

තොරතුරු තාක්ෂණ පහසුකම් සඳහා
ප්‍රවේශ මුරපද භාවිතය පිළිබඳ
ප්‍රතිපත්තිය



ප්‍රධාන ලේකම් කාර්යාලය - දකුණු පළාත.

උපායමාර්ගය :

මුරපද මගින් ප්‍රවේශය පාලනය සඳහා වන මූලික උපාය මාර්ගය වන්නේ ප්‍රධාන ලේකම් කාර්යාලයෙහි නිලධාරීන්ට ඔවුන්ගේ රාජකාරි කටයුතු ඉටුකිරීමේදී ලබා දී ඇති පරිගණක, පරිගණක මෘදුකාංග පද්ධති, ජාල, යෙදවුම් මෘදුකාංග සහ පරිගණකගත දත්ත හා තොරතුරු වෙත ප්‍රවේශය ආරක්ෂිතව සලසා ගැනීම හා එය කළමනාකරණය කිරීමයි. මෙහිදී බලයලත් පුද්ගලයන් සඳහා පමණක් ප්‍රවේශය සැපයීමත් ප්‍රවේශ පාලනයත් (access control), නිලධාරීන්ගේ මේ සම්බන්ධ වගකීමත් කෙරෙහි අවධානය යොමු කරනු ලැබේ.

ප්‍රතිපත්ති හා මේ සම්බන්ධ පනත් :

කාර්යාලයේ සියළුම නිලධාරීන් පරිගණක, බාහිර දත්තගබඩා කරන උපාංග හෝ ජාල හරහා ගබඩා කර ඇති හෝ ප්‍රවේශ වන සියලුම කාර්යාලීය තොරතුරු සුරක්ෂිත කිරීමට කැපවී සිටී.

1. පරිගණක පද්ධති, දත්ත හා තොරතුරු වෙත ප්‍රවේශය එම ප්‍රවේශය සඳහා අවසර දී ඇති නිලධාරීන්ට පමණක් සීමා කළ යුතු අතර, සුදුසු අනන්‍ය පරිශීලක නාම සහ මුරපද නිකුත් කිරීම හෝ සකසා ගැනීම කළ යුතුය.
2. කාර්යාලීය කටයුතු සඳහා භාවිතා කරන මුරපද ඉතා රහසිගත ලෙස සැලකේ. මේ මගින් පරිගණක හෝ පරිගණක පද්ධති පරිශීලකයින්ට ඔවුන්ගේම මුරපද යළි සැකසීමට ඉඩ දෙන තාක්ෂණය වැනි වෙනත් ප්‍රවේශ පාලන යාන්ත්‍රණ භාවිතය බැහැර නොකෙරේ.
3. සියලුම නිලධාරීන් මෙම ප්‍රතිපත්තියට අනුකූල වීම සඳහා පරිගණක, මෘදුකාංග, යෙදුම් මෘදුකාංග, පරිගණක ජාල, ඊමේල්, අන්තර්ජාලය, සහ වෙනත් සම්පත් හෝ මාධ්‍ය වෙත විද්‍යුත් සත්‍යාපනය කිරීමේ මුරපද ක්‍රියාත්මක කළ යුතු අතර මෙය ක්‍රියාත්මක වන බවට වගකිව යුතුය.
4. ආරක්ෂාව හෝ පරිපාලන ප්‍රවේශ පාලනයන් මග හැරීමට වෙනත් අයෙකු උත්සාහ කිරීම හෝ ඉල්ලීම් කිරීම මෙම ප්‍රතිපත්තිය උල්ලංඝනය කිරීමකි. තවද, පද්ධති පරිශීලක නාම, මුරපද හෝ රහස්‍ය තොරතුරු අනවසරයෙන් භාවිතා කිරීම, වෙනස් කිරීම, විනාශ කිරීම හෝ හෙළිදරව් කිරීම 2007 අංක 24 දරන පරිගණක අපරාධ පනත (අංක 7,8,9, සහ 10 වගන්ති) යටතේ දඬුවම් ලැබිය හැකි වරදකි. තවද එය විනය ක්‍රියාමාර්ගවලට ද යටත් විය හැකිය.
5. මෙම ප්‍රතිපත්තියේ කිසියම් අංගයක් උල්ලංඝනය කළහොත් පරිගණක පද්ධති වලට ප්‍රවේශය අවලංගු කළ හැක.
6. නිශ්චිත පද්ධති කාර්යයන් වෙත සහ දත්ත සම්පත් වෙත ප්‍රවේශය එක් එක් පරිශීලකයාගේ රැකියා විෂය පථයට සහ රැකියා වගකීම්වලට අනුකූල ලබා දීම අවශ්‍ය වේ.
7. SLCERT ආයතනය මගින් ප්‍රකාශිත රාජ්‍ය ආයතන සඳහා තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තියෙහි 4.3.4 (අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය පිළිබඳ ප්‍රතිපත්තිය) හා 4.3.5 (ශක්තිමත් සත්‍යාපනය පිළිපද ප්‍රතිපත්තිය) වගන්ති ද මෙයට අදාල වේ.
8. 2022 අංක 09 දරන පෞද්ගලික දත්ත ආරක්ෂණ පනත 35 (ආ) වගන්තිය හා 40 වගන්තිය.
9. 2006 අංක 19 දරන ඉලෙක්ට්‍රොනික ගනුදෙනු පනත 8.(2).(d) වගන්තිය

10. ඩෙස්ක්ටොප් පරිගණක/ලැප්ටොප් හෝ එවැනි පරිගණක උපාංග සඳහා මුරපද සහිත තිර සුරැකුම් භාවිතා කළ යුතු අතර අක්‍රියතාවයෙන් මිනිත්තු 15 ට නොවැඩි කාලයකට පසු මුරපද යෙදා සක්‍රිය කළ හැකි පරිදි සකස් කිරීමෙන් අනවසර ප්‍රවේශයන් වලක්වා ගත හැකිය.
11. ප්‍රවේශයට තවත් ආරක්ෂිත ස්ථරයක් එක් කිරීම, එනම් ජංගම සත්‍යාපන කේතයක් වැනි දෙවන සාධකයක් භාවිතා කිරීම (2FA) මගින් ගිණුම් වලට වැඩි ආරක්ෂාවක් සපයා ගත හැකිය.
12. මුරපද ආරක්ෂණ වෙනුවට විකල්ප සත්‍යාපන තාක්ෂණයන්, උදා: ජෛවමිතික හෝ smart කාඩ්පත් භාවිතා කළ හැක.

මුද්දර ගාස්තු කළමනාකරණ පද්ධතිය			
විගණන විමසුම් තොරතුරු කළමනාකරණ පද්ධතිය			
තීරු බදු රහිත වාහන බලපත්‍ර නිකුත් කිරීමේ වැඩසටහන			
තැපැල කළමනාකරණ පරිගණක වැඩසටහන			
සැපයුම්කරුවන් සහ කොන්ත්‍රාත්කරුවන් ලියාපදිංචි කිරීමේ වැඩසටහන			