නිවසේ සිට වැඩකරන විට සැලකිලිමත් විය යුතු කරුණු

පහත කරුණු මූලාශ්‍ර කීපයක්ත් උපුටා ගෙන ඇත. උපදෙසක් පමනක් ලෙස සැලකිය යුතුයි.

කොවිඩ් - 19 කොරෝනාවෛරස් රෝගය නිසා නිවසෙන් වැඩ කිරීමේදී ආයතනයක් ලෙස හා සේවකයෙකු ලෙස සැලකිලිමත් විය යුතු කරුණු කීපයක් ගැන සලකා බලමු. සමාජ දුරස්ථභාවය (social distancing) පවත්ගැනීම මේ මොහොතේ වැදගත් ය.

මයික්‍රොසොෆ්ට්, ගූගල් ඇතුළු ලෝකයේ ප්‍රමුඛ පෙලේ සමාගම් රාශියක් මේ වන විට තම සේවකයන් නිවෙස් වල සිට වැඩ කිරීම ආරම්භ කර ඇත. සේවයකයන් බොහෝ දෙනෙකු අද වන විට ලැප්ටොප් පරිගණක ආශ්‍රයෙන් කටයුතු කිරීම මෙයට තවත් රුකුලක් වී තිබේ.

කුඩා ආයතන වල මේ තත්වයන් බොහෝ දුරට වෙනස් විය හැකිය. ඒවායේ සේවක පිරිස සුළු ප්‍රමාණයක් විය හැකිය. එසේම ඔවුන් අන්තර්ජාලය හරහා කරන රාජකාරි බොහෝවිට ඊමේල් වැනි සේවාවන් විය හැකිය. අධ්‍යාපන ක්ෂේත්‍රය ගැන සැලකීමේදී විශ්ව විද්‍යාල විසින් මේ වන විට නිවසේ සිටින ශිෂ්‍යයන්ට දේශන පැවැත්වීම කරගෙන යන අතර පාසල් දරුවන්ටද අධ්‍යාපන අමාත්‍යාංශයේ e-තක්සලාව සේවාව හරහා ඉගැන්වීම් කටයුතු කිරීම පිළිබඳව මේ වන විට අවධානය යොමු වී ඇත.

සේවා අවශ්‍යතා මත ආයතනික සේවක පිරිස කණ්ඩායම් කිහිපයකට බෙදා ඔවුන්ගේ අවශ්‍යතා අනුව කටයුතු කල හැකිය. කෙසේ වෙතත් එහිදී අත්‍යවශ්‍යම කාරණා කෙරෙහි වැඩි අවධානයකින් කණ්ඩායම් වෙන් කිරීම සුදුසු වේ.

නිවස් සිට වැඩ කිරීමේදී ඵලදායිතාවය ඉහල නංවා ගැනීමට කරුණු කිහිපයක් වැදගත් ය.

- පරිගණකයක් (හෝ දුරකතනයක් / ටැබයක්).
- හොඳ අන්තර්ජාල සබඳතාවක්.
- සන්නිවේදන කටයුතු සඳහා වන මෘදුකාංග (වැට් කිරීම සහ ඇමතුම් සඳහා Skype, රැස්වීම් පැවැත්වීම සඳහා Zoom වැනි)
- රාජකාරි කරගෙන යාමට සුදුසු ස්ථානයක්.
- දුරකතනයක් තිබීම අත්‍යවශ්‍ය නැතත් වැදගත් වනු ඇත.
- රාජකාරිය කරගෙන යාමට උනන්දුව සහ කැපවීම.
- දෛනික වැඩ සැලැස්මක්.

දුරකතනයක් අත්‍යවශ්‍ය නොවන්නේ ඇයි? අපට හොඳ අන්තර්ජාල සබඳතාවයක් සහ සන්නිවේදන මෘදුකාංග ඇත්නම් දුරකථනය අත්‍යවශ්‍ය නැත. සන්නිවේදන මෘදුකාංග හරහා ආයතනයේ සේවක පිරිසට අවශ්‍ය සන්නිවේදනය පවත්වාගත හැකිය. නමුත් පාරිභෝගික සේවා සපයන සේවකයන්ට හෝ දුරකථන සහය සපයන කාර්යාලීය සේවකයන්ට දුරකතනයක් තිබීම අත්‍යවශ්‍ය වේ. නමුත් සියලුම සේවකයින් හට දුරකතනයක් තිබීම රාජකාරි කටයුතු සඳහා අත්‍යවශ්‍ය නොවේ.

නිවෙස් සිට වැඩ කරන විට තම ආයතනයේ හා එහි සේවකයන්ගේ ජාලගත ආරක්ෂාව හෙවත් සයිබර් ආරක්ෂණය ගැන සැලකිලිමත් විය යුතුයි. මෙහි හඳුනාගත හැකි අභියෝග කිහිපයක් ඇත.

උපකරණ වල භෞතිකමය ආරක්ෂාව.

සේවකයන් නිවසේ සිට වැඩ කිරීමේදී භාවිතා කරන උපකරණ වලට ආයතන පරිශ්‍රයේ ඇති ආරක්ෂාව ඒ ආකාරයෙන්ම ලබා දීම අපහසුය. උපකරණ සොරකම් කිරීමට හෝ ඒවායේ ඇති දත්ත සොරා ගැනීමට ඇති ඉඩකඩ බොහෝ වැඩිය. ඒ නිසා ඊට සුදුසු ක්‍රියාමාර්ග ගත යුතුයි.

- පරිගණකයේ මතක තැටි (hard drive) වල ඇතුලත් දත්තයන් සංකේතනය (encrypt) කල යුතුයි. එවිට යම් හෙයකින් එම උපකරණ සොරකම් කලද ඒවායේ අඩංගු තොරතුරු කිසිවෙකුට ලබා ගැනීමට නොහැකි වේ.
- අන්තර්ජාලය ආශ්‍රිත ගිණුම් (ඊමේල්, ආයතන පද්ධතියේ පරිශීලක ගිණුම්) භාවිත නොකරන විට ගිනුමෙන් ඉවත් වෙන්න (log out). මෙවිට යමෙකු ඔබේ ගිණුමට පිවිස අනවශ්‍ය ඊමේල් පණිවිඩ යැවීම හෝ ඔබේ පණිවිඩ බැලීම වලක්වා ගත හැකිය.
- ශක්තිමත් මුරපද භාවිතා කරන්න. ගිණුම් හා පරිගණක ශක්තිමත් මුරපදයක් යොදා ආරක්ෂා කල යුතුය. තවද පරිගණකය පන ගැන්වෙන විට මුරපදයක් ඉල්ලා සිටිය යුතුයි. පරිගණකය පනගන්වා භාවිත නොකර ඇති අවස්ථාවක ස්වයන්ක්‍රීයව එය අගුලු වැටෙන ලෙස සැකසුම් කල යුතුයි. එසේම මුරපදය ලියූ කොළ කැබලි වැනි දෑ කිසිවෙකුවත් අතට පත් වන්නට ඉඩ තබන්න එපා.
- පිටත පරිසරයට උපකරණ නිරාවරණය කරන්න එපා. උපකරණයක් භාවිත නොකරන විට නොපොනන ස්ථානයක තැබිය යුතුයි.

ගෘහස්ථ තාක්ෂණික පරිසරය

නිවසේ සිට වැඩ කිරීමට පෙර භාවිත කරන ජාල හා උපකරණ වල තත්වය ගැන සැලකිලිමත් විය යුතුය. එම පද්ධති යාවත්කාලීන කල යුතුයි. යල්පැන ගිය පද්ධති හරහා බලාපොරොත්තු වන ඵලදායිතාවය ලබාගත නොහැකි විය හැකිය. එසේම අන්තර්ජාල සම්බන්ධතාවයන්ගේ ආරක්ෂාව පිලිබඳ සලකා බැලිය යුතුයි. උපකරණ වලට ශක්තිමත් මුරපද ඇතුලත් කර ආරක්ෂාව තහවුරු කරගත යුතුය.

ආයතනික පද්ධති සහ ජාලයන්ට පිවිසීම

ආයතනයේ ඊමේල් සහ අනෙකුත් සේවාවන් වලට පිවිසීමට අවශ්‍ය සේවකයන්ට එම අවසරයන් ලබා දිය යුතුයි. මෙම සේවා ක්ලවුඩ් (cloud) හරහා වුවද ලබා දිය හැකිය. එසේම ඔවුන් සේවා ලබාගන්නා විට සියලුම පහසුකම් නිවසේ දී ලබා දීම අවශ්‍ය නොවිය හැකියි. මෙහිදී පහත කරුණු ගැන අවධානය යොමු කිරීම වැදගත්ය.

- අභ්‍යන්තර පද්ධතීන්ට සම්පූර්ණ පිවිසීමට අවශ්‍ය නම්, ආයතනයට අයත් උපකරණ භාවිතා කරවීම වඩා සුදුසු වේ. ඒ මන්දයත් එවිට ආයතනයේ තොරතුරු තාක්ෂණික නිලධාරීන්ට එම උපකරණ නිසි පරිදි සැකසීම හෝ වෙනස් කිරීම කල හැකිය. සේවකයාට අයත් උපකරණ වල BYOD මෘදුකාංග ස්ථාපනය කල යුතුයි.
- Virtual Private Network (VPN) එකක් හරහා දුරස්ථ සේවකයන් සම්බන්ද කිරීම වැදගත් වේ. ඒ මඟින් බාහිර පුද්ගලයන් ආයතනික ජාලයට අනවසරයෙන් ඇතුළුවීම වලක්වාගත හැකිය.

- Remote Desktop යෙදුමක් භාවිතයෙන් සේවකයාගේ පරිගණකයකින් ආයතනික පද්ධති සුරක්ෂිතව සම්බන්ද කල හැකිය.
- USB හෝ වෙනත් බාහිර උපකරණ භාවිතය පාලනය කල යුතුයි.
- පරිගණක සහ ජාලයට සම්බන්ධ වන උපකරණ මැල්වෙයාර් (malware) හා පරිගණක වෛරස් වලින් ආරක්ෂා කරන වැඩසටහන් (virus guard / antivirus) ඇතුලත් කළ යුතුයි. එසේම අවශ්‍ය බලපත්‍ර (license) සැපයිය යුතුයි. ආයතනය තුලදී උපකරණ ආරක්ෂා කරන වැඩසටහනම දුරස්ථ පරිගණක වලට ඇතුලත් කල යුතුයි.
- දත්ත බාගත කිරීම (download) හා ගබඩා කිරීම (save) සීමා කල යුතුයි. වැදගත් ආයතනික දත්ත පිටස්තරයන් අතට පත්වීම වලක්වාගැනීමට මෙය ඉතා වැදගත්ය.
- සේවකයන් ආයතනික ජාලයට පිවිසීම තහවුරු කරගැනීම සඳහා බහුවිධ පිවිසුම් සත්‍යාපනය (multi-factor authentication) භාවිතා කිරීම සුදුසුයි. මෙය කෙටි පණිවිඩයක් (SMS) හරහා කේතයක් ලබා දීමෙන් හෝ යෙදවුමක් (app) හරහා හෝ දෘඩාංගයක් මගින් කල හැකිය.

අවශ්‍ය මෙවලම්, මෘදුකාංග සහ පිවිසුම් පහසුකම් ලබාදීම.

- සේවකයින්ට අවශ්‍ය වීඩියෝ ඇමතුම් හෝ එවන් අනෙකුත් සම්බන්ධතා මාර්ගවලට අවශ්‍ය පහසුකම් සපයාදිය යුතු වේ. වැඩි ඵලදායිතාවයක් සහ ඉහළ ගුණාත්මක භාවයක් ලබා ගැනීම සඳහා සේවකයන් අතර සන්නිවේදනය වැදගත් වේ.
- සන්නිවේදන මෘදුකාංග හරහා අනුමැති ලබා ගත යුතුය. නිවසේ සිට වැඩ කරන මේ කාලය තුල ව්‍යාජ ලෙස ඊමේල් එවීම හරහා මුදල් වංචා කිරීම සහ ආයතන නොමඟ යැවීම කිරීමට ඉඩ ඇත.

පුහුණු කිරීම සහ දැනුවත් කිරීම

කොවිඩ් 19 වෛරස් ව්‍යාප්තියත් සමඟම අන්තර්ජාලය හරහා විවිධ වංචා සිදුකරන පුද්ගලයන් බහුල වී තිබේ. මුහුණු ආවරණ සම්බන්ධයෙන්, ඖෂධ වර්ග සම්බන්ධයෙන් සහ නොමඟ යවනසුලු තොරතුරු ඇතුලත් කරමින් සකස් කෙරුණු ලිපි, වෙළඳ දැන්වීම් සහ ලින්ක් හුවමාරු වීම සිදුවේ. නිවසේ සිට වැඩ කරන පුද්ගලයින් මෙම ලින්ක් වලට පිවිසීම සහ ලිපි කියවීමට උත්සාහ කිරීම සිදුවීමට ඉඩ තිබේ. ඒ හරහා අනන්‍යතා සොරුන්, දත්ත සොරුන් සහ හැකර්වරුන්ට පද්ධතියට අනවසරයෙන් ඇතුළුවිය හැකිය. කාර්යාලයේදී මෙන් තම සහෝදර සේවකයන්ගෙන් විමසීම කල නොහැකි නිසා බොහෝදෙනෙක් මේවාට අසු විය හැකිය.

මේ නිසා අන්තර්ජාල ආරක්ෂණය සම්බන්ධව නිවසේ සිට වැඩ කරන සේවකයන් දැනුවත් කිරීම අත්‍යවශ්‍ය කරුණකි. මෙවන් තර්ජනයන් ගැන සේවකයන්ට අවබෝධය ලබාදෙන වැඩසටහනක් සංවිධානය කර එය ඉහත කී ආකාර සන්නිවේදන මෘදුකාංගයක් හරහා හෝ ඊමේල් පණිවිඩයක් ආකාරයෙන් දියත් කිරීම සුදුසුය.

ආපදා කළමනාකරණය සහ සහයෝගය ලබාදීම

නිවසේ සිට වැඩ කිරීමට අවකාශ ඉක්මනින් සැලසීමේදී අන්තර්ජාල ආරක්ෂණය පිලිබඳ සැලකිල්ල ගිලිහී යා හැකිය. මේ සම්බන්ධයෙන් තොරතුරු තාක්ෂණ සේවා කණ්ඩායමේ සේවකයන් ඇතුළුව ආයතනික

සේවකයින් දැනුවත් කිරීම අවශ්‍ය වේ. එසේ නැතිවුවහොත් නිවසේ සිට රාජකාරී කිරීම යම් දුරකට අසාර්ථක වීමට ඉඩ තිබේ.

තාක්ෂණික කරුණු කාරනා ගැන සැලකිලිමත් වන අතරම දුරස්ථව රැකියාවෙහි නිරත වන විට සැලකිය යුතු තවත් කාරණා කිහිපයක් ඇත. ඒවා තාක්ෂණික නොවන සමාජීය කරුණු වේ.

- **සන්නිවේදනය** - සේවකයන් අතර දිනකට වරක් වත් සාමූහාක ඇමතුමක් (team call) හරහා සම්බන්ධ වන්න. එහිදී එකිනෙකා අතර හුවමාරු වන අදහස් ඔස්සේ එකිනෙකාගේ දෛනික අත්දැකීම් හුවමාරු කරගත හැකියි.
- **ප්‍රතිචාර දැක්වීම** - දුරස්ථ රාජකාරි කිරීම කාර්යාලිය පරිසරයේ සිට වැඩ කිරීම තරම්ම සමාන නොවන නිසා ඊමේල්, වෙනත් දැනුවත් කිරීම් සහ කැඳවීම් වලට ප්‍රතිචාර දැක්වීමේ උපදෙස් සේවකයන් අතර හුමාරු කරවීම වැදගත් වේ.
- **වාර්තාකරණය** - කණ්ඩායම් ප්‍රධානීන් හෝ කළමනාකරුවන් තමන්ගේ කණ්ඩායමේ සියලුදෙනා අදාල කටයුතුවල නිරතවන බවට දැනුවත් වීම වැදගත්ය. මෙයට අදාලව සතිපතා, මාස්පතා හෝ දෛනික වාර්තා කිරීම අවශ්‍ය වේ.
- **වැඩ සැලැස්ම** - රාජකාරි ආරම්භ කරන අවස්ථාවේදී සියලුදෙනා වැඩ ආරම්භ කරන බව හා වැඩ අවසන් කරන බව දැනුවත් කිරීමට ක්‍රමයක් භාවිතා කල හැකිය.
- **සෞඛ්‍යාරක්ෂාව** - නිවසේ සිට රාජකාරි කරන සේවකයින්ගේ සෞඛ්‍ය සහ සුවතාව ගැන සැලකිය යුතුය. සමහරවිට සේවකයන්ට තමා කාර්යාලයේ වැඩ කරන පරිගණකය හෝ අනෙකුත් උපාංග වඩාත් සුවපහසු වනු ඇත. එවන් අවස්ථාවකදී හැකිනම් එම සේවකයාට එම උපකරණ සපයා දීමෙන් ඔහුගේ ගුණාත්මක භාවය ඉහල නංවනු ඇත.
- **ආරක්ෂාව** - ආයතනික උපකරණ හරහා නිවසේ සිට වැඩ කරන අතතුරදී එම උපකරණ ආරක්ෂාව සහ ඒවායේ භාවිතය ගැන සේවකයා සහ ආයතනය අතර සන්නිවේදනයක් පවත්වාගත යුතුයි.
- **තාක්ෂණික සහය** - තොරතුරු තාක්ෂණ අංශයේ සහ අනෙකුත් සේවකයන්ගේ දුරකථන අංක සහ ඇමතිය හැකි ආකාර ගැන දැනුවත් කල යුතුයි. හදිසි අවශ්‍යතාවයකදී පහසුවෙන් එම පුද්ගලයන් හා සම්බන්ධ විය හැකි විය යුතුය.
- **සම්බන්ධතාවය** - පුද්ගලයන් අතර සම්බන්ධතාවය හොඳ මට්ටමක තබාගැනීමෙන් ආයතනික පරිසරයේදී ලෙසටම සියලුදෙනාට එකතුවී කටයුතු කල යුතුයි. සමාජ ජාල මෘදුකාංග හෝ වෙනත් සන්නිවේදන මෘදුකාංගයක් හරහා සේවකයන් අතර දුරස්ථභාවය අඩු කල හැකිය.

කෙසේවෙතත් නිවසේ සිට වැඩ කිරීම සියලුම දෙනාට පහසු කරුණක් නොවේ. එසේම ආයතනික පරිසරය සහ නිවසේ පරිසරය එකිනෙකට වෙනස් වීම අනිවාර්ය බැවින් එය යමෙකුට තරමක් දුෂ්කර වනු ඇත. නමුත් කෙසේ හෝ අත්‍යවශ්‍ය සේවා අවශ්‍යතා සඳහා අන්තර්ජාලය සහ අනෙකුත් තාක්ෂණික මෙවලම් හරහා පුද්ගලයන්ව සම්බන්ධ කර තබා ගැනීමට ආයතනික මටටමෙන් උත්සාහ කල යුතු අතර සේවකයන්ද මෙහිදී හැකිතාක් ඵලදායි ආකාරයෙන් නිවසේ සිට වැඩ කල යුතුය.

මෙම වසංගත තත්වය සියලු දෙනාට තම ජීවිතයේ පළමුවරට අත්දැකීමට සිදුවී තිබෙන තත්වයකි. මේ හරහා ආයතන වලට නව වැඩ කිරීමේ සංස්කෘතියක් හඳුනාගැනීමට සහ ක්‍රියාත්මක කිරීමට අවස්ථාව සැලසෙනු ඇත. එය බොහෝදුරට අනාගත ලෝකයේ ආරක්ෂාව සහ සුන්දරත්වය වැඩි කරනු ඇත.

සියලුදෙනාට ආරක්ෂා සහිත සෞඛ්‍යසම්පන්න ජීවිතයක් ප්‍රාර්ථනා කරමු. දැනුවත් වෙමු, ආරක්ෂා වෙමු, වගකීමෙන් කටයුතු කරමු!