට අනුවර්ත වියහැකි බලපෑමේ මට්ටම් පහත සඳහන් වගුව මගින් පැහැදිලි කරයි.

බලපෑමේ මට්ටම	විස්තරය	
1	අවම (නොසලකාහැරිය හැකි)	▪ ආයතනයේ තිබෙන යම්කිසි ක්‍රියාවලියකට, එනම් විශේෂ සේවාවකට/පහසුකමකට, බලපෑමක් ඇතිකරයි.
2	මධ්‍යම (මධ්‍යස්ථ)	▪ ආයතනය සතු ක්‍රියාවලීන් ගණනාවකට බලපෑම් ඇතිකරයි.
3	ඉහළ (දැඩි)	▪ මහජනතාවට අත්‍යවශ්‍ය වන සේවාවල ප්‍රමිතීන් සම්බන්ධව සැලකියයුතු ලෙස බලපෑම් ඇතිකරයි. ▪ ආයතනික ප්‍රතිරූපයට බලපෑම් එල්ල කරයි. ▪ එක් ආයතනයක හෝ ආයතන කිහිපයක කටයුතු සඳහා බලපෑම් ඇතිකරයි. ▪ පුරවැසියන් සහ ඔවුන්ගේ පෞද්ගලිකත්වය සම්බන්ධ පුද්ගලික තොරතුරු; ඔවුන්ගේ සෞඛ්‍ය, ජීවිතය හෝ යහපැවැත්මට අනර්ථයක් නොවන අයුරින්, සුරක්ෂිත කිරීම සඳහා පුරවැසියන්ගේ මූලික අයතිවාසිකම් වලට ගරු කිරීම සම්බන්ධව බලපෑම් ඇතිකරයි. ▪ තම ව්‍යාපාර වල පැවැත්ම සහ තරඟකාරී වාසිය සම්බන්ධව ව්‍යාපාර ආයතන මගින් ලබාදෙන ලද රහසිගත තොරතුරු වල ආරක්ෂණයට ගරු කිරීම සම්බන්ධව බලපෑම් ඇතිකරයි.
4	ඉතාම ඉහළ (ඉතාම බරපතල)	▪ මහජනතාවට අත්‍යවශ්‍ය වන එක් සේවාවක් හෝ සේවාවන් කිහිපයක් සැපයිය නොහැකිවීම. ▪ පුරවැසියන්ගේ සෞඛ්‍ය, ජීවිතය හෝ යහපැවැත්ම තර්ජනයට ලක්කිරීම. ▪ පුරවැසියන් සහ ඔවුන්ගේ පෞද්ගලිකත්වය සම්බන්ධ පුද්ගලික තොරතුරු සුරක්ෂිත කිරීම සඳහා පුරවැසියන්ගේ මූලික අයතිවාසිකම් වලට ගරු කිරීම සම්බන්ධව බලපෑම් ඇතිකිරීම මගින් ඔවුන්ගේ සෞඛ්‍ය, ජීවිතය හෝ යහපැවැත්ම තර්ජනයට ලක්කිරීම. ▪ ප්‍රචාරය ඇතිව හෝ නැතිව රාජ්‍ය සන්නාමයට බලපෑම් ඇතිකිරීම.

මෙයට අමතරව පැවැත්ම, විශ්වාසනීයත්වය සහ රහස්‍යභාවය පිළිබඳ බලපෑමේ මට්ටම් පහත වගුව ඇසුරෙන් පැහැදිලිකර ඇත.

ආරක්ෂණ නිර්ණායකය	බලපෑමේ මට්ටම			
	පළමු මට්ටම (අවම)	දෙවන මට්ටම (මධ්‍යස්ථ)	තෙවන මට්ටම (ඉහළ)	සිවුවන මට්ටම (ඉතාම ඉහළ)
පැවැත්ම	තොරතුරු වෙත ප්‍රවේශයට හෝ තොරතුරු භාවිතයට බාධා පැමිණවීම ආයතනය වෙත ඉතා අවම බලපෑමක් ඇති කරයි.	තොරතුරු වෙත ප්‍රවේශය හෝ තොරතුරු භාවිතයට බාධා පැමිණවීම ආයතනය වෙත මධ්‍යස්ථ බලපෑමක් ඇති කරයි.	තොරතුරු වෙත ප්‍රවේශය හෝ තොරතුරු භාවිතයට බාධා පැමිණවීම ආයතනය වෙත ඉහළ බලපෑමක් ඇති කරයි.	තොරතුරු වෙත ප්‍රවේශය හෝ තොරතුරු භාවිතයට බාධා පැමිණවීම ආයතනය වෙත ඉතාම ඉහළ බලපෑමක් ඇති කරයි.
විශ්වාසනීයත්වය	අනවසරයෙන් තොරතුරු වෙනස් කිරීම හෝ විනාශ කිරීම ආයතනය වෙත නොසලකාහැරිය හැකි මට්ටමේ බලපෑමක් ඇති කරයි	අනවසරයෙන් තොරතුරු වෙනස් කිරීම හෝ විනාශ කිරීම ආයතනය වෙත මධ්‍යස්ථ බලපෑමක් ඇති කරයි	අනවසරයෙන් තොරතුරු වෙනස් කිරීම හෝ විනාශ කිරීම ආයතනය වෙත ඉහළ මට්ටමේ බලපෑමක් ඇති කරයි	අනවසරයෙන් තොරතුරු වෙනස් කිරීම හෝ විනාශ කිරීම ආයතනය වෙත ඉතාම ඉහළ මට්ටමේ බලපෑමක් ඇති කරයි
රහස්‍යභාවය	තොරතුරු වෙත අනවසර ප්‍රවේශය හෝ තොරතුරු අනවසරයෙන් හෙළිදරව් කිරීම ආයතනය වෙත නොසලකාහැරිය හැකි මට්ටමේ බලපෑමක් ඇති කරයි	තොරතුරු වෙත අනවසර ප්‍රවේශය හෝ තොරතුරු අනවසරයෙන් හෙළිදරව් කිරීම ආයතනය වෙත මධ්‍යස්ථ බලපෑමක් ඇති කරයි	තොරතුරු වෙත අනවසර ප්‍රවේශය හෝ තොරතුරු අනවසරයෙන් හෙළිදරව් කිරීම ආයතනය වෙත ඉහළ මට්ටමේ බලපෑමක් ඇති කරයි	තොරතුරු වෙත අනවසර ප්‍රවේශය හෝ තොරතුරු අනවසරයෙන් හෙළිදරව් කිරීම ආයතනය වෙත ඉතාම ඉහළ මට්ටමේ බලපෑමක් ඇති කරයි

2 තොරතුරු වර්ගීකරණය

බලපෑම සහ වටිනාකම පාදක කරගනිමින් තොරතුරු සඳහා වර්ගීකරණයක් ලබාදීමට යොදා ගැනෙන පද්ධති ආවරණය කෙරෙන මූලධර්ම, ක්‍රමවේද, උපාංග සහ රාමු තොරතුරු වර්ගීකරණය ලෙස හැඳින්වේ. තොරතුරු වර්ගීකරණය සම්බන්ධව නොයෙකුත් නිර්වචන ඇතත්, ඒ සැම එකක්ම පොදුවේ පහත සඳහන් මූලධර්මයන්ට යටත් වේ.

- සමස්ථ ආයතනය සතු සියළුම තොරතුරු (ඕනෑම මාදිලියක සහ ප්‍රමාණයක) සඳහා අදාළ වීම.
- ආයතනය තුළ දත්ත හුවමාරු කරගැනීම සහ දත්ත ප්‍රවේශය සම්බන්ධව පදනමක් සැපයීම.
- තොරතුරු ආරක්ෂණයේ රහස්‍යභාවය, විශ්වාසනීයත්වය සහ පැවැත්ම පිළිබඳ මූලධර්ම තහවුරු කිරීම.
- තොරතුරු වල සංවේදීභාවය සහ වටිනාකම අනුව, නමුත් එයට පමණක් සීමා නොවී, වර්ගීකරණය කිරීම.
- තේරුම් ගැනීමට සහ ක්‍රියාත්මක කිරීමට පහසු සරල රාමුවක් වීම.
- කාලය, නියාමන අවශ්‍යතාවයන් සහ ආයතනික වෙනස්කම් සමඟ තොරතුරු වල වටිනාකම ද වෙනස් වීම.
- වර්ගීකරණය පාලන රීතින් කට්ටලයක් මිස නොයෙකුත් පුද්ගලයන්ට අර්ථ දැක්වීමට විවෘතව පවතින හෝ යමක් මත පදනම් වන දෙයක් නොවීම.
- තොරතුරු වල ජීවන චක්‍රය පුරාවටම වර්ගීකරණය සිදුකිරීම.
- තොරතුරු වර්ගීකරණය තුළ 'විස්තෘත ආයතනය' සංකල්පය අන්තර්ගතවීම. එනම්, දෙපාර්තමේන්තු, ව්‍යාපාර ගනුදෙනුකරුවන්, කොන්ත්‍රාත්කරුවන්, අනෙකුත් ආයතන සහ පුරවැසියන්.
- වර්ගීකරණය එක් පුද්ගලයෙකු සතු වගකීමක් පමණක් නොවීම සහ එය සියළුදෙනාටම බලපෑමක් ඇති කිරීම.
- වර්ගීකරණ නීති ගතික ස්වභාවයක් ගන්නා බැවින් නිරන්තරව යාවත්කාලීන වියයුතු වීම.

2.1 තොරතුරු වර්ගීකරණය පැවරීම

සෑම රාජ්‍ය ආයතනයක්ම තොරතුරු වල අයිතිකරු විසින් අවසරදෙන ලද වර්ගීකරණයක් සහිත බව සහ අයිතිකරු විසින් පනවන ලද රීතීන්ට අනුව තොරතුරු පවත්වා ගැනීමට හා ක්‍රියාත්මක කිරීමට පත්කරන ලද භාරකරුවෙකු සිටින බව තහවුරු කිරීමට වගකීමෙන් බැඳී සිටී.

අයිතිකරු හෝ උත්පාදකයා (Originator) විසින් යම් තොරතුරක සංවේදීභාවය පිළිබඳව දැනුවත් වූ වහාම, අයිතිකරු/අභිනියෝතයා විසින් හැකි ඉක්මනින් එය වර්ගීකරණය කළයුතුය. බාහිරව ජනනය කරන

තොරතුරු, නැත්නම් වර්ගීකරණය නොකරනලද තොරතුරු ආයතනය වෙනුවෙන් ලබාගන්නා නිලධාරියා විසින් එම තොරතුරු වත්කම් සඳහා අයිතිකරුවෙකු සහ භාරකරුවෙකු පත්කර ඇති බවටත් ගැළපෙන පරිදි එම වත්කම ආයතනික වත්කම් නාමලේඛනයට ඇතුළත් කර ඇති බවටත් සහතික විය යුතුය.

2.2 තොරතුරු වර්ගීකරණය වෙනස් කිරීම

මූලිකවම, යම් තොරතුරක ආරක්ෂණ වර්ගීකරණය වෙනස්කළ හැකිවන්නේ එම තොරතුරු වලට මුලින්ම වර්ගීකරණය ලබාදුන් ආයතනයට (තොරතුරු අයිති ආයතනයට) පමණි.

ආරක්ෂණ වර්ගීකරණය නුසුදුසුයැයි හැඟෙයි නම් එම තොරතුරු වලට මුලින්ම වර්ගීකරණය ලබාදුන් ආයතනයෙන් හෝ දැනට එම තොරතුරු සම්බන්ධව වගකීම දරන ආයතනයෙන් ප්‍රශ්න කළයුතුය. මුල් ආයතනය ඉවත්කර හෝ ඒකාබද්ධ කර ඇත්නම්, මුල් ආයතනයේ වගකීම් භාරගත් ආයතනයට එහි වර්ගීකරණය වෙනස් කළහැක. රාජ්‍ය ලේඛනාගාරයේ භාරකාරත්වයට පත්කර ඇති තොරතුරු සඳහා ද එයට වෙන් වූ ආරක්ෂණ වර්ගීකරණයක් මගින් ගබඩා කර හැසිරවීම වඩාත් සුදුසුය.

2.3 තොරතුරු වර්ගීකරණයේ කාලසීමාව

ආරක්ෂණ වර්ගීකරණයේ කාලසීමාව යනු යම් තොරතුරක් කොපමණ කාලයක් සංවේදී ලෙස සැලකිය යුතු ද සහ එයට අදාළ ආරක්ෂණ වර්ගීකරණයට අනුව ගබඩාකර තබාගනිමින් භාවිතා කලයුතු ද යන්නයි.

යම් තොරතුරු වත්කමක් වර්ගීකරණයකල පසු වෙනස්කම් ඇතිවිය හැකි නිශ්චිත දිනයක් හෝ සිද්ධියක් තීරණය කිරීමට හැකිවනු ඇත. යම් සිදුවීමක් තොරතුරු වල සංවේදීභාවය වැඩිවීමට හේතුවිය හැක. උදාහරණයක් ලෙස මානව සම්පත් පෝරමයක්, එය පිරවීමෙන් හෝ සම්පූරණ කිරීමෙන් පසුව 'රහසිගත' ලෙස සැලකේ.

තොරතුරු වර්ගීකරණය කිරීමේ කාලසීමාව පහත සඳහන් ක්‍රම මගින් පැහැදිලිකල හැක.

- තොරතුරු වල අයිතිය සතුවන හෝ එයට ආරක්ෂණ වර්ගීකරණයක් යොදන ආයතනයට, තොරතුරුවල සංවේදීභාවයේ කාලසීමාව අනුව, එය තවදුරටත් රහස්‍ය ලෙස වර්ගීකරණයවීම නැවත්වීම සඳහා නිශ්චිත දිනයක් හෝ සිද්ධියක් තීරණය කළහැක. එම දිනය හෝ සිද්ධියට පසුව ස්වයංක්‍රීයව තොරතුරු වර්ගීකරණයෙන් නිදහස් වේ.
- වර්ගීකරණය නවත්වන කාලසීමාව යම් තොරතුරක් ආශ්‍රිතව සිදුකල අවසාන ක්‍රියාවෙන් පසුව යොදන දිනයක් මගින් ද තීරණය කළහැක (උදාහරණයක් ලෙස අවසාන වරට එය භාවිතා කිරීමන් මාස 6කට පසුව).

- ආරක්ෂණ වර්ගීකරණය යොදන ආයතනයට වර්ගීකරණය ඉවත් කිරීමට නිශ්චිත දිනයක් හෝ සිද්ධියක් තීරණය කළ නොහැකි නම්, එම තොරතුරු වල වර්ගීකරණය නැවත්වීම අදාළ රාජ්‍ය සම්මතයන්ට අනුව, මූලික වර්ගීකරණයෙන් වසර 10කට පසුව වැනි, පූර්ව නිශ්චිත කාලසීමාවක් තුළදී සිදුකල හැක.

- ආරක්ෂක වර්ගීකරණ තොරතුරු සඳහා වන ප්‍රොටෝකෝල සහ මාර්ගෝපදේශයන්ට අනුව, ආරක්ෂණ වර්ගීකරණය යොදන ආයතනයට, එය බලාත්මක වන කාලසීමාව දීර්ඝ කිරීමට, ආරක්ෂණ වර්ගීකරණය වෙනස් කිරීමට හෝ යම් තොරතුරු නැවත වර්ගීකරණය කිරීමට හැකි වේ.

- අසීමිත කාලසීමාවකට වුවද තොරතුරු ආරක්ෂණ වර්ගීකරණය සිදුකල හැකි අතර කැබිනට් ලේඛන එයට අයත් නොවේ.

2.4 ආරක්ෂණ වර්ගීකරණ මට්ටම්

ආරක්ෂණ වර්ගීකරණයේ මට්ටම් පහක් (වර්ගීකරණ මට්ටම් හතරක් සහ වර්ගීකරණය නොකරන ලද මට්ටම) පුළුල් ලෙස හඳුනාගෙන ඇත.

- වර්ගීකරණය නොකළ (සුදු)
- පොදු (කොළ)
- සීමිත බෙදාගැනීම (කහ)
- රහසිගත (රතු) සහ
- රහස්‍ය (තද රතු)

2.4.1 වර්ගීකරණය නොකළ

සියළුම රාජ්‍ය තොරතුරු, වටිනාකම තක්සේරු කර වර්ගීකරණය කරනතුරු, අන්තර්කාලීන වර්ගීකරණ තත්ත්වයට (වර්ගීකරණය නොකළ) යොමුකළ යුතුය. ඕනෑම වර්ගීකරණය නොකළ තොරතුරක්, සීමිත බෙදාගැනීම යටතට ගැනෙන තොරතුරු හා සමානව හෝ ඊට ඉහළ තත්ත්වයෙන් සැලකිය යුතුය - සීමිත බෙදාගැනීම. වර්ගීකරණය නොකරනලද තොරතුරක් ප්‍රසිද්ධ කිරීමේදී තොරතුරු අයිතිකරුගෙන් පූර්ව අවසරයක් ලබාගත යුතුය. (එය තොරතුරු වර්ගීකරණය වෙනස් කිරීමකි).

2.4.2 පොදු

ව්‍යවස්ථාවෙන් ‘පොදු’ ලෙස පිළිගෙන ඇති හෝ සාමාන්‍ය හෙළිදරව් කිරීමේ ප්‍රතිපත්තියක් මගින් ‘පොදු’ ලෙස වර්ගීකරණය කරන ලද මහජනතාවට, රාජ්‍ය නිලධාරීන්ට, ආයතන වලට, නියාමකයින්ට, ව්‍යාපෘති කළමණාකාරවරුන්ට, සහාය සේවකයන්ට සහ කොන්ත්‍රාත්කරුවන්ට පහසුවෙන් ලබාගත හැකි ඕනෑම

තොරතුරුක් 'පොදු' ලෙස වර්ගීකරණය කළහැක. මෙවැනි තොරතුරු හෙළිදරව් කිරීමෙන් වැළක්වීම ඉතාම අවම මට්ටමක නැතහොත් ආරක්ෂාව අවශ්‍යම නොවන මට්ටමක පවතී. 'පොදු' තොරතුරු සඳහා නිදසුන් කිහිපයක් පහත දැක්වේ.

- රාජ්‍ය පනත් සහ ප්‍රතිපත්ති
- ආයතනික සම්බන්ධතා නිලධාරීන්
- රජය විසින් මහජනතාවට සපයන සේවාවන් පිළිබඳ තොරතුරු
- කාලගුණික තොරතුරු
- නව ඇබෑර්තු සඳහා වන දැන්වීම්

<u>සටහන:</u>

ආරක්ෂාව පිළිබඳ අවශ්‍යතාවයක් පොදු තොරතුරු සම්බන්ධව නොමැති බැවින් එම තොරතුරු නිකුත් කිරීමට ප්‍රථම එහි නිරවද්‍යතාව සහ සම්පූර්ණබව (විශ්වාසනීයත්වය) තහවුරු කළයුතුය. උදාහරණයක් ලෙස, වෙබ් අඩවියක පළකරන තොරතුරු විකෘති කිරීමන් සහ වෙනස් කිරීමෙන් ආරක්ෂා කළයුතුය. තොරතුරු වර්ගීකරණය කිරීමේ රාමුව පොදු තොරතුරු වල විශ්වාසනීයත්වය සහ පැවැත්ම පිළිබඳ සාකච්ඡා නොකරන අතර එම තොරතුරු අවශ්‍ය ඕනෑම මොහොතක ලබාගත හැකි බවත් විකෘති කර නැති බවත් තහවුරු කිරීමට රාජ්‍ය ආයතන විසින් නිසි ක්‍රියාමාර්ග ගතයුතුය.

පොදු පරිහරණය සඳහා වන ඇතැම් තොරතුරු නිකුත් කිරීමට ප්‍රථම රහස්‍යභාවය පිළිබඳ අවශ්‍යතා තිබිය හැක (උදාහරණයක් ලෙස අයවැය ලේඛන). මෙහිදී එම තොරතුරු 'පොදු' ලෙස නැවත වර්ගීකරණය කරන අවස්ථාව පිළිබඳවත් සඳහන් කළයුතුය.

තොරතුරු නිකුත් කිරීමට පෙර 'පොදු' ලෙස නිශ්චිතවම වර්ගීකරණය කළයුතුය. සැමවිටම 'පොදු' තොරතුරු, එහි අයිතිකරු විසින් 'පොදු' ලෙස අනුමතකර තිබිය යුතුය. වර්ගීකරණයකර නොමැති තොරතුරු, වර්ගීකරණය නොකළ තොරතුරු ලෙස මිස 'පොදු' තොරතුරු ලෙස නොසැලකිය යුතුය.

2.4.3 සීමිත බෙදාගැනීම

යම් තොරතුරු හෙළිදරව් කිරීමක් මගින් රජයට, වාණිජ්‍යමය ආයතනයකට හෝ මහජනතාවට සීමිත හානියක් සිදුකිරීමේ සුළු සම්භාවිතාවක් ඇත්නම්, එවැනි තොරතුරු 'සීමිත බෙදාගැනීම' ලෙස වර්ගීකරණය කෙරේ. මෙවැනි තොරතුරු අනවසරයෙන් හෙළිදරව් කිරීම මගින් අභ්‍යන්තර ආරක්ෂාවට, ත්‍රිවිධ හමුදාවට හෝ ශ්‍රී ලංකාවේ විදේශ සබඳතා වලට නොසලකාහැරිය හැකි මට්ටමේ හෝ කිසිදු හානියක් සිදු නොවේ. සීමිත බෙදාගැනීම යටතට ගැනෙන තොරතුරු සඳහා නිදසුන් කිහිපයක් පහත දැක්වේ.

- ආයතනික ක්‍රියාවලීන් සහ තොරතුරු
- පුරවැසියන්ගේ පෞද්ගලික තොරතුරු[1]
- ව්‍යාපාර ආයතනවල රහස්‍ය තොරතුරු
- ආයතනික රැස්වීම් සටහන් සහ වෙනත් සටහන්
- ආයතනයක නිෂ්පාදනයක් සම්බන්ධව රජයේ තක්සේරුව
- භාණ්ඩ ලේඛනය (Inventory) පිළිබඳ දත්ත

2.4.4 රහසිගත

යම් තොරතුරුක් හෙළිදරව් කිරීමෙන් ජාතික ආරක්ෂාව, අභ්‍යන්තර ස්ථාවරත්වය, ජාතික යටිතල පහසුකම, ත්‍රිවිධ හමුදාව, ව්‍යාපාරික ආයතන හෝ මහජනතාව වෙත හානි පැමිණවීමේ ඉහළ සම්භාවිතාවක් ඇත්නම්, එවැනි තොරතුරු 'රහසිගත' ලෙස වර්ගීකරණය කෙරේ.

'රහසිගත' ලෙස සලකුණු කර ඇති තොරතුරු හෙළිදරව් කිරීමේ හැකියාව ඉතා අවම මට්ටමක හෝ තහනම් කර ඇත. 'රහසිගත' තොරතුරු සඳහා උදාහරණ කිහිපයක් පහතින් දැක්වේ.

- ප්‍රතිලාභ, වැඩසටහන් ලිපිගොනු හෝ පෞද්ගලික ලිපිගොනු වැනි පුද්ගලික ගොනු
- ආයතනික බදු වාර්තා හෝ මූල්‍ය ස්ථාවරත්වය
- පුද්ගලයෙකුගේ පෞද්ගලික සෞඛ්‍ය පිළිබඳ තොරතුරු හුවමාරු කරගැනීම
- වෙළඳ රහස්
- වැටුප් පිළිබඳ තොරතුරු

2.4.5 රහස්‍ය

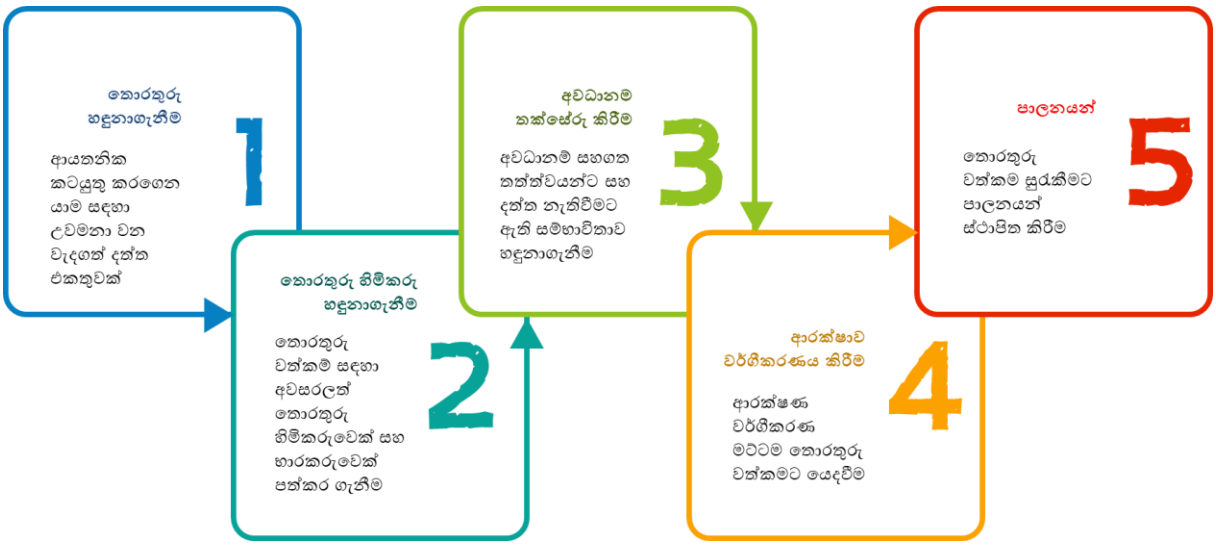
යම් තොරතුරක් හෙළිදරව් කිරීමෙන් ජාතික ආරක්ෂාවට, රජයට, ජාතික වශයෙන් වැදගත් වන ආර්ථිකමය/වාණිජ්‍යමය අවශ්‍යතා වෙත දැඩිලෙස හානි පමුණුවයි නම් හෝ ජීවිතය අවදානමකට ලක්කරයි නම්, එවැනි තොරතුරු 'රහස්‍ය' ලෙස වර්ගීකරණය කෙරේ. එමඟින් අන්තර්ජාතික නොසන්සුන්තාවය වර්ධනය කෙරෙන අතරම සෙසු රාජ්‍යයන් සමඟ ඇති සබඳතා වලට දරුණු ලෙස හානි පමුණුවයි. තවද එය සැලකියයුතු ලෙස ජාතික යටිතල පහසුකම් වලට බාධා ඇතිකරමින් දරුණු ලෙස ශ්‍රී ලංකාවේ හෝ වෙනත් රටවල අභ්‍යන්තර ස්ථාවරත්වයට හානි ගෙන දෙයි. රහස්‍ය ලෙස සැලකෙන තොරතුරු සඳහා උදාහරණ කිහිපයක් පහතින් දැක්වේ.

[1] 2022 අංක 19 දරණ පුද්ගලික දත්ත ආරක්ෂණ පනත මඟින් පාලනය වේ

- ලිංගික වරදකරුවන් සහ විනිදිතයන් පිළිබඳ තොරතුරු
- ප්‍රධාන ගණයේ අපරාධ සඳහා සිදුකරන අපරාධ පරීක්ෂණ තොරතුරු
- විදේශ සබඳතා පිළිබඳ තොරතුරු
- කැබිනට් මණ්ඩල ලේඛන පිළිබඳ තොරතුරු
- ප්‍රකාශයට පත්කිරීමට පෙර ප්‍රාදේශීය අයවැය පිළිබඳ තොරතුරු

3 තොරතුරු වර්ගීකරණය කිරීමේ ක්‍රියා පටිපාටිය

මෙය සජීවී ක්‍රියා පිළිවෙතක් බව අවබෝධ කරගැනීම අවශ්‍ය වේ. එනම් තොරතුරු වර්ගීකරණයේ අවශ්‍යතාව නිරන්තරව සහ කාලානුරූපීව නැවත නැවතත් තක්සේරු කළයුතු අතර මෙම ක්‍රියා පිළිවෙත එක් වරක් පමණක් යොදාගැනීම තොරතුරු සඳහා අවශ්‍ය ආරක්ෂණය ලබාදීමට තරම් ප්‍රමාණවත් නොවේ.



3.1 පියවර 1: තොරතුරු වත්කම් හඳුනාගැනීම

තොරතුරු වත්කම් යනු ඕනෑම ආකාරයකින් ගබඩා කර ඇති, යම් නියෝජිතායතනයකට එහි කාර්යයන් ඉටු කිරීමට වටිනාකමක් ඇති ලෙස හඳුනාගත් සහ එමඟින් නියෝජිතායතනයේ පිළිගත් අවශ්‍යතාවයක් තෘප්තිමත් කෙරෙන දත්ත එකතුවක් ලෙස අර්ථ දක්වා ඇත.

පහත උදාහරණ, නමුත් එපමණකට සීමා නොවී, තොරතුරු වත්කම් ලෙස හැඳින්විය හැක.

- වාර්තා
- ලේඛන
- විද්‍යුත් පණිවුඩ
- පරිගණක දත්ත ගබඩාවක ඇති පේළි (Rows) ගණන
- ලේඛනයක ඇති වගු (Tables) සහ සංඛ්‍යා (Figures)
- පරිගණක දත්ත ගබඩාවක ඇති වගු (Tables) ගණන
- තනි තාර්කික වස්තුවක් හෝ ‘පාරිභෝගිකයා’ වැනි සංකල්පයක් පිළිබඳ එක්රැස් කරනලද දත්ත
- Uniform Resource Locators (URLs) හෝ Uniform Resource Identifiers (URIs) මගින් හඳුනාගත් දත්ත

- අනෙකුත් තොරතුරු වත්කම් පිළිබඳ තිබෙන පාරදත්ත (metadata)

පුළුල් වර්ගීකරණ පාලනයක් පවත්වාගෙන යන බව සහතික වීම සඳහා, යම් තොරතුරක් මාධ්‍යයන් හෝ ආකෘතීන් කිහිපයක් අතර පැතිර පවතින විට ඒ සෑම මාධ්‍යයයකටම/ආකෘතියකටම වර්ගීකරණ අවශ්‍යතා නිසි පරිදි යොදවා ඇතිබව තහවුරු කළයුතුය.

ලිඛිතව හෝ ඉලෙක්ට්‍රොනිකව ගබඩා නොකළ යම් තොරතුරු වත්කමක් වේ නම් (පින්තූර හෝ පරීක්ෂණ සාම්පල වැනි), එවැනි තොරතුරු ද තොරතුරු ආරක්ෂණ වර්ගීකරණය යටතේ වර්ගීකරණය කළයුතු අතර අනුකූලතාවය හා භාවිතය තහවුරු කිරීම සඳහා ආයතන මගින් අමතර ප්‍රතිපත්ති සැකසිය යුතු වේ.

තොරතුරු හා සන්නිවේදන තාක්ෂණික වත්කම් ලෙස වඩා නිවැරදිව විස්තර කෙරෙන තොරතුරු ගබඩා කිරීම, සැකසීම, ප්‍රවේශවීම, මෙහෙයවීම ආශ්‍රිත තාක්ෂණයන් හැඳින්වීමට තොරතුරු වත්කම නමැති යෙදුම භාවිතා නොකරයි. තොරතුරු වත්කම් ලෙස නොසළකන තොරතුරු හා සන්නිවේදන තාක්ෂණික වත්කම් කිහිපයක් පහතින් දැක්වේ.

- යෙදුම් සහ පද්ධති මෘදුකාංග, සංවර්ධන මෙවලම් සහ උපයෝගිතා සහ ඒ ආශ්‍රිත බලපත්‍ර ඇතුළු මෘදුකාංග.

- පරිගණක උපකරණ, ගබඩා මාධ්‍යය (සීඩී, ඩීවීඩී, ටේප් සහ තැටි), බල සැපයුම්, වායු සමීකරණ, සහ තොරතුරු සම්පත්වල රහස්‍යභාවය, පවතින බව හෝ විශ්වාසනීයත්වයට බලපෑම් කළ හැකි වෙනත් තාක්ෂණික උපකරණ වැනි භෞතික වත්කම්.

3.2 පියවර 2: තොරතුරු වත්කම් සඳහා හිමිකරුවෙකු හඳුනාගැනීම

ආයතනික තොරතුරු වත්කම් සඳහා තොරතුරු වල හිමිකරු විසින් අනුමත කරනලද ආරක්ෂණ වර්ගීකරණයක් ඇති බවත්, එම තොරතුරු හිමිකරු විසින් පනවන ලද නීතිරීතීන්ට අනුව තොරතුරු වත්කම් ක්‍රියාත්මක/නඩත්තු කෙරෙන භාරකරුවෙකු සිටින බවත් සෑම ආයතනයක් විසින්ම තහවුරු කළයුතුය. තොරතුරු වත්කම් සංවේදීතාවය පිළිබඳව එහි ආරම්භකයා හෝ හිමිකරු දැනුවත් වූ වහාම තොරතුරු හිමිකරු හෝ නියෝජිත විසින් හැකි ඉක්මනින් එය වර්ගීකරණයට යටත් කළයුතුය.

වර්ගීකරණය නොකළ බාහිරව ජනනය කරනලද තොරතුරු වත්කම් ලබාගන්නා ආයතන නිලධාරියා විසින් එයට හිමිකරුවෙකු හා භාරකරුවෙකු යොදවා ඇති බවත් නිසි පරිදි තම ආයතනික තොරතුරු වත්කම් ලැයිස්තුවට (Information Asset Register) එය අන්තර්ගතකර ඇති බවත් තහවුරු කළයුතුය.

සටහන:

තොරතුරු හිමිකරුවන් විසින් ආයතනයක තොරතුරු වත්කම් පාලනය කෙරෙන ප්‍රතිපත්තිය නිර්වචනය කෙරෙයි. උදාහරණයක් ලෙස තොරතුරු වත්කම් වර්ගීකරණය පිළිබඳ තීරණය කිරීම. හිමිකරුවෙකු සැමවිටම තොරතුරු වත්කමක මෙහෙයුම් වගකීම එහි ගුණාත්මකබව, ආරක්ෂාව, විශ්වාසනීයත්වය, නිවැරදිබව, පුද්ගලිකත්වය සහ ප්‍රවේශය ආදී හිමිකරුගේ අරමුණු සහ උපදෙස් ක්‍රියාත්මකවන පරිදි එයට නිසි පාලනයන් (Controls) යොදවන භාරකරුවෙකු වෙත පවරනු ලබයි.

3.3 පියවර 3: අවදානම විශ්ලේෂණය සඳහා තොරතුරු වත්කමක බලපෑම තක්සේරු කිරීම

මෙම තක්සේරුකරණයේ අවශ්‍යතාවය වන්නේ අවදානම ඇතිවීමේ සම්භාවිතාවය හෝ වියහැකිබව දැනගැනීම සහ යම් හෙයකින් විශ්වාසනීයත්වය, රහස්‍යබව හෝ තොරතුරු වත්කමෙහි වටිනාකම ආදියට හානියක් වුවහොත් එහි බලපෑම කුමක් විය හැකි ද යන්න දැනගැනීමයි.

තොරතුරු වත්කමක් හෝ විෂයපථයක් සඳහා නිවැරදි තොරතුරු ආරක්ෂණ වර්ගීකරණය තීරණය කිරීමේදී කරුණු මාලාවක් කෙරෙහි අවධානය යොමුකළ යුතුය. තොරතුරු වත්කමක් ව්‍යවස්ථාවට, රීතීන්ට, ප්‍රතිපත්ති වලට, ගිවිසුම් හෝ වෙනත් ඕනෑම පූර්ව නිශ්චිත කරුණකට අනුව ආරක්ෂණ වර්ගීකරණය කළහැකි නම්, එසේ කළයුතුය. උදාහරණයක් ලෙස, තුන්වන පාර්ශව විසින් සපයන ලද තොරතුරු වල රහස්‍යභාවය නඩත්තු කිරීමේ වගකීම කඩකරමින් සහ කළමනාකරණයට අදාළ ව්‍යවස්ථානුකූල සීමාවන් කඩකරමින් තොරතුරු හෙළිදරව් කිරීම පිළිබඳව සැලකිලිමත් විය යුතුය. මෙමඟින් අවසාන ආරක්ෂණ වර්ගීකරණයට බලපෑම් ඇතිකළ හැක.

3.4 පියවර 4: තොරතුරු වත්කමෙහි ආරක්ෂණ වර්ගීකරණය තීරණය කිරීම

බලපෑම තක්සේරු කිරීමේදී තීරණය කරන ලද ඉහළම ආරක්ෂණ වර්ගීකරණය යොදාගත යුතුය.

3.5 පියවර 5: ආරක්ෂණ වර්ගීකරණය අනුව පාලනයන් යෙදවීම

තොරතුරු වත්කම් සඳහා ලබා දී ඇති ආරක්ෂාව යොදා ඇති ආරක්ෂණ වර්ගීකරණය සමඟ අනුරූපවන බව තහවුරු කිරීම සඳහා 'ජාතික දත්ත හුවමාරු කිරීම පිළිබඳ ප්‍රතිපත්තිය' මගින් නියම කර ඇති පරිදි නිසි පාලනයන් යොදා ගැනීම.