MAS HR ප්‍රතිපත්ති අංකය	
ප්‍රතිපත්තියේ නම	තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තිය
ප්‍රතිපත්ති හිමිකරු	ප්‍රධාන තොරතුරු නිලධාරී
අවසන් සංශෝධනය	2018 දෙසැම්බර් 14
අනුමත කරන්නා	ප්‍රධාන තොරතුරු නිලධාරී
අනුමත කළ දිනය	2018 දෙසැම්බර් 14
බලපවත්වන දිනය	2019 ජනවාරි 01
සමාලෝචන දිනය	

MAS
CHANGE IS COURAGE

තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තිය

අන්තර්ගතය

1. අරමුණ 2
2. විෂය පථය 2
3. තොරතුරු ආරක්ෂණය යනු කුමක්ද? 3
4. තොරතුරු පද්ධති භාවිතය 3
5. සත්‍යාපනය 4
6. ඊමේල් සහ පණිවුඩ 6
7. අන්තර්ජාල භාවිතය 8
8. දුරස්ථ ප්‍රවේශ සේවාව 9
9. සමාගම සතු උපකරණ සඳහා MAS තොරතුරු තාක්ෂණ සේවා භාවිතා කිරීම 11
10. පුද්ගලිකව අයිති උපකරණ සඳහා MAS තොරතුරු තාක්ෂණ සේවා භාවිතා කිරීම 12
11. සමාගම් සතු දත්ත ගබඩා කිරීම සඳහා ෆ්ලෑෂ් ඩ්‍රයිව් සහ වෙනත් ඉවත් කළ හැකි මාධ්‍ය භාවිතා කිරීම . 15
12. ඇගයීම සහ විපරම් කිරීම 15
13. අනුකූල නොවීම් 16
14. වගකීම 16
15. MAS තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තියෙහි වලංගුභාවය 16
16. අර්ථ දැක්වීම් 17

MAS HR ප්‍රතිපත්ති අංකය	
ප්‍රතිපත්තියේ නම	තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තිය
ප්‍රතිපත්ති හිමිකරු	ප්‍රධාන තොරතුරු නිලධාරී
අවසන් සංශෝධනය	2018 දෙසැම්බර් 14
අනුමත කරන්නා	ප්‍රධාන තොරතුරු නිලධාරී
අනුමත කළ දිනය	2018 දෙසැම්බර් 14
බලපවත්වන දිනය	2019 ජනවාරි 01
සමාලෝචන දිනය	

MAS
CHANGE IS COURAGE

1. අරමුණ

1.1. MAS සිය සේවකයින්ට සහ බලයලත් තෙවන පාර්ශවයන්ට, එහි තොරතුරු පද්ධති සහ තොරතුරු තාක්ෂණ සේවාවන් වෙත ප්‍රවේශය, අවශ්‍යතාවය මත පදනම්ව සහ ඔවුන්ට පවරා ඇති රාජකාරි හා වගකීම් ඉටු කිරීමට අවශ්‍ය අවම වරප්‍රසාද අනුව, ආරක්ෂිත, ඵලදායී හා කාර්යක්ෂම ආකාරයකින් සපයයි.

- IT සේවා සතුව පහත දේ අඩංගු වේ:
- ලැප්ටොප්, ටැබ්ලට් සහ ඩෙස්ක්ටොප් පරිගණක සඳහා ප්‍රවේශය
- මුද්‍රණ සේවාවන් සඳහා ප්‍රවේශය
- ආයතනික විද්‍යුත් තැපැල් සේවාවන් සඳහා ප්‍රවේශය
- ව්‍යාපාර යෙදුම් සහ දත්ත සඳහා ප්‍රවේශය
- අන්තර්ජාලයට පිවිසීම සහ ක්ලවුඩ් ආචයනය
- අන්තර්ජාල සහ ගොනු හුවමාරු සඳහා ප්‍රවේශය
- ව්‍යාපාර යෙදුම් සඳහා දුරස්ථ ප්‍රවේශය
- විද්‍යුත් තැපැල් සේවාවන් සඳහා දුරස්ථ ප්‍රවේශය
- කථන සහ වීඩියෝ සම්මන්ත්‍රණ සඳහා ප්‍රවේශය

1.2. මෙම ප්‍රතිපත්තිය මඟින් MAS විසින් එහි සේවකයින්ට සහ තෙවන පාර්ශවීය පරිශීලකයින්ට සපයනු ලබන එවැනි තොරතුරු පද්ධති සහ තොරතුරු තාක්ෂණ සේවාවන්ගේ පිළිගත හැකි භාවිතය සඳහා පැහැදිලි, යුක්ති සහගත හා සාධාරණ ප්‍රමිතියක් ස්ථාපිත කරයි.

2. විෂය පථය

2.1. මෙම MAS තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තිය පහත සඳහන් පාර්ශවයන්ට / කණ්ඩායම් වලට අදාළ වේ:

- ගිවිසුම්ගත නියමයන් හෝ ගිවිසුම් ලිපි ("සේවකයින්") යටතේ MAS සමඟ සම්බන්ධ වී සිටින උපදේශකයින් සහ සීමාවාසිකයින් ඇතුළත්ව සියළුම ස්ථිර (ස්ථාවර කාලීන / කොන්ත්‍රාත් සේවකයින් ඇතුළුව), ස්ථිර නොවන සේවකයින්;
- උපදේශකයින්, විධායක නොවන අධ්‍යක්ෂවරුන් සහ උපදේශක මණ්ඩල සාමාජිකයින් (" උපදේශකයින්");
- MAS පරිශ්‍රයට පැමිණෙන සියළුම ආයතනික සහ තනි පුද්ගල ආගන්තුකයන් ("අමුත්තන්");
- MAS සමඟ ගනුදෙනු කරන සියලුම සැපයුම්කරුවන්, උප කොන්ත්‍රාත්කරුවන් සහ ඔවුන්ගේ නියෝජිතයින් ("සැපයුම්කරුවන්");
- MAS සමඟ සබඳතා දක්වමින් ගනුදෙනු කරන සියළු MAS පාරිභෝගිකයන් හා ඔවුන්ගේ නියෝජිතයන් ("ගනුදෙනුකරුවන්"); වෙත MAS තොරතුරු පද්ධති සහ IT සේවාවන්ට පිවිසුම් ලබා දී ඇත. (සහ එක්ව ගනිමින් "පරිශීලකයන්" ලෙස දක්වා ඇත).

2.2. MAS තොරතුරු පද්ධති පරිශීලකයින්ට සහ අදාළ තෙවන පාර්ශවයන්ට MAS තොරතුරු පද්ධති සහ තොරතුරු තාක්ෂණ සේවාවන් වෙත ප්‍රවේශය ලබා ගැනීමට පෙර මෙම තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තිය කියවීම, තේරුම් ගැනීම සහ විධිමත් ලෙස පිළිගැනීම අවශ්‍ය වේ.

2.3. MAS තොරතුරු පද්ධති භාවිතා කරන්නන් සහ තෙවන පාර්ශවයන් MAS හෝල්ඩින්ග්ස් තොරතුරු පද්ධති සහ තොරතුරු තාක්ෂණ සේවාවන් වෙත ප්‍රවේශ වීමේදී සෑම විටම රහස්‍යතා ප්‍රතිපත්තිය, තොරතුරු ආරක්ෂණ ප්‍රතිපත්තිය සහ මෙම තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තියට අනුකූල විය යුතුයි.

2.4. තොරතුරු ආරක්ෂණ ප්‍රතිපත්තිය හෝ මෙම තොරතුරු පද්ධති භාවිත ප්‍රතිපත්තිය හා අනුකූල නොවීම හෝ උල්ලංඝණය කිරීම තොරතුරු ආරක්ෂණ උල්ලංඝණයක් ලෙස සලකනු ලබන අතර විනය ක්‍රියාමාර්ගවලට තුඩු දිය හැකිය.

3. තොරතුරු සුරක්ෂිතතාවය යනු කුමක්ද?

3.1. තොරතුරු සුරක්ෂිතතාවය යනු සමාගමේ සංවේදී හා ව්‍යාපාරික තීරණාත්මක තොරතුරු වත්කම්, විද්‍යුත් හෝ භෞතික ස්වරූපයෙන්, අනවසරයෙන් ප්‍රවේශ වීම, භාවිතය, අනාවරණය කිරීම, කඩාකප්පල් කිරීම, වෙනස් කිරීම, බාධා කිරීම්, පටිගත කිරීම් හෝ විනාශ කිරීම් වලින් ආරක්ෂා කිරීමේ ක්‍රියාවලිය සහ පරිචාරය යි.

3.2. MAS හි තොරතුරු සුරක්ෂිතතාවයේ ප්‍රධාන අරමුණු වන්නේ පහත දෑ සහතික කිරීමයි:

3.2.1. **තොරතුරු වල රහස්‍යභාවය -** පාරිභෝගික, සැපයුම් සහ MAS හි සංවේදී තොරතුරු ලබා ගත හැක්කේ එවැනි තොරතුරු ලබා ගැනීමට බලයලත් අයට පමණි.

3.2.2. **තොරතුරු වල සම්පූර්ණ බව -** පාරිභෝගික, සැපයුම්කරු සහ MAS ව්‍යාපාර තීරණාත්මක තොරතුරු නිරවද්‍ය, දෝෂ රහිත සහ අතපසු වීම් නොමැතිව පවතිනු ඇත.

3.2.3. **තොරතුරු ලබා ගැනීමේ හැකියාව** - බලයලත් පරිශීලකයින්ට අවශ්‍ය විටෙක තීරණාත්මක ව්‍යාපාරික තොරතුරු වෙත ප්‍රවේශය තිබිය යුතුය; සහ

3.2.4. **ඉලෙක්ට්‍රොනික ගනුදෙනු ප්‍රතික්ෂේප නොකිරීම -** විද්‍යුත් ගනුදෙනු වලදී ඔවුන්ගේ ක්‍රියාවන්ට පරිශීලකයින් වගකිව යුතුය.

සැ.යු: තොරතුරු වත්කම යනු කිසියම් ආකාරයකින් ගබඩා කර ඇති නිශ්චිත තොරතුරු කොටසක් වන අතර එය සමාගමට 'වටිනා' ලෙස පිළිගැනේ.

4. තොරතුරු පද්ධතිය භාවිතය

4.1. MAS තොරතුරු තාක්ෂණ පද්ධති සහ තොරතුරු වත්කම් සොරකම් කිරීමෙන් හා / හෝ අහම්බෙන් සිදුවන හානිවලින් ආරක්ෂා කිරීමට පරිශීලකයින් නිසි සැලකිල්ලක් දැක්විය යුතුය.

4.1.1. ඩෙස්ක්ටොප්, ලැප්ටොප්, ජංගම උපාංග, මුද්‍රණ යන්ත්‍ර, ෆැක්ස් යන්ත්‍ර, ඡායා පිටපත් යන්ත්‍ර, මෙන්ම ජාල, සේවාදායක සහ යෙදුම් ඇතුළුව සියලුම MAS තොරතුරු පද්ධති භාවිතා කළ යුත්තේ අපේක්ෂිත හා බලයලත් ව්‍යාපාරික අරමුණු සඳහා පමණි.

4.1.2. අයුතු හෝ නීති විරෝධී අරමුණු සඳහා MAS තොරතුරු පද්ධති භාවිතා කිරීමට පරිශීලකයින්ට අවසර නොමැත.

4.2. IT පද්ධතිවල අයුතු හෝ නීති විරෝධී භාවිත

තොරතුරු තාක්ෂණ පද්ධති නීතිවිරෝධී හෝ නීති විරෝධී ලෙස භාවිතා කිරීමට: ප්‍රකාශන හිමිකම් උල්ලංඝණය කිරීම, වංචාව, අපහාස කිරීම, රචනා සොරකම, හිරිහැර කිරීම, බිය ගැන්වීම, අසභ්‍ය වචන, ව්‍යාජ ලේඛන, ව්‍යාජ ලෙස පෙනී සිටීම, සූදුව, පරිගණක හිරිහැර කිරීම (උදා: පරිගණක වෛරස් පැතිරීම ආදිය) හෝ අනවසර පරිගණක ප්‍රවේශය ඇතුළත් නමුත් ඒවාට පමණක් සීමා නොවේ.

4.3. පරිශීලකයන් ප්‍රධාන තොරතුරු නිලධාරියා විසින් පූර්ව-අනුමත කරන ලද සහ නිසි පරිදි බලය සපයන ලද බලපත් සහිත මෘදුකාංග පමණක්ම ස්ථාපනය කළ යුතුයි.

4.3.1. පරිපාලන අයිතිවාසිකම් (administrative rights) ඇති පරිශීලකයින් MAS ජාල සහ තොරතුරු වත්කම් ආරක්ෂා කිරීම සඳහා ක්‍රියාත්මක කරන ලද ප්‍රති-වයිරස මෘදුකාංග, ප්‍රොක්සි සර්වර් සහ ෆයර්වෝල් වැනි කිසිදු පාලනයක් අක්‍රීය කිරීම හෝ පසු කිරීම නොකළ යුතුය.

4.3.2. පරිශීලකයින් MAS, එහි සැපයුම්කරුවන් හෝ ගනුදෙනුකරුවන් පිළිබඳ සංවේදී හෝ රහස්‍ය තොරතුරු සමාජ මාධ්‍ය වෙබ් අඩවි, චැට් සේවා, තැපැල් ලැයිස්තු, බ්ලොග් හෝ පොදු ප්‍රවෘත්ති කණ්ඩායම් (news groups) වැනි පොදු ප්‍රවේශ විය හැකි අන්තර්ජාල වෙබ් අඩවි වල පළ නොකළ යුතුය.

4.3.3. MAS, එහි සැපයුම්කරුවන් හෝ ගනුදෙනුකරුවන් පිළිබඳ තොරතුරු ප්‍රසිද්ධියේ ප්‍රවේශ විය හැකි අන්තර්ජාල වෙබ් අඩවි වල පළ කිරීමට අදහස් කරන ඕනෑම පරිශීලකයෙකු පළමුව **සමූහ ආයතනික සන්නිවේදන අංශය (Group Corporate Communications)** වෙතින් අනුමැතිය ලබා ගත යුතුය.

4.3.4. කිසියම් හිමිකාර ද්‍රව්‍යයක් (proprietary material) භාවිතා කිරීමට පෙර පරිශීලකයින් සුදුසු බුද්ධිමය දේපල අයිතිවාසිකම් / ප්‍රකාශන හිමිකම් හෝ ගිවිසුම්ගත අවසර ලබා ගත යුතුය.

4.3.5. ප්‍රමාණවත් ආරක්ෂණ පාලනයකින් තොරව පරිශීලකයින් ජාලය හරහා සංවේදී හෝ රහස්‍ය තොරතුරු සම්ප්‍රේෂණය නොකළ යුතුය. අවශ්‍ය නම්, පරිශීලකයා පළමුව **සමූහ ආයතනික සන්නිවේදන අංශයෙන්** අනුමැතිය ලබා ගත යුතුය.

සැ.යු: සංවේදී හෝ රහස්‍ය තොරතුරු සන්නිවේදනය කිරීමේදී පරිශීලකයෙකුට සහාය අවශ්‍ය නම්, ඔහු හෝ ඇය තොරතුරු තාක්ෂණ උපකාරක කවුළුව හෝ SBU / අංශයෙහි තොරතුරු තාක්ෂණ නියෝජිතයා සම්බන්ධ කර ගත යුතුය.
සැ.යු: පරිශීලකයින් ප්‍රසිද්ධියේ, කිසිදු MAS , එහි සැපයුම්කරුවන්ගේ හෝ ගනුදෙනුකරුවන්ගේ සංවේදී හෝ රහස්‍ය තොරතුරු හෙළි කිරීම හෝ සන්නිවේදනය නොකළ යුතුය.

5. සත්‍යාපනය

සත්‍යාපනය යනු MAS පද්ධති වෙත ප්‍රවේශ වන්නේ ඔබ බවට ආයතනය විසින් හඳුනා ගන්නා ආකාරයයි.

ආයතනය පුරාවට තීරණාත්මක දත්තවල ආරක්ෂාව වැඩි කිරීමට උපකාරී වන විවිධ විසඳුම් MAS සිය අභිමතය පරිදි හඳුන්වා දෙනු ඇත. මෙම මෙවලම් මඟින් එක් එක් යෙදුම තුළ පරිශීලකයා විසින් සිදුකරන ප්‍රවේශය සහ ක්‍රියාකාරකම් පිළිබඳ තත්‍ය කාලීන දෘශ්‍යතාව සහ පාලනය ලබා දෙයි. කිසියම් සැක කටයුතු ක්‍රියාවක් අනාවරණය වුවහොත් අනන්‍යතා අවහිර වන අතර, එවැනි අවස්ථාවලදී, පරිශීලකයින් ගිණුම් අවහිරය ඉවත් කරලීම සඳහා ඔවුන්ගේ තොරතුරු තාක්ෂණ පරිපාලකයින් සම්බන්ධ කර ගත යුතුය.

5.1. මුරපද ආරක්ෂණය

තමන්ගේ පිවිසුම් හිණුම් යටතේ සිදුවන සියලුම සිදුවීම් සඳහා පරිශීලකයින් පෞද්ගලිකව වගකිව යුතුය. එබැවින්, තම මුරපද රහස්‍යව තබා ගැනීම පරිශීලකයින්ගේ වගකීම වේ.

5.1.1. කිසිදු අවස්ථාවක පරිශීලකයින් තම මුරපදය වෙනත් පුද්ගලයෙකුට (තොරතුරු තාක්ෂණ කාර්ය මණ්ඩලය, සේවා සපයන්නන්, ඉහළ නිලධාරීන්, වෙනත් සම සේවකයින්, මිතුරන් හෝ පවුලේ සාමාජිකයන් ඇතුළුව) ලබා දීමට, පැවසීමට, බෙදා ගැනීමට හෝ ඉඟි කිරීමට කටයුතු නොකළ යුතුය.

5.1.2. පරිශීලකයන් යෙදුම්වල (Internet explorer, විද්‍යුත් තැපැල් වැඩසටහන් ආදියේ) ඇති “remember password” විශේෂාංගය භාවිතා නොකළ යුතුය.

5.1.3. පරිශීලකයින් සෑම දින 60 කට වරක් මුරපද වෙනස් කළ යුතුය. වෙනස් වූ පසු, එය නැවත වෙනස් කිරීමට පරිශීලකයාට පැය 24 ක් බලා සිටීමට සිදු වනු ඇත.

5.1.4. පරිශීලකයින්ට පහසුවෙන් මතක තබා ගත හැකි නමුත් වෙනත් කිසිවෙකුට අනුමාන කිරීමට අපහසු නව මුරපද භාවිතා කළ යුතුය.

5.1.5. පැහැදිලි පෙළ මුරපද පොදු අන්තර්ජාල සම්බන්ධතා හරහා සම්ප්‍රේෂණය නොකළ යුතුය.

5.1.6. පරිශීලකයන් මුරපද ලෙස ශබ්ද කෝෂ වචන හෝ සංයෝජන භාවිතා නොකළ යුතුය.

5.1.7. සමාගම් ජාලයට ප්‍රවේශ වීම සඳහා පරිශීලකයින් පුද්ගලික අරමුණු සඳහා (හොට්මේල්, ජීමේල්, ස්කයිප් හෝ අන්තර්ජාල බැංකුකරණය වැනි) භාවිතා කරන මුරපද භාවිතා නොකළ යුතුය.

5.1.8. පරිශීලකයින් දිගු මුරපද භාවිතා කළ යුතු අතර, ඒවා අක්ෂරාංක හා විශේෂ අක්ෂර මිශ්‍ර කර සකසා ගත යුතුයි. ප්‍රකට හෝ පහසුවෙන් ප්‍රවේශ විය හැකි පුද්ගලික තොරතුරු (කලත්‍රයාගේ නම, සුරතලාගේ නම, මැද නම, දරුවාගේ නම ආදිය) මත මුරපද පදනම් නොවිය යුතුය.

5.1.9. සංකීර්ණ මුරපදයක ලක්ෂණ

- මුරපද අක්ෂර 8 කට වඩා දිගු විය යුතුය;
- මුරපදයේ පහත දේ ඇතුළත් විය යුතුය:
  - කැපිටල් හෝ සිම්පල් අක්ෂර හෝ අක්ෂරාංක (A-Z, a-z);
  - සංඛ්‍යා (0-9); සහ
  - විශේෂ අක්ෂර (!@#$%^&*)

5.1.10. පරිශීලකයන් තම මුරපද යළි සැකසීමට හෝ වෙනස් කිරීමේදී Password Self-Service Portal හරහා මුරපද ස්වයං සේවා පහසුකම ලබා ගත යුතුය.

5.2. බහුසාධක සත්‍යාපනය (MULTI FACTOR AUTHENTICATION / MFA) - අනිවාර්ය සාධකයක් ලෙස ඇතැම් යෙදුම් සඳහා අනන්‍යතා MFA යොදාගෙන ආරක්ෂා කර ඇත. සහාය නොදක්වන / පැරණි යෙදුම් App password හරහා සත්‍යාපනය කළ යුතුය.

පරිශීලකයින් ඔවුන්ගේ මුරපදය සමඟ MAS විසින් පිරිනමනු ලබන ඕනෑම සේවාවක් හෝ MFA ආරක්ෂිත යෙදුමකට ලොගින් වන විට, ලියාපදිංචි කර ඇති උපාංගයකින් එම ප්‍රවේශ වීම තහවුරු කිරීම සිදුකළ යුතුය. මෙම කටයුත්ත සඳහා, පරිශීලකයින් ඔවුන්ගේ දෙවන සත්‍යාපන ක්‍රමය ලෙස පහත සත්‍යාපන විකල්ප එකක් හෝ කිහිපයක් සැකසිය යුතුය.

- සත්‍යාපන දුරකථනය
- කාර්යාලීය දුරකථනය

- විකල්ප සත්‍යාපන දුරකතනය
- සත්‍යාපන App එක

සැ.යු. පරිශීලකයෙකු ඔහුගේ / ඇයගේ මුරපදය අන්සතු වී ඇති බව දන්නේනම් හෝ සැක කරන්නේ නම්, එය තොරතුරු තාක්ෂණ උපකාරක මණ්ඩලයට හෝ SBU / අංශයෙහි තොරතුරු තාක්ෂණ නියෝජිතයාට වාර්තා කළ යුතු අතර මුරපදය වහාම වෙනස් කළ යුතුය.

6. විද්‍යුත් තැපැල් සහ පණිවිඩ යැවීම

MAS හි අරමුණු හා අරමුණු සමඟ සහයෝගයෙන් කටයුතු කිරීම සහ ඉදිරියට ගෙනයාම සඳහා මෙන්ම ව්‍යාපාර හා භූමිකාව මත පදනම් වූ කාර්යයන් ඉටු කිරීම සඳහා සමාගම විසින් සපයන ලද ඊමේල්, පණිවිඩ යැවීම සහ ආයතනික සමාජ ජාල සේවා භාවිතා කිරීමට පරිශීලකයින් දිරිමත් කරනු ලැබේ.

6.1. MAS, එහි සැපයුම්කරුවන් හෝ ගනුදෙනුකරුවන්ගේ සංවේදී හෝ රහස්‍ය තොරතුරු අනාවරණය නොකිරීමට සමාගම විසින් සපයන ලද ඊමේල්, පණිවිඩ යැවීම සහ ආයතනික සමාජ ජාල මෙවලම් හරහා බෙදාහදා ගන්නා හෝ පළ කරන ඕනෑම අන්තර්ගතයක් පිළිබඳව පරිශීලකයින් නිතරම සැලකිලිමත් විය යුතුය.

6.1.1. පරිශීලකයින් නිල නොවන අරමුණු සඳහා හෝ නිල නොවන විද්‍යුත් තැපැල් යැවීමේ ක්‍රමයක් ලෙස සමාගම් විද්‍යුත් තැපෑල භාවිතා නොකළ යුතුය

6.1.2. නිල නොවන අරමුණු සඳහා, පුද්ගලික භාවිතය සඳහා ප්‍රවේශ වීමක් ලෙස, හෝ පුද්ගලික වෙබ් අඩවි වලට පිවිසීමේ ක්‍රමයක් ලෙස සහ හිමිකාරිත්වය ඇති, ඕනෑම පරිගණකයක මෘදුකාංග සඳහා සමාගම විසින් සපයන ලද විද්‍යුත් තැපැල් ලිපිනය භාවිතා නොකළ යුතුය.

6.1.3. සමූහ ආයතනික සන්නිවේදන අංශයේ පැහැදිලි අනුමැතියකින් තොරව කාර්යාල කටයුතු හා සම්බන්ධ අරමුණු සඳහා අදාළ නොවන අන්තර්ගතයන් සංසරණය නොකළ යුතුය.

6.2. MAS තුළදී, ආයතනය විසින් සැපයූ ඊමේල් ලිපිනය හා මයික්‍රොසොෆ්ට් කණ්ඩායම සපයන සේවා ඇති Microsoft 365, මෙන්ම Yammer, ආයතනික විද්‍යුත් සන්නිවේදනයන් සඳහා නිල ක්‍රමවේදය සේ සැලකෙන අතර පරිශීලකයන් ඊමේල් බැලීම, කණ්ඩායම් සන්නිවේදනය හා Yammer පළ කිරීම් සඳහා, නිරන්තර හා කාලීන අවධානය යොමුකරමින් පත්කිරීම්, වැඩ කටයුතු, පණිවිඩ හා දැනුම්දීම් පිළිබඳව දැනුවත්ව සිටීම අපේක්ෂා කෙරේ.

6.3. පිළිවෙළ කිරීම්, සුරක්ෂණය හෝ නිෂ්කාෂණය කිරීම් ඇතුළු මේල් බොක්ස් කළමනාකරණ වගකීම පරිශීලකයන් සතුය.

6.3.1. ඊමේල් ප්‍රමාණයේ සීමාකාරී මට්ටමක් තිබේ. කරුණාකර ඔබේ තොරතුරු තාක්ෂණ නියෝජිතයාගේ සහාය ලබාගන්න.

6.3.2. ඊ-තැපැල් කළමනාකරණය කරන්නේ ක්ලවුඩ් එක හරහායි. පුද්ගලික ෆෝල්ඩරවල මේල් නඩත්තු කිරීමට තවමත් අදහස් කරන පරිශීලකයින් එවැනි ඊමේල් කළමනාකරණය සහ උපස්ථ (backup) කිරීම සඳහා වගකිව යුතුය.

6.4. ඔබගේ විද්‍යුත් තැපැල් ගිණුම / මුරපදය ආරක්ෂා කිරීම

6.4.1. විද්‍යුත් තැපැල් ගිණුම සහ මුරපදය විද්‍යුත් තැපැල් පද්ධතියට පරිශීලකයෙකු අනන්‍ය ලෙස හඳුනා ගනී. විද්‍යුත් තැපැල් ගිණුම භාවිතයෙන් සිදුකරන ඕනෑම ක්‍රියාවක් පද්ධතිය තුළ නිශ්චිත පරිශීලකයෙකු විසින් කරනු ලබන ක්‍රියාවන් ලෙස දක්වනු ඇත. එබැවින්, සම්මුති විරහිත හෝ හවුල් ඊමේල් ගිණුමක් භාවිතා

කරමින් වංචනික හෝ අනවසර ක්‍රියාකාරකමක් සිදු වුවහොත් එම විද්‍යුත් තැපැල් ගිණුමේ නිශ්චිත හිමිකරුට වරද පැටවේ.

6.5. MAS හි විද්‍යුත් තැපැල් ප්‍රවේශය පාලනය වන්නේ තනි ගිණුම් සහ මුරපද හරහා ය. තමන්ගේ ගිණුමේ රහස්‍යභාවය සහ මුරපද තොරතුරු ආරක්ෂා කිරීම පරිශීලකයාගේ වගකීම වේ.

6.6. ව්‍යාපාරයට සම්බන්ධ සියලුම විද්‍යුත් තැපැල් සන්නිවේදනයන්හි දී පරිශීලකයින් සංවිධානයේ සුදුසු වියාචනයන් සමඟ සම්මත ඊමේල් අත්සන අච්චුව (signature template) භාවිතා කළ යුතුය.

6.7. අවසර දී ඇත්නම් මිස වෙනත් පරිශීලකයෙකුගේ ඊමේල් ගිණුමක් එම පරිශීලකයා වෙනුවෙන් භාවිතා කිරීමට වෙනත් අයෙක්ට අවසර නැත.

6.8. පරිශීලකයින් නොදන්නා හෝ විශ්වාසදායක නොවන ප්‍රභවයන්ගෙන් ලැබෙන ඊමේල් සහ ඇමුණුම් විවෘත කිරීම, ක්‍රියාත්මක කිරීම හෝ ගබඩා කිරීම නොකළ යුතු අතර එවැනි විද්‍යුත් තැපැල් හෝ ඇමුණුම් තොරතුරු තාක්ෂණ උපකාරක කවුළුවට වාර්තා කළ යුතුය.

සංවිධානයෙන් පිටත සිට පණිවිඩය පැමිණ ඇති බව දැක්වීමට බාහිරව ආරම්භ වූ සියලුම ඊමේල් "[External Email]" (එක්ස්ටර්නල් ඊමේල්) යන ටැගයෙන් යුතුවේ.

6.9. රහස්‍ය හෝ සංවේදී අන්තර්ගතයන් හෝ ඇමුණුම් අඩංගු ඊමේල් ආරක්ෂා කර රහස්‍යතා ප්‍රතිපත්තියට අනුකූලව හැසිරවිය යුතුය.

6.10. ව්‍යාපාරික පණිවුඩකරණ කටයුතු සඳහා පුද්ගලික විද්‍යුත් තැපැල් සේවා (හොට්මේල්, යාහූ මේල් හෝ ජීමේල් වැනි) භාවිතා කිරීමට පරිශීලකයින්ට අවසර නැත.

6.11. පරිශීලකයින් තොරතුරු ආරක්ෂණ සඳහා සංවිධානයේ නීති උල්ලංඝණය කිරීමේ අවදානම දරා ගත යුතු බැවින් ව්‍යාපාරික අරමුණු සඳහා සමාජ මාධ්‍ය ජාල හෝ පොදු චැට් සේවා (වට්ස්ඇප්, ස්කයිප්, ගූගල් ටෝක් ආදිය) භාවිතා කිරීමේදී පරිශීලකයින් ප්‍රවේශම් විය යුතුවේ, වැඩි විස්තර සඳහා කරුණාකර **සමාජ මාධ්‍ය ප්‍රතිපත්තිය** බලන්න.

6.12. පොදු උපාංග-යෙදුම් (device-apps) සහ සේවාවන් භාවිතා කිරීමට තීරණය කිරීමට පෙර ඒවාට සමාන නිර්දේශිත උපාංග-යෙදුම් සහ සේවාවන් තිබේදැයි පරීක්ෂා කිරීම සඳහා පරිශීලකයින් නිරන්තරයෙන් ඔවුන් තොරතුරු තාක්ෂණ සහාය කණ්ඩායම් උපදෙස් පැතිය යුතුය.

6.13. පරිශීලකයින්ට ඔවුන්ගේ කාර්යාල ඊමේල් ලිපින භාවිතා කරමින් පොදු සමාජ මාධ්‍ය වෙබ් අඩවි, චැට් සේවා, තැපැල් ලැයිස්තු හෝ ප්‍රවෘත්ති කණ්ඩායම් වෙත කිසිදු අන්තර්ගතයක් හෝ අදහස් දැක්වීමට අවසර නැත. සාමාන්‍ය රාජකාරී කටයුතුවලදී එවැනි පළ කිරීමක් අවශ්‍ය නම්, සමූහ ආයතනික සන්නිවේදනයන්ගෙන් සුදුසු පූර්ව අනුමැතිය ලබා ගත යුතුය.

6.14. රහස්‍ය / සංවේදී ඊමේල් ආරක්ෂා කිරීම

රහස්‍ය හා සංවේදී විද්‍යුත් තැපැල් අන්තර්ගතයන් සහ ඇමුණුම් අනවසර ප්‍රවේශ වීම් වලින් වළක්වා ගැනීම සඳහා තම විද්‍යුත් තැපැල් සහ කාර්යාල යෙදුම් සමඟ සපයා ඇති තොරතුරු ආරක්ෂණ ක්‍රියාකාරිත්වය භාවිතා කිරීමට පරිශීලකයින් උනන්දු කරනු ලැබේ.

6.15. පරිශීලකයින් MAS සමඟ ඇති සම්බන්ධය අවසන් කළ විට පරිශීලකයින්ගේ විද්‍යුත් තැපෑල, පණිවිඩ යැවීම සහ ආයතනික සමාජ ජාල ප්‍රවේශය අහෝසි වේ.

සැ.යු: ඵලදායිතාව සහ පහසුව වැඩි දියුණු කිරීම සඳහා පුද්ගලික පරිගණක / ලැප්ටොප් සහ ජංගම උපාංග භාවිතා කරමින් පරිශීලකයින්ට ඔවුන්ගේ ආයතනික විද්‍යුත් තැපැල් ලිපිනයට ප්‍රවේශ වීමට අවසර ඇත. කෙසේ වෙතත්, ආයතනික විද්‍යුත් තැපැල් වෙත ප්‍රවේශ වීමට සහ භාවිතා කිරීමට යොදා ගන්නා සියලුම පුද්ගලික උපාංග සෑම විටම ආරක්ෂිත බව පරිශීලකයින් සහතික කළ යුතුය. පුද්ගලිකව අයිති උපාංගවල MAS තොරතුරු තාක්ෂණ සේවාවන් භාවිතා කිරීම බලන්න.

සැ.යු: නැතිවූ හෝ අස්ථානගත වූ උපාංග තිබේ නම්, පරිශීලකයින් වහාම තොරතුරු තාක්ෂණ උපකාරක සේවාවට හෝ SBU / අංශ තොරතුරු තාක්ෂණ නියෝජිතයාට දැනුම් දී මුරපදය වෙනස් කළ යුතුය.

සමාගම විසින් සපයනු ලබන සහයෝගිතා මෙවලම් හෝ පොදු ප්‍රවේශ කළ හැකි වෙබ් අඩවි, සමාජ මාධ්‍ය වෙබ් අඩවි, තැපැල් ලැයිස්තුව (mailing list) හෝ ප්‍රවෘත්ති කණ්ඩායම් තුළ ඇති MAS, එහි සැපයුම්කරුවන්ගේ හෝ ගනුදෙනුකරුවන්ගේ සංවේදී හෝ රහස්‍ය තොරතුරු පරිශීලකයින් දුටුවහොත්, වහාම ඒ බව තොරතුරු තාක්ෂණ උපකාරක සේවාව වෙත වාර්තා කළ යුතුය.

7. අන්තර්ජාල භාවිතය

7.1. MAS හි අරමුණු හා අරමුණු ඉදිරියට ගෙනයාමට මෙන්ම ව්‍යාපාර හා රැකියාව මත පදනම් වූ කාර්යයන් ඉටු කිරීම සඳහා අන්තර්ජාලය භාවිතා කිරීමට පරිශීලකයින් දිරිමත් කරනු ලැබේ. කෙසේ වෙතත්, පරිශීලකයින් ඔවුන් බෙදා හරින අන්තර්ගතයට හෝ MAS විසින් සපයනු ලබන අන්තර්ජාල සේවාවන් හරහා ප්‍රවේශ වන තොරතුරු වලට පූර්ණව වගකිව යුතුය.

7.2. පරිශීලකයින් MAS විසින් සපයන ලද අන්තර්ජාල සේවා භාවිතා කළ යුත්තේ ව්‍යාපාර ආශ්‍රිත ක්‍රියාකාරකම් සඳහා පමණි. එවැනි සේවාවක් නීති විරෝධී හෝ ව්‍යාපාරික නොවන ලෙස භාවිතා කිරීමට අවසර නැත.

7.3. අන්තර්ජාල සේවා ලොග් සටහන් තැබීම හා නිරීක්ෂණය

MAS අන්තර්ජාල සේවාව භාවිතයෙන් සිදුකරන සියලුම පරිශීලක ක්‍රියාකාරකම් ව්‍යාභිචාර සහ අනවසර ක්‍රියාකාරකම් හඳුනා ගැනීම සඳහා පටිගත කිරීම, නඩත්තු කිරීම සහ විශ්ලේෂණය කිරීම, සහ වරදකාරී ක්‍රියාවන්ට එරෙහිව ප්‍රතිකර්ම හෝ විනය ක්‍රියාමාර්ග ගැනීම.

7.3.1. සමාගම සපයන ලැප්ටොප් සහ ඩෙස්ක්ටොප් පරිගණකවල පරිශීලකයින් අන්තර්ජාල ප්‍රවේශ සැකසුම් සහ වින්‍යාස වෙනස් කිරීම හෝ වෙනස් කිරීමට උත්සාහ කිරීම නොකළ යුතුය.

7.3.2. MAS අන්තර්ජාල ආරක්ෂණ පාලනයන් මඟ හරින යෙදුම් ස්ථාපනය කිරීම හෝ භාවිතා කිරීම පරිශීලකයින්ට තහනම්ය.

7.3.3. සමාගම සපයන ලැප්ටොප් සහ ඩෙස්ක්ටොප් පරිගණකවල ගොනු හුවමාරුව, සෘජු පරිගණක සබඳතා (peer-to-peer), කතාබස් සහ පණිවිඩ යෙදුම් ස්ථාපනය කිරීම හෝ භාවිතා කිරීම පරිශීලකයින්ට තහනම්ය.

7.3.4. අන්තර්ජාලයෙන් අනවසර අන්තර්ගතයන් හෝ පුද්ගලික අන්තර්ගතයන් බාගත කිරීමට හෝ ක්‍රියාත්මක කිරීමට පරිශීලකයින් MAS අන්තර්ජාල සම්බන්ධතාවය භාවිතා නොකළ යුතුය.

7.3.5. ස්ථානීය රැහැන් ජාල සම්බන්ධතාවයක් හරහා හෝ ස්ථානීය රැහැන් රහිත ජාල සම්බන්ධතාවයක් හරහා MAS සමාගම් ජාලයට භෞතික ප්‍රවේශය ලබා ගත නොහැකි අවස්ථාවකදී ම පමණක් MAS සපයන ලද ඩොන්ගල් භාවිතයට ගත යුතුයි.

7.3.6. මාර්ගගත (online) වංචා ක්‍රමවේදයන් සහ අන්තර්ජාලය පදනම් කරගත් වෙනත් තර්ජන පිළිබඳව පරිශීලකයින් නිරන්තරයෙන් දැනුවත්ව සිටිය යුතුය. අන්තර්ජාලය, විශේෂයෙන් වෙබ් අඩවි හෝ යෙදුම් වෙත ප්‍රවේශ වන විට පරිශීලකයින් ප්‍රවේශම් විය යුතු අතර සාධාරණ සැක සහිත ක්‍රියා කළ යුතුය.

7.3.7. ඊමේල් සහ MAS විසින් සපයන ලද ගොනු ගබඩා ස්ථාන (උදා: Office 365 සතු One Drive / Share point) ආදී MAS යෙදුම් සමඟ ප්‍රවේශවීමේදී හා ගනුදෙනු කිරීමේදී පරිශීලකයින් කිසි විටෙක ඩෙස්ක්ටොප්, ලැප්ටොප්, ස්මාර්ට්ෆෝන් සහ ටැබ්ලට් උපාංගවල වාණිජ්‍යමය වශයෙන් නිදහස් හෝ ගෙවන ලද අන්තර්ජාල VPN යෙදුම් භාවිතා නොකළ යුතුය,.

7.3.8. පරිශීලකයන් අන්තර්ජාල භාවිතයේදී ඇතිවන දෝෂ, ගැටළු සියල්ල තොරතුරු තාක්ෂණ උපකාර සේවාවට හෝ SBU/අංශ IT නියෝජිතයාට දැන්විය යුතුය.

7.3.9. පරිශීලකයින් MAS ආශ්‍රිත පිටු හෝ සමාජ මාධ්‍ය ගිණුම් නිර්මාණය කිරීම හෝ MAS ආශ්‍රිත අන්තර්ගතයන් සමාජ වෙබ් අඩවි වල හෝ වෙනත් අන්තර්ජාල මුහුණුවරකින් පළ කිරීම හෝ MAS ආශ්‍රිත අන්තර්ගතයන් අඩංගු කර ගැනීම සඳහා තනිවම වෙබ් අඩවියක් නිර්මාණය කිරීම නොකළ යුතුය. පරිශීලකයා වැනි අවශ්‍යතා සමූහ ආයතනික සන්නිවේදන අංශය වෙත යොමු කළ යුතුය.

සැ.යු.කාර්යාලයෙන් පිටත සිට අන්තර්ජාලයට පිවිසීමේදී, සපයන ලද ලැප්ටොප් පරිගණක භාවිතා කරන විට හෝ පුද්ගලික පරිගණක, ලැප්ටොප් හෝ වෙනත් ජංගම පරිගණක උපාංග භාවිතා කිරීමේදී ප්‍රවේශම් වන්නැයි පරිශීලකයින්ට උපදෙස් දෙනු ලැබේ. ව්‍යාජ වෙබ් අඩවි වලට පරිශීලකයා ආකර්ෂණය කර ගැනීමට, අනවසර මෘදුකාංග ස්ථාපනය කිරීමට, පරිගණක වෛරස් පැතිරවීමට, මුරපද සොරකම් කිරීමට සහ / හෝ සංවේදී සමාගම් සහ පුද්ගලික තොරතුරු වෙත ප්‍රවේශය ලබා ගැනීමට දැනුමැති ප්‍රහාරකයෙකුට නවීන තාක්ෂණික ක්‍රම භාවිතා කළ හැකිය.

8. දුරස්ථ පිවිසුම් (Remote Access) සේවාව

හඳුනාගත් පරිශීලකයින්ට දුරස්ථ ප්‍රවේශ සේවාව මඟින් කාර්යාල ජාලයෙන් පිටත සිට විද්‍යුත් තැපැල් සහ වෙනත් ව්‍යාපාරික යෙදුම් වෙත ප්‍රවේශය ලබා දේ. ලබා දී ඇති වැනි පිවිසුම් ව්‍යාපාර අවශ්‍යතාවයන් මත සහ පවරා ඇති රැකියා වගකීම් ඉටු කිරීමට අවශ්‍ය අවම වරප්‍රසාද අනුව පදනම් වේ.

8.1. ඵලදායිතාව ඉහළ නැංවීම සහ පහසුව වැඩි දියුණු කිරීම සඳහා දුරස්ථ ප්‍රවේශ පහසුකම් භාවිතා කිරීමට පරිශීලකයින් දිරිමත් කරනු ලැබේ. කෙසේ වෙතත්, සමාගමේ අරමුණ සහ අභිප්‍රාය සඳහා පමණක් දුරස්ථ ප්‍රවේශ සේවාව වගකිවයුතු, විශ්වාසදායක සහ ආරක්ෂිත ආකාරයකින් භාවිතා කරන බවට වග බලා ගැනීම පරිශීලකයින්ගේ වගකීම වේ.

8.2. පුද්ගලික හෝ සමාගම විසින් සපයනු ලබන ව්‍යාපාරික ක්‍රියාකාරකම් සඳහා භාවිතා කරන සියලුම දුරස්ථ පරිගණක උපකරණ සහ ජංගම උපාංග අනවසරයෙන් ප්‍රවේශ වීම හෝ අනිසි ලෙස භාවිතා කිරීම වළක්වා ගැනීම සඳහා භෞතික හා තාක්ෂණික ආරක්ෂක පාලනයන් සමඟ ක්‍රියාත්මක කළ යුතුය.

8.3. එවැනි පරිගණක / උපාංගවල සුදුසු ප්‍රති-වයිරස මෘදුකාංග ස්ථාපනය කර, යාවත්කාලීන කරමින් ඵලදායී ලෙස ක්‍රියාත්මක වීමට ඉඩ සැලසිය යුතුය.

8.4. එවැනි පරිගණක / උපාංග සඳහා සමාගම විසින් අනුමත කරන ලද පුද්ගලික ෆයර්වෝලයක් ස්ථාපනය කර, යාවත්කාලීන කර ඵලදායී ලෙස ක්‍රියාත්මක කළ යුතුය

8.5. ප්‍රති-වයිරස සහ පුද්ගලික ෆයර්වෝල්

බොහෝ නවීන පරිගණක / උපාංග මෙහෙයුම් පද්ධති ප්‍රති-වයිරස තාක්ෂණයන් සහ පුද්ගලික ෆයර්වෝල් සඳහා සහය දක්වයි. ප්‍රති-වයිරස සහ පුද්ගලික ෆයර්වෝල් මඟින් අසාමාන්‍ය හැසිරීම් සඳහා පද්ධතිය සහ සම්බන්ධතා නිරීක්ෂණය කරනු ඇති අතර අවහිර කිරීම් / දැනුම්දීම් කරනු ඇත.

8.5.1. පරිගණක / පරිගණක උපාංග ඒවා සහය දක්වන මෙහෙයුම් පද්ධතියේ නවතම අනුවාදය ක්‍රියාත්මක වන බවට පරිශීලකයා සහතික විය යුතුය. මුල් උපකරණ නිෂ්පාදකයා (OEM) වෙතින් ලබා ගත් වහාම නවතම මෙහෙයුම් පද්ධති පැච් සහ යාවත්කාලීන කිරීම් බාගත කර ස්ථාපනය කර ඇති බව පරිශීලකයා තවදුරටත් සහතික විය යුතුය. (පරිශීලකයාට මෙය සහතික කළ නොහැකි බැවින් ඉහත තොරතුරු පරීක්ෂා කිරීම සඳහා පරිශීලකයා තම උපාංග අංශයේ තොරතුරු තාක්ෂණ කණ්ඩායම විසින් සන්නිවේදනය කරන ලද සැලසුම් කළ කාලසටහන අනුව ඉදිරිපත් කළ යුතුය)

8.5.2. පරිශීලකයින් දුරස්ථ සම්බන්ධතා සැකසුම් හෝ වින්‍යාසයන් වෙනස් කිරීම හෝ වෙනස් කිරීම නොකළ යුතුය.

8.5.3. පරිශීලකයින් දුරස්ථ ප්‍රවේශ සේවාව භාවිතයේ නොමැති විට එය ක්‍රියා විරහිත කළ යුතුය.

8.6. බ්ලූටූත් සහ රැහැන් රහිත සේවා

බොහෝ නවීන පරිගණක / උපාංග පරිගණක සහ උපාංග පහසුවෙන් හා නම්‍යශීලී අන්තර් සම්බන්ධතාවයක් ඇති කිරීම සඳහා බ්ලූටූත් සහ රැහැන් රහිත තාක්ෂණයෙන් සමන්විත වේ. කෙසේ වෙතත්, දුර්වල ආරක්ෂාව හේතුවෙන්, පරිගණක / උපාංග වෙත අනවසරයෙන් ප්‍රවේශ වීම සඳහා මෙම තාක්ෂණයන් සාපේක්ෂව පහසුවෙන් ලක් වේ. එබැවින්;

8.6.1. සමාගම් ජාලයට සම්බන්ධ වී සිටියදී පරිශීලකයින් තම පරිගණක / උපාංග වෙනත් ජාලයකට සම්බන්ධ නොවන බවට සහතික විය යුතුය
උදා: MAS පුද්ගලික ආයතනික වයිෆයි හෝ වයර් (LAN) ජාලයට සම්බන්ධ වී සිටිමින් බ්‍රෝඩ් බෑන්ඩ් ඩොන්ගල් එකක් වෙත සම්බන්ධ වීම.

8.6.2. පරිශීලකයින් දුරස්ථ ප්‍රවේශය සඳහා භාවිතා කරන පරිගණක / උපාංග නොසලකා හැරදා යාම සිදු නොකළ යුතුයි. භාවිතයේ නොමැති විට, එවැනි පරිගණක / උපාංග නිසි ලෙස අගුළු දමා සුරක්ෂිත කළ යුතුය.

8.6.3. නැතිවූ හෝ අස්ථානගත වූ පරිගණක / උපාංග සම්බන්ධයෙන්, පරිශීලකයින් වහාම තොරතුරු තාක්ෂණ උපකාරක කවුළුවට හෝ SBU / අංශ තොරතුරු තාක්ෂණ නියෝජිතයාට දැනුම් දී මුරපදය වෙනස් කළ යුතුය.

සැ.යු: සමාගම් සම්පත් සහ තොරතුරු තාක්ෂණ පද්ධති වෙත ප්‍රවේශ වීම සඳහා පරිශීලකයින් පොදු පරිගණක (අන්තර්ජාල කැෆේවල හවුල් පරිගණක වැනි) භාවිතා කිරීමෙන් වැළකී සිටිය යුතුය. අපරාධකරුවන් තිරය නිරීක්ෂණය කිරීමෙන් සහ රහස්‍ය තොරතුරු ග්‍රහණය කර ගැනීමෙන් වළක්වා ගැනීම සඳහා පරිශීලකයින් තම පරිගණක / උපාංග පොදු ස්ථානවල (ගුවන්තොටුපල විවේකාගාර, කෝපි හල්, සංක්‍රමණයේ සිටියදී යනාදිය) භාවිතා කිරීමේදී ප්‍රවේශමී විය යුතුය.

9. ආයතන උපාංග වලින් MAS තොරතුරු සේවා වෙත පිවිසීම

9.1. පුද්ගලික පරිගණක

MAS සිය සියලුම සේවකයින්ට තොරතුරු තාක්ෂණ ප්‍රමිතීන්ට අනුව නවතම සම්මත මෙහෙයුම් පද්ධති සහ පැච් ධාවනය කරන ලැප්ටොප් සහ ඩෙස්ක්ටොප් යන පුද්ගලික පරිගණක සපයයි. තාක්ෂණ සේවා විසින් මිැර-ෂෘ එකක් සැපයීම, එම සේවකයාගේ කළමනාකරු විසින් නියම කර ඇති අවශ්‍යතාවයට අනුව MAS හි විවිධ යෙදුම් පද්ධති වෙත ප්‍රවේශ වීම සඳහා පුද්ගලික පරිගණකයක් හෝ උපාංගයක් ලබා දීමේදී සිදු කරයි.

කාර්යාල පරිශ්‍රයෙන් පිටත මෙම උපකරණ භාවිතා කිරීම සහ බ්‍රෝඩ්බෑන්ඩ් අන්තර්ජාල පහසුකම් ලබා දීම, එම සේවකයාගේ කළමනාකරුගේ අනුමැතිය මත පදනම්ව අවසර දෙනු ලැබේ.

9.2. ජංගම උපාංග (ටැබ්ලට් සහ ස්මාර්ට්ෆෝන්)

9.2.1. MAS MPLS ජාලය තුළ විශේෂිත රැහැන් රහිත ජාල වලට MAS SBU සතු සහ MAS තාක්ෂණික සේවා කණ්ඩායම් කළමනාකරණය කරන මොබයිල් උපාංග වලට පමණක් පිවිසුම් අවසර දෙනු ලැබේ.

9.2.2. MAS නම් කළ යෙදුම් එකතුව App store වෙත පෙදු අන්තර්ජාල සබඳතා හරහා පිවිසුම් හැකියාවන් MAS සතු ජංගම උපාංග සඳහා ලබාදී ඇත.

9.3. තොරතුරු සහ පද්ධති වෙත ප්‍රවේශ වීමට බලයලත් අය හැර වෙනත් පාර්ශවයක් විසින් ඔවුන්ගේ උපාංගය හරහා කටයුතු කිරීම වැළැක්වීම පරිශීලකයින්ගේ වගකීම වේ. උපාංගය වෙනත් අයෙකුට ස්ථිරව ලබා දෙන්නේ නම්, පරිශීලකයා තොරතුරු තාක්ෂණ උපකාරක කවුළුව වෙත දැනුම් දිය යුතු අතර MAS තොරතුරු සහ පද්ධති වෙත ප්‍රවේශය අවලංගු කරන බවට සහතික විය යුතුය.

9.4. සමාගමේ සංවේදී තොරතුරු වැනි පුද්ගලික පරිගණක / උපාංගවල ගබඩා කර හෝ නඩත්තු නොකිරීමට හෝ පුද්ගලික ක්ලවුඩ් ගබඩා සේවා හරහා උපස්ථ නොකිරීමට පරිශීලකයින් සහතික විය යුතුය.

9.5. පුද්ගලික වලාකුළු ආචයන සේවාවන්ට (Cloud Storage Services) මේවා ඇතුළත් වන අතර ඒවා **පාරිභෝගික අනුවාදයන්ට** පමණක් සීමා නොවේ:

- Dropbox

- Box
- Apple iCloud
- Google Drive
- Microsoft Personal OneDrive

*කෙසේ නමුත්, කාර්යාලීය භාවිතය සඳහා අනුමත කර ඇත්තේ **Microsoft OneDrive for Business** බව දැක්විය යුතුයි. එම නිසා MAS කාර්ය මණ්ඩලය හා බාහිර පාර්ශවයන් සමග තොරතුරු හුවමාරු කරගැනීමේදී **Microsoft OneDrive for business** පමණක් ම භාවිතා කළ යුතුයි.

සැ.යු.කිසියම් ආරක්ෂක උල්ලංඝණය කිරීමක්, හෝ එවැන්නක් ගැන සැක නම්, සුදුසු ප්‍රතිකර්ම ක්‍රියාමාර්ග ගත හැකි වන පරිදි පරිශීලකයින් විසින් තොරතුරු තාක්ෂණ උපකාරක කවුළුවට හෝ SBU / අංශයේ තොරතුරු තාක්ෂණ නියෝජිතයාට දැනුම් දිය යුතුය.

10. පුද්ගලිකව අයත් උපාංගවල MAS තොරතුරු තාක්ෂණ සේවා භාවිතය

MAS තමන්ගේ උපාංග ගෙන ඒම (BYOD) MAS හි **පුද්ගලික ජාලය** වෙත සබැඳීමක් සේ සලකයි. **මෙය තහනම් ක්‍රියාවකි.**

කෙසේ වෙතත්, පහත දැක්වෙන ප්‍රතිපත්ති රීති මත පදනම්ව, **පොදු අන්තර්ජාලය හරහා** ප්‍රවේශ විය හැකි විද්‍යුත් තැපෑල හා MAS හි තොරතුරු තාක්ෂණ යෙදුම් ආදිය සමඟ සම්බන්ධ වීම සඳහා පුද්ගලිකව අයත් උපාංග භාවිතා කිරීමට MAS ඉඩ දෙයි.

10.1. පුද්ගලික පරිගණක

10.1.1. පුද්ගලික පරිගණක අයත් පුද්ගලයින් වනම් …

- කොන්ත්‍රාත් සේවකයින්
- සීමාවාසිකයන්
- වෙනත්, MAS හි සේවයේ නියුතු කළමණාකරුවෙකුගේ අධීක්ෂණයෙන් ඇතැම් ව්‍යාපාර ක්‍රියාවලීන් සඳහා බාහිරින් ලබා ගන්නා බාහිර සේවා සපයන්නන්,

… යන අයට MAS හි තොරතුරු තාක්ෂණ පද්ධති සහ සේවාවන් අන්තර්ජාලය හරහා, සෘජුව හෝ අතථ්‍ය ඩෙස්ක්ටොප් අතුරුමුහුණතක් හරහා ප්‍රවේශ වී ඇත්නම්, එම ඔවුන්ට MAS විසින් සපයනු ලබන වෙනම user-ID මගින් සත්‍යාපනය කරනු ලැබේ.

10.1.2. ඊට අමතරව, පහත සඳහන් නීති රීති අදාළ පුද්ගලයින් සඳහා ද බලපැවැත්වේ …

- ඔවුන් පුද්ගලික පරිගණක භාවිතා කළ යුත්තේ තොරතුරු තාක්ෂණ පරිපාලක වෙත ලබාදී ඇති තොරතුරු තාක්ෂණ ප්‍රමිති ලේඛනයට අනුව MAS තාක්ෂණ සේවා විසින් අනුමත කරන ලද නවතම මෙහෙයුම් පද්ධති සහ පැච් සමඟ පමණි.

- ඔවුන් කිසි විටෙකත් බලපත්‍ර රහිත මෘදුකාංග හෝ ආරක්ෂා සීමා මගහරින (ජේල් බ්‍රේක් කළ) උපාංග (බ්‍රෝඩ්බෑන්ඩ් ජාල උපාංග වැනි) ඔවුන්ගේ පුද්ගලික පරිගණක තුළ භාවිතා නොකළ යුතුය.

- ඔවුන් සම්බන්ධ විය යුත්තේ MAS විසින් එම පහසුකම ලබා දෙන පොදු අන්තර්ජාලය වෙත පමණක් වන අතර ඔවුන් ස්ථානගත කර ඇති MAS ව්‍යාපාරික පරිශ්‍රයේ පුද්ගලික ජාලයට කිසි විටෙකත් සම්බන්ධ නොවිය යුතුය.

- මෙම පරිගණකවල සමාගම විසින් අනුමත කරන ලද ප්‍රති-වයිරස මෘදුකාංග, පුද්ගලික ෆයර්වෝල් සහ ජංගම උපාංග කළමනාකරණ මෘදුකාංග ස්ථාපනය කර, යාවත්කාලීන කර ඵලදායී ලෙස ක්‍රියාත්මක වන බවට ඔවුන් සහතික විය යුතුය.

- සමාගමට අයත් යැයි සලකනු ලබන සහ පුද්ගලිකව අයිති පරිගණක භාවිතා කරන මෙම පුද්ගලයින් විසින් භාවිතා කරන ලද හෝ නිර්මාණය කරන ලද සියලුම දත්ත ලිපිගොනු, සමාගම විසින් සපයනු ලබන ක්ලවුඩ් ආචයන ස්ථානවල කළමනාකාරීත්වයට පිවිසිය හැකි අවසර සහිතව ගබඩා කළ යුතු අතර කිසිවිටෙකත් පුද්ගලිකව අයත් පරිගණකවල ගබඩා නොකළ යුතුය.

- MAS යෙදුම්, විද්‍යුත් තැපෑල සහ MAS සමඟ ලිපිගොනු ගබඩා කරන ස්ථාන (උදා:Office 365 හි OneDrive/SharePoint) සමඟ ප්‍රවේශවීමේදී හා ගනුදෙනු කිරීමේදී පරිශීලකයින් කිසි විටෙක පුද්ගලික පරිගණක සහ ලැප්ටොප්වල වාණිජ්‍යමය වශයෙන් නිදහස් හෝ ගෙවන ලද අන්තර්ජාල VPN යෙදුම් භාවිතා නොකළ යුතුය.

10.2. ජංගම උපාංග (ටැබ්ලට් සහ ස්මාර්ට්ෆෝන්)

10.2.1. පුද්ගලිකව ඇති ජංගම උපාංගවලට පොදු අන්තර්ජාලය හරහා පමණක් සම්බන්ධ වීමට අවසර ඇති අතර මෙම උපාංග සඳහා MAS පුද්ගලික ජාලයට සම්බන්ධතාවය අවහිර කරනු ලැබේ.

10.2.2. MAS නිර්දේශිත යෙදුම් චකතුව වෙත පොදු අන්තර්ජාලය හරහා App store මගින් පිවිසිය හැකි අතර පුද්ගලික හිමිකාරිත්වය ඇති ජංගම උපාංග භාවිතා කරන්නන්ගේ පරිභෝජනය උදෙසා ආරක්ෂිතව ලබා දෙනු ඇත.

10.3. MAS සඳහා සේවය කරන කාල සීමාව තුළ, MAS තොරතුරු සහ පද්ධති වෙත ප්‍රවේශ වීමට බලයලත් අය හැර වෙනත් පාර්ශවයක් විසින් පුද්ගලික උපාංග හරහා ප්‍රවේශ වීමෙන් ආරක්ෂා කිරීම පරිශීලකයින්ගේ වගකීම වේ.

10.4. සමාගමේ සංවේදී තොරතුරු වැනි පුද්ගලික පරිගණක / උපාංගවල ගබඩා කර හෝ නඩත්තු නොකිරීමට හෝ පුද්ගලික ක්ලවුඩ් ගබඩා සේවා හරහා උපස්ථ නොකිරීමට පරිශීලකයින් සහතික විය යුතුය. අතථ්‍ය ඩෙස්ක්ටොප් අතුරුමුහුණතක් හෝ සමාගම් යෙදුමක්, අදාළ වන ඕනෑම තැනක සැපයීම සහ වම අතථ්‍ය ඩෙස්ක්ටොප් අතුරුමුහුණත හෝ යෙදුමට පමණක් ප්‍රවේශ වීම ද මෙම පාලනය හරහා සහතික කරනු ඇතැයි අපේක්ෂා කෙරේ.

10.5. MAS යෙදුම්, ඊමේල් සහ MAS සපයන ලද ගොනු ගබඩා ස්ථාන (උදා. Office 365 හි OneDrive/SharePoint) වෙත ප්‍රවේශවීමේදී හා ගනුදෙනු කිරීමේදී පරිශීලකයින් කිසි විටෙක ස්මාර්ට් ෆෝන් සහ ටැබ්ලට් උපාංගවල වාණිජ්‍යමය වශයෙන් නිදහස් හෝ ගෙවන ලද අන්තර්ජාල VPN යෙදුම් භාවිතා නොකළ යුතුය.

*කෙසේ නමුත්, කාර්යාලීය භාවිතය සඳහා අනුමත කර ඇත්තේ **Microsoft OneDrive for Business** බව දැක්විය යුතුයි. එම නිසා MAS කාර්ය මණ්ඩලය හා බාහිර පාර්ශවයන් සමග තොරතුරු හුවමාරු කරගැනීමේදී **Microsoft OneDrive for business** පමණක් ම භාවිතා කළ යුතුයි.

සැ.යු. කිසියම් ආරක්ෂක උල්ලංඝණය කිරීමක්, හෝ එවැන්නක් ගැන සැක නම්, සුදුසු ප්‍රතිකර්ම ක්‍රියාමාර්ග ගත හැකි වන පරිදි පරිශීලකයින් විසින් තොරතුරු තාක්ෂණ උපකාරක කවුළුවට හෝ SBU / අංශයේ තොරතුරු තාක්ෂණ නියෝජිතයාට දැනුම් දිය යුතුය.

11. සමාගම සතු දත්ත ගබඩා කිරීම සඳහා ෆ්ලෑෂ් ඩ්‍රයිව් සහ වෙනත් ඉවත් කළ හැකි මාධ්‍ය භාවිතා කිරීම

ෆ්ලෑෂ් ඩ්‍රයිව් සහ ඉවත් කළ හැකි දත්ත ගබඩා මාධ්‍ය වන යූඑස්බී හාඩ් ඩිස්ක්, සීඩී හෝ ඩීවීඩී යනාදිය සොරකම් හා අලාභහානි වලට ගොදුරු වේ.

එබැවින් ඒවා භාවිතා කරන්නේ කෙසේද යන්න පිළිබඳව පරිශීලකයින් සැලකිලිමත් වීම වැදගත්ය.

මෙම මාධ්‍ය සිය සේවකයින් විසින් ආරක්ෂිතව හා ඵලදායී ලෙස භාවිතා කරන බව සහතික කිරීම සඳහා සමාගම පහත සඳහන් නීති රීති සපයයි.

11.1. සේවකයින් සහ ආශ්‍රිතයන්ට පුද්ගලික සීඩී තැටි සහ ඩීවීඩී භාවිතා කිරීමට අවසර නැත. තොරතුරු තාක්ෂණ සහායක කණ්ඩායම් අධීක්ෂණය සමඟ භාවිතා කිරීමට අවසර දී ඇත්තේ සමාගමට අයත් සීඩී සහ ඩීවීඩී පමණි. ව්‍යාපාර ඒකකයේ කළමනාකාරිත්වය විසින් පමණක්ම මාධ්‍ය ගබඩා කළ යුතුය.

11.2. MAS හි සෑම ව්‍යාපාර ඒකකයකම තොරතුරු තාක්ෂණ සහායක කණ්ඩායම විසින් නඩත්තු කර බෙදා හරිනු ලබන සමාගමට අයත් ගුප්ත කේතනය කළ ෆ්ලෑෂ් ඩ්‍රයිව් සහ යූඑස්බී ඩිස්ක් ඩ්‍රයිව් භාවිතා කිරීමට පමණක් අවසර ඇත. මෙම ධාවකයන් ව්‍යාපාරික ඒකකය විසින් සේවකයා භාවිතා කරන කාලසීමාව සඳහා තොරතුරු තාක්ෂණ සහාය හරහා ලබා දෙනු ඇත. කාල සීමාව අවසානයේදී, සේවකයා විසින් එම උපාංගවල දත්ත ඉවත් කර ඒවා පරීක්ෂා කිරීම සහ ගබඩා කිරීම සඳහා තොරතුරු තාක්ෂණ සහාය වෙත ආපසු භාර දිය යුතුය.

11.3. එසේම, පරිශීලක නිර්මිත දත්ත හෝ ගොනු නිර්මාණයේදී හෝ වෙනස් කිරීමේදී සේවකයන් විසින් සෑම අවස්ථාවකදීම ඒවායේ හිමිකම් ආරක්ෂා කිරීම තරයේ නිර්දේශිත අතර ඉන් අනවසර ප්‍රවිශ්ටවීම් වලදී ආරක්ෂාව සැලසෙනු ඇත.

12. ඇගයීම සහ අධීක්ෂණය

12.1. MAS තොරතුරු තාක්ෂණ පද්ධති සහ සේවාවන් වෙත ප්‍රවේශය ලබා ගැනීමට පෙර, සියලුම පරිශීලකයින් මෙම ප්‍රතිපත්තියේ අන්තර්ගතය කියවා තේරුම් ගෙන ඇති බව සමාලෝචනය කර තහවුරු කළ යුතු අතර ඔවුන් ඒ අනුව කටයුතු කරනු ඇත.

12.2. මෙම ප්‍රතිපත්තිය, තොරතුරු ආරක්ෂණ ප්‍රතිපත්තිය සහ තොරතුරු තාක්ෂණ පාලනය සහ කළමනාකරණ ප්‍රතිපත්තිය නිරීක්ෂණය කිරීම සහ බලාත්මක කිරීම සඳහා ක්‍රියාවලි සහ මෙවලම් යොදවනු ලැබේ.

12.3. සමාගමේ අදාළ බලයලත් පුද්ගලයින්ට විද්‍යුත් තැපෑල, අන්තඃජාල (Intranet) අඩවි සහ දත්ත ගබඩා කිරීමේ පහසුකම්, නිර්මාණය කිරීම නඩත්තු කිරීම සහ පරිශීලකයන්ට අවසර ලබා දී ඇති යෙදුම්වල (SAP වැනි) දත්ත අන්තර්ගතයට ප්‍රවේශ වීමට අයිතිය ද ඇත.

13. අනුකූල නොවීම්

13.1. පහත දැක්වෙන ක්‍රමවේදයකින් ප්‍රතිපත්තියට අනුකූල නොවන අවස්ථා වාර්තා කරන්න;

- ඔබේ අංශයේ තොරතුරු තාක්ෂණ නිලධාරීන් සමඟ කතා කරන්න හෝ තොරතුරු තාක්ෂණ උපකාරක කවුළුවේ පැමිණිල්ලක් එක් කරන්න
- ඔබේ SBU, ප්‍රාදේශීය හෝ කණ්ඩායම් නෛතික නිලධාරියා සමඟ කතා කරන්න
- DNA උපකාරක කවුළුවේ පැමිණිල්ලක් එක් කරන්න
- masdnahelpdesk.ethicspoint.com වෙත පිවිසෙන්න
- 0112 430 430 අමතා ඉංග්‍රීසි පටිගත හඬට පසු 855 867 7899 අමතන්න

13.2. MAS ආචාර ධර්ම කමිටුව සහ අනෙකුත් වගකිවයුතු පාර්ශවයන් විසින් පැමිණිල්ල විභාග කිරීම හා විමර්ශනය කිරීම සම්බන්ධ සියලු පාර්ශ්වයන්ගේ රහස්‍යභාවය පවත්වාගෙන යනු ඇත.

13.3. MAS ආචාර ධර්ම කමිටුවේ සාමාජිකයෙකු විසින් ඔබව සම්බන්ධ කර ගනු ලැබුවහොත්, විවෘතව, අවංකව සහ රහස්‍යභාවය පවත්වා ගනිමින් අඛණ්ඩ පරීක්ෂණවලට සහාය වීම ඔබේ වගකීමකි.

13.4. පැමිණිල්ලක් ඉදිරිපත් කරන්නෙකුගෙන් හෝ ඉදිරිපත් කිරීමට සූදානම් වන්නකුගෙන් පළිගැනීම, වින්දිතයෙකුට සහාය වීම හෝ විමර්ශනවලට සහභාගී නොවීම; MAS DNA (චර්යාධර්ම පද්ධතිය) සහ ප්‍රතිපත්තියට අනුකූල නොවීමක් සේ සැලකේ.

13.5. කීර්ති නාමයට කැළලක් ඇති කිරීමේ අරමුණින්, ද්වේශ සහගතව වැරදි චේතනා සහිතව පදනම් විරහිත අසත්‍ය චෝදනා වාර්තා කිරීම, MAS DNA හා අනුකූල නොවීමකි.

13.6. කිසියම් පැහැදිලි කරගැනීමක් අවශ්‍ය වුවහොත් DNA උපකාරක කවුළුව වෙත policyinfo@masholdings.com හෝ අංශයේ තොරතුරු තාක්ෂණ සහාය විශේෂඥයාගෙන් හෝ තොරතුරු තාක්ෂණ උපකාර කවුළුව policyinfo@masholdings.com වෙත සම්බන්ධ වන්න.

14. වගකීම

14.1. විධායක කාර්ය මණ්ඩලයේ සියලුම සේවකයින් දැනුවත් කිරීම සහ මෙම ප්‍රතිපත්තිය පිළිපැදීම සහතික කිරීම සෑම ඒකක ප්‍රධානියෙකුගේම / කළමනාකරුවෙකුගේ වගකීමකි; ප්‍රතිපත්තිය උල්ලඝණය කිරීම් පිළිබඳව ඔවුන්ගේ අවධානය යොමු කිරීම, පෙන්වාදීම හෝ ඊට එරෙහිව ක්‍රියා කිරීමට වහාම සුදුසු පියවර ගන්න.

15. MAS තොරතුරු පද්ධතිය භාවිතා කිරීමේ ප්‍රතිපත්තියෙහි වලංගුභාවය

මෙම ප්‍රතිපත්තිය MAS හි ඇඟලුම් මණ්ඩලය විසින් සමාලෝචනය කර අනුමත කර ඇත.

තොරතුරු තාක්ෂණ පරිසරයෙහි වෙනස්වීම්, අදාළ නීති සම්පාදනය, ගිවිසුම්ගත විධිවිධාන, යහ භාවිතයන් හෝ එහි හඳුනාගත් අයෙකුට ප්‍රතිචාර වශයෙන් දක්වන ඵලදායීතාවය වෙනුවෙන් එය වාර්ෂිකව සමාලෝචනය කෙරේ.

16. අර්ථ දැක්වීම්

- ප්‍රති-වයිරස - ජාලය හරහා සම්ප්‍රේෂණය වීම හෝ පරිගණක පද්ධති වලට බලපෑම් කිරීම වැනි අනිෂ්ට හෝ අනවසර මෘදුකාංග කේත (වෛරස්) හඳුනාගෙන වැළැක්වීමට භාවිතා කරන මෘදුකාංගයකි.

- ගුප්ත කේතනය - ගුප්ත කේතනය යනු ඇල්ගොරිතමයක් භාවිතා කරමින් තොරතුරු අවසර නොමැති අයට කියවිය නොහැකි තත්ත්වයට පරිවර්තනය කිරීමේ ක්‍රියාවලියකි. විකේතනය යනු එම ගුප්ත කේතිත තොරතුරු නැවත කියවිය හැකි බවට පත් කිරීමේ ක්‍රියාවලියකි.

- ෆයර්වෝල් - විශ්වාසදායක නොවන ජාල වලින් සංවේදී ජාල හෝ පද්ධති ආරක්ෂා කිරීමට යොදවා ඇති සේවාදායකයක (සර්වර් එකක) ක්‍රියාත්මක වන දෘඩාංග උපාංගයක් හෝ මෘදුකාංග යෙදුමකි.

- ප්‍රොක්සි සර්වරය - ප්‍රොක්සි සර්වරය/සේවාදායකය යනු අන්තර්ජාලයට පිවිසෙන අභ්‍යන්තර පරිශීලකයින් බාහිර තර්ජන වලින් ආරක්ෂා කිරීම සඳහා භාවිතා කරන ආරක්ෂක පද්ධතියකි.
- MAS - මාස් හෝල්ඩිංස් (පුද්ගලික) සමාගම සහ එහි උප සමාගම්, අනුබද්ධ සහ හවුල් ව්‍යාපාර හවුල්කරුවන්.

- SBU / Strategic Business Unit - උපායමාර්ගික ව්‍යාපාර ඒකකය MAS හි උප සමාගමක් හෝ අනුබද්ධ ආයතනයකි

- අංශය - MAS SBU තුල ඇති මූල්‍ය, මානව සම්පත් (HR), තොරතුරු තාක්ෂණ, නවෝත්පාදන සහ ඒවාට පමණක් සීමා නොවූ කොට්ඨාශය

- තෙවන පාර්ශවයක් - MAS හෝ එහි හවුල්ව්‍යාපාර ක්‍රියාකාරිත්වයේ කොටසක් නොවන ඕනෑම සමාගමක්.

- තොරතුරු තාක්ෂණ උපකාරක කවුළුව - පරිශීලකයින්ට සහය දැක්වීමට සහ පරිශීලක ඉල්ලීම් හා පැමිණිලි වලට ප්‍රතිචාර දැක්වීමට කැපවී සිටින තාක්ෂණික සේවාවන් තුළ ඇති පහසුකමකි.