தகவல் அமைப்பு பயன்படுத்தல் கொள்கை

உள்ளடக்கம்

1. நோக்கம்
2. செயற்பரப்பு
3. தகவல் பாதுகாப்பு என்றால் என்ன?
4. தகவல் அமைப்பின் பாவனை
5. உறுதிப்படுத்துதல்
6. மின்னஞ்சல் மற்றும் செய்தி அனுப்பல்
7. இணையப்பாவனை
8. தொலைவிட அணுகல் சேவை (REMOTE ACCESS SERVICE)
9. நிறுவனத்திற்கு சொந்தமான உபகரணங்களில் MAS தகவல் தொழிநுட்ப (IT) சேவையின் பாவனை
10. தனிப்பட்ட ரீதியில் சொந்தமான உபகரணங்களில் MAS தகவல் தொழிநுட்ப (IT) சேவையின் பாவனை
11. நிறுவனத்திற்கு சொந்தமான தரவுகளை சேமிப்பதில் FLASH DRIVES மற்றும் அகற்றக்கூடிய சேமிப்புக் கருவிகளின் பாவனை
12. மதிப்பீடு மற்றும் கண்காணிப்பு
13. இணக்கமின்மை
14. பொறுப்பு
15. MAS IT அமைப்புப் பாவனைக் கொள்கையின் செல்லுபடியாகும் காலம்
16. வரைவிலக்கணங்கள்

1. நோக்கம்

1.1 MAS அதன் ஊழியர்களுக்கும் அங்கீகரிக்கப்பட்ட மூன்றாம் தரப்பினருக்கும், அதன் அதிகாரமளிக்கப்பட்ட மூன்றாம் தரப்புகளுக்கும், தகவல் அமைப்புகள் மற்றும் தகவல் தொழில்நுட்ப சேவைகளுக்கான அணுகல் வசதியை, தேவையின் அடிப்படையில் மற்றும் தங்களுக்கு ஒதுக்கப்பட்ட கடமைகளையும் பொறுப்புகளையும் நிறைவேற்றத் தேவையான குறைந்தபட்ச சலுகைகளுக்கு ஏற்ப, பாதுகாப்பான, பயனுள்ள மற்றும் திறமையான முறையில் வழங்குகிறது

வழங்கப்படும் IT சேவைகளில் பின்வருவன உள்ளடங்குகின்றன:

- மடிக்கணினி, Tablet மற்றும் Desktop கணினிகளுக்கான அணுகல்
- அச்சீட்டு உபகரணங்களுக்கான அணுகல்
- கூட்டு நிறுவன மின்னஞ்சல் சேவைகளுக்கான அணுகல்
- வணிக செயலிகள் மற்றும் தரவுகளுக்கான அணுகல்
- இணையம் மற்றும் Cloud சேமிப்பகத்திற்கான அணுகல்
- இணையத்தள அணுகல்
- வணிக செயலிகளுக்கான தொலை அணுகல் (Remote access)
- மின்னஞ்சல் சேவைகளுக்கான தொலை அணுகல் (Remote access)
- குரல் மற்றும் காணொளி மூல கலந்துரையாடலுக்கான அணுகல்

MAS நிறுவனத்தினால் லழங்கப்படும் தகவல் அமைப்புகள் மற்றும் தகவல் தொழில்நுட்பச் சேவைகளின் ஏற்றுக்கொள்ளத்தக்க பயன்பாடு தொடர்பில் ஊழியர்கள் மற்றும் மூன்றாம் தரப்பினர் கைக்கொள்ள வேண்டிய தெளிவான மற்றும் நியாயமான தரநியமங்களை இக் கொள்கை நிறுவுகின்றது.

2. செயற்பரப்பு

2.1 MAS தகவல் அமைப்பின் பயன்படுத்தல் கொள்கையானது பின்வரும் தரப்புகளுக்கு/பிரிவினருக்கு பிரயோகிக்கப்படும்:

- அனைத்து நிரந்தர ஊழியர்களும் (நிலையான கால/ஒப்பந்த ஊழியர்கள் உட்பட) ஒப்பந்த விதிமுறைகள் அல்லது கடிதங்கள் மூலம் MAS உடன் இணைந்துள்ள ஆலோசகர்கள் மற்றும் பயிற்சியாளர்கள் உள்ளிட்ட நிரந்தரமற்ற ஊழியர்கள் (“ஊழியர்கள்”).

- ஆலோசகர்கள், நிறைவேற்றுப் பொறுப்பற்ற பணிப்பாளர்கள் மற்றும் ஆலோசனைச் சபை உறுப்பினர்கள் (“ஆலோசகர்கள்”)

- MAS தொடர்பு வைத்திருக்கும் வழங்குநர்கள், துணை ஒப்பந்தகாரர்கள் மற்றும் அவர்களின் முகவர்கள் (“வழங்குநர்கள்”)

- அனைத்து MAS வாடிக்கையாளர்களும் MAS தொடர்பு வைத்திருக்கும் அவர்களின் முகவர்களும் (“வாடிக்கையாளர்கள்”). இவர்கள் அனைவரும் MAS உடனான தமது உறவின்போது, MAS தகவல் அமைப்புகள் மற்றும் தகவல் தொழில்நுட்ப சேவைகளுக்கான அணுகல் வழங்கப்பட்டவர்கள் (இவர்களைப் பொதுவாக “பயனர்கள்” என்று குறிப்பிட முடியும்).

2.2. MAS தகவல் அமைப்புப் பயனர்கள் மற்றும் தொடர்புடைய மூன்றாம் தரப்பினர் MAS தகவல் அமைப்புகள் மற்றும் தகவல் தொழில்நுட்ப சேவைகளுக்கான அணுகலைப் பெறுவதற்கு முன்பு இந்த

தகவல் அமைப்பு பயன்பாட்டுக் கொள்கையை வாசித்து, புரிந்து கொண்டு, முறையாக ஏற்றுக்கொள்ள வேண்டும்.

2.3 MAS தகவல் அமைப்பு பயனர்கள் மற்றும் MAS Holdings தகவல் அமைப்புகள் மற்றும் தகவல் தொழில்நுட்ப சேவைகளுக்கான அணுகலைப் பெற்றுக்கொண்டுள்ள மூன்றாம் தரப்பினர் ஆகியோர், எல்லா நேரங்களிலும், இரகசியத்தன்மைக் கொள்கை மற்றும் இத் தகவல் அமைப்பு பயன்பாட்டுக் கொள்கையை அனுசரித்து நடக்க வேண்டும்.

2.4 தகவல் பாதுகாப்புக் கொள்கை அல்லது இந்த தகவல் அமைப்பு பயன்பாட்டுக் கொள்கையுடனான எந்தவொரு இணக்கமின்மை அல்லது மீறலும் தகவல் பாதுகாப்பு மீறலாகக் கருதப்படும் என்பதுடன், ஒழுங்கு நடவடிக்கைகளுக்கும் வழிவகுக்கும்.

3. தகவல் பாதுகாப்பு என்றால் என்ன?

3.1 தகவல் பாதுகாப்பு என்பது நிறுவனத்தின் உணர்திறன் மற்றும் வணிக ரீதியில் முக்கியமான தகவல் சொத்துக்களை மின்னணு அல்லது தொடுகைக்கு ஏதுவான வடிவத்தில், அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, வெளிப்படுத்தல், இடையூறு, மாற்றம், இடைமறிப்பு, பதிவு செய்தல் அல்லது அழித்தல் ஆகியவற்றிலிருந்து பாதுகாக்கும் செயல்முறை மற்றும் நடைமுறை ஆகும்.

பின்வருவனவற்றை உறுதிப்படுத்துவதே MASஇல் தகவல் பாதுகாப்பின் முக்கிய இலக்குகளாகும்:

3.2.1 தகவலின் இரகசியத்தன்மை - உணர்திறன் வாய்ந்த வாடிக்கையாளர், வழங்குநர் மற்றும் MAS தகவல்களை அவற்றை அணுகுவதற்கு அங்கீகரிக்கப்பட்டவர்களால் மட்டுமே அணுகக்கூடியதாக இருக்க வேண்டும்.

3.2.2. தகவலின் ஒருமைப்பாடு - வணிக ரீதியில் சிக்கலான வாடிக்கையாளர், வழங்குநர் மற்றும் MAS தகவல்கள் துல்லியமாகவும் பிழையில்லாமலும் பூரணமாகவும் இருக்க வேண்டும்.

3.2.3 தகவலின் கிடைக்கும் தன்மை - அங்கீகரிக்கப்பட்ட பயனர்கள் தேவைப்படும்போது முக்கியமான வணிகத் தகவல்களை அணுகக் கூடியதாக இருக்க வேண்டும்.

3.2.4 மின்னணு பரிவர்த்தனைகளை நிராகரிக்காமலிருப்பது - மின்னணு பரிவர்த்தனைகளில் பயனர்கள் செய்த செயல்களுக்கு அவர்கள் பொறுப்பேற்க வேண்டும்.

(தகவல் சொத்து என்பது ஒரு திட்டவட்டமான, எந்த முறையிலேனும் சேமிக்கப்படக்கூடிய தகவல்களாகும். இது நிறுவனத்திற்கு ''பெறுமதிமிக்கது'' என்று கருதப்படுகின்றது.)

4. தகவல் அமைப்பின் பாவனை

4.1 MAS IT அமைப்புகள் மற்றும் தகவல் சொத்துக்களை முறைகேடான உபயோகம் மற்றும்/அல்லது தற்செயலான சேதங்களிலிருந்து பாதுகாப்பதில் பயனர்கள் போதிய கவனம் செலுத்த வேண்டும். காப்புறுதித் திட்டத்தின் மூலம் இழப்பீடு கோரக்கூடிய ஒரு சேதமாக இருந்தால், நிறுவனம் அது தொடர்பில் அவசியமானதைச் செய்யும். ஆனால், வேண்டுமென்றே அல்லது கவனயீனத்தினால் ஏற்படுத்தப்பட்ட சேதமாக இருந்தால், சம்பந்தப்பட்ட பயனரே அதற்கான பொறுப்பை ஏற்க வேண்டும். (முதல் சம்பவத்தின்போது எச்சரிக்கைக் கடிதம் வழங்கப்படும். இரண்டாவது தடவையிலிருந்து தண்டம் அறவிடப்படும்).

4.1.1. கணினிகள், மடிக்கணினிகள், மொபைல் சாதனங்கள், அச்சுப்பொறிகள், தொலைநகல் இயந்திரங்கள், நிழற்பட பிரதியெடுக்கும் இயந்திரங்கள், அத்துடன் வலையமைப்புக்கள், சேவையகங்கள் மற்றும் செயலிகள் உட்பட அனைத்து MAS தகவல் அமைப்புகளும் குறிப்பிட்ட தேவைக்காகவும் அங்கீகரிக்கப்பட்ட வணிக நோக்கங்களுக்காகவும் மட்டுமே பயன்படுத்தப்பட வேண்டும்

4.1.2. சட்டவிரோத அல்லது முறைகேடான நோக்கங்களுக்காக MAS தகவல் அமைப்புகளைப் பயன்படுத்த பயனர்களுக்கு அனுமதி இல்லை.

4.2 சட்டவிரோத அல்லது முறைகேடான தகவல் தொழிநுட்ப அமைப்பு பயன்பாடு

தகவல் தொழில்நுட்ப அமைப்புகளின் சட்டவிரோத அல்லது முறைகேடான பயன்பாடுகளில் பின்வருவன அடங்கும்: பதிப்புரிமை மீறல், மோசடி, அவதூறு, திருட்டு, துன்புறுத்தல், அச்சுறுத்தல், ஆபாசம், ஆள்மாறாட்டம், சூதாட்டம், கணினி சேதப்படுத்துதல் (உதா: கணினி வைரஸ்கள் பரவுதல் போன்றவை) அல்லது அங்கீகரிக்கப்படாத கணினி அணுகல்.

4.3 பயனர்கள் தலைமை தகவல் அலுவலரால் முறையாக அனுமதியளிக்கப்பட்ட மற்றும் முன் அங்கீகரிக்கப்பட்ட உரிமம் பெற்ற மென்பொருட்களை மட்டுமே நிறுவி பயன்படுத்த வேண்டும்.

4.3.1 நிர்வாக உரிமைகளைக் கொண்ட பயனர்கள் MAS வலையமைப்புக்கள் மற்றும் தகவல் சொத்துக்களைப் பாதுகாக்க செயல்படுத்தப்பட்ட வைரஸ் தடுப்பு மென்பொருள், Proxy சேவையகங்கள் மற்றும் தீச்சுவர்கள்(Firewalls) போன்ற எந்த கட்டுப்பாடுகளையும் முடக்கவோ அல்லது கடந்து செல்லவோ கூடாது.

4.3.2 சமூக ஊடக தளங்கள், Chat சேவைகள், அஞ்சல் பட்டியல்கள், வலைப்பதிவுகள் அல்லது பொது செய்தி குழுக்கள் போன்ற பொதுவாக அணுகக்கூடிய இணைய தளங்களில் பயனர்கள் MAS, அதன் வழங்குநர்கள் அல்லது வாடிக்கையாளர்கள் பற்றிய முக்கியமான அல்லது ரகசிய தகவல்களை வெளியிடக்கூடாது.

4.3.3 பொதுவாக அணுகக்கூடிய இணைய தளங்களில் MAS, அதன் வழங்குநர்கள் அல்லது வாடிக்கையாளர்கள் பற்றிய தகவல்களை இடுகையிட விரும்பும் எந்தவொரு பயனரும் முதலில் **குழும் நிறுவனத் தொடர்பாடல்** பிரிவிடமிருந்து ஒப்புதலைப் பெற வேண்டும்.

4.3.4 எந்தவொரு தனியுரிம பொருளையும் பயன்படுத்துவதற்கு முன்பு பயனர்கள் பொருத்தமான அறிவுசார் சொத்துரிமை/ பதிப்புரிமை அல்லது ஒப்பந்த அனுமதிகளைப் பெற வேண்டும்

4.3.5 பயனர்கள், போதுமான பாதுகாப்பு கட்டுப்பாடுகள் இல்லாமல் (உதா: மின்னஞ்சல்கள் அனுப்பப்படுவதற்கு முன்னர் முறைப்படி வகைப்படுத்தப்பட வேண்டும்) வலையமைப்பில் முக்கியமான அல்லது இரகசிய தகவல்களை பரிமாற கூடாது. தேவையேற்படின், பயனர் முதலில் குழும **நிறுவனத் தொடர்பாடல்** பிரிவிடமிருந்து ஒப்புதலைப் பெற வேண்டும்.

4.3.6 சகல ஆலோசகர்களும் (அதாவது, சபை/ஆலோசனைக் குழு இணைப்பாளர்கள், ஆலோசகர்கள், நிறைவேற்றுத் தரத்திலல்லாத பணிப்பாளர்கள் மற்றும் ஆலோசனைச் சபை உறுப்பினர்கள்) சபை அறிக்கைகள் மற்றும் ஆதார ஆவணங்கள் எவற்றையும் BoardPac இற்கு வெளியே பகிர்ந்துகொள்ளக் கூடாது. அவசர தேவை ஏற்படும் பட்சத்தில், "Do-Not-Forward" கட்டுப்பாட்டுடன் "MAS-Confidential" வகைப்படுத்தலின் கீழ் "<name>_C@masholdings.com" என்ற மின்னஞ்சல் ஊடாக ஆவணங்கள் உறுப்பினர்களுடன் பகிர்ந்துகொள்ளப்படலாம்.

4.3.7 எவரேனும் புதிய ஆலோசகர்கள் /உறுப்பினர்களின் <name>_C@masholdings.com மின்னஞ்சல் முகவரிகளைக் கேட்டுப் பெறும்படி சபை/ஆலோசனைக் குழு இணைப்பாளர்களுக்கு அறிவுறுத்தல் வழங்கப்பட்டுள்ளது.

4.3.8 பயனர்கள் எவ்விதமான உணர்திறன் வாய்ந்த அல்லது இரகசியமான தகவல்களையும் உள்ளிட இயந்திரத்தில் சேமித்துவைக்கக் கூடாது. அத்தகைய உணர்திறன் வாய்ந்த அல்லது இரகசிய தகவல்கள் நிறுவனத்தில் OneDriveஇல் சேமிக்கப்படும்போது வகைப்படுத்தப்பட வேண்டும்.

கவனிக்கவும்: ஏதேனும் உணர்திறன் வாய்ந்த அல்லது இரகசிய தகவலைத் தொடர்பாடல் செய்ய ஒரு பயனருக்கு உதவி தேவைப்பட்டால், அவர் IT உதவிப் பிரிவுடன் அல்லது SKU/பிரிவு பிரதிநியுடன் தொடர்புகொள்ள வேண்டும்.

கவனிக்கவும்: MAS நிறுவனத்தின், அதன் வழங்குநர்களின் அல்லது வாடிக்கையாளர்களின் உணர்திறன் வாய்ந்த அல்லது இரகசியமான தகவல்கள் எவற்றையும் பயனர்கள் வெளியிடவோ, தொடர்பாடல் செய்யவோ அல்லது பகிரங்கமாகக் கலந்துரையாடவோ கூடாது.

5. உறுதிப்படுத்தல் (Authentication)

MAS அமைப்புகளை அணுகும் நபர் யார் என்பதை அடையாளம் காண்பதற்கு நிறுவனம் பயன்படுத்தும் வழிமுறையே உறுதிப்படுத்தல் ஆகும்.

MAS அதன் விருப்பப்படி வெவ்வேறு தீர்வுகளை அறிமுகப்படுத்தும், இது நிறுவனம் முழுவதும் முக்கியமான தரவுகளின் பாதுகாப்பை அதிகரிக்க உதவும். இந்த கருவிகள் ஒவ்வொரு பயன்பாட்டிலும் பயனரால் நிகழ்த்தப்படும் அணுகல் மற்றும் செயல்பாடுகள் குறித்த நிகழ்நேர தெரிவுநிலையையும் கட்டுப்பாட்டையும் தருகின்றன. ஏதேனும் சந்தேகத்திற்கிடமான செயற்பாடு கண்டறியப்பட்டால் அடையாளங்காணப்பட்டவர்கள் தடுக்கப்படுவார்கள், மேலும் இதுபோன்ற சந்தர்ப்பங்களில், பயனர்கள் கணக்கின் தடையை அகற்றிக்கொள்ள தங்கள் தகவல் தொழில்நுட்ப நிர்வாகிகளைத் தொடர்பு கொள்ள வேண்டும்.

கடவுச்சொல் பாதுகாப்பு

பயனர்கள் தங்கள் உள்நுழைவு கணக்குகளின் கீழ் நிகழும் அனைத்து நிகழ்வுகளுக்கும் தனிப்பட்ட முறையில் பொறுப்புக்கூற வேண்டும். எனவே, பயனர்கள் தங்கள் கடவுச்சொற்களை இரகசியமாக வைத்திருப்பது அவர்களுடைய பொறுப்பு ஆகும்.

5.1.1. எந்தவொரு சூழ்நிலையிலும் பயனர்கள் தமது கடவுச்சொல்லை வேறொரு நபருக்கு (தகவல் தொழில்நுட்ப ஊழியர்கள், சேவை வழங்குநர்கள், மேலதிகாரிகள், பிற சக ஊழியர்கள், நண்பர்கள் அல்லது குடும்ப உறுப்பினர்கள் உட்பட) கொடுக்கவோ, சொல்லவோ, பகிர்ந்துகொள்ளவோ அல்லது மறைமுகமாகக் குறிப்பிடவோ கூடாது.

5.1.2. செயலிகளின் பயன்பாடுகளின் போது (Internet explorer, மின்னஞ்சல் நிரல்கள் போன்றவை) "கடவுச்சொல்லை நினைவில் கொள்ளுங்கள்(remember password)"அம்சத்தை பயனர்கள் பயன்படுத்தக் கூடாது.

5.1.3. பயனர்கள் ஒவ்வொரு 60 நாட்களுக்கும் ஒரு தடவை தமது கடவுச்சொற்களை மாற்ற வேண்டும். மாற்றப்பட்டதும், அதை மீண்டும் மாற்றுவதற்கு 24 மணித்தியாலங்கள் பயனர் காத்திருக்க வேண்டும்

5.1.4. பயனர்கள் புதிய கடவுச்சொற்களைப் பயன்படுத்தும்போது, அவை எளிதில் நினைவில் வைக்கக்கூடியதாகவும் ஆனால் வேறு நபர்கள் ஊகிக்க கடினமானதாகவும் இருக்க வேண்டும்.

5.1.5. தெளிவான உரை கடவுச்சொற்கள் பொது இணைய இணைப்புகளில் பரிமாறப்படாது.

5.1.6. பயனர்கள் அகராதி சொற்களையோ அல்லது சேர்க்கைகளையோ கடவுச்சொற்களாகப் பயன்படுத்தக்கூடாது.

5.1.7. நிறுவனத்தின் வலையமைப்புக்களை அணுக பயனர்கள் தனிப்பட்ட நோக்கங்களுக்காக (Hotmail, Gmail, skype அல்லது இணைய வங்கியை அணுகுவது போன்றவை) பயன்படுத்தும் அதே கடவுச்சொற்களைப் பயன்படுத்தக்கூடாது.

5.1.8. பயனர்கள் நீண்ட கடவுச்சொற்களைப் பயன்படுத்த வேண்டும், அதில் எண்ணெழுத்து மற்றும் சிறப்புக் குறியீடுகள் கலந்திருக வேண்டும். கடவுச்சொற்கள் நன்கு அறியப்பட்ட அல்லது எளிதில் அணுகக்கூடிய தனிப்பட்ட தகவல்களை (மனைவியின் பெயர், செல்லப் பெயர், நடுப்பெயர், குழந்தையின் பெயர் போன்றவை) அடிப்படையாகக் கொண்டிருக்கக்கூடாது.

5.1.9. சிக்கலான கடவுச்சொற்களுக்கான தேவைகள்.

- கடவுச்சொற்கள் 8 க்கு மேற்பட்ட எண், எழுத்துகளை கொண்டிருக்க □□□□□□□□
- கடவுச்சொற்களில் பின்வருவன இடம்பெற வேண்டும்: □
  - பெரிய எழுத்துகள் மற்றும் சிறிய எழுத்துகள் (A-Z, a-z);

- எண்கள் (0-9)
- சிறப்புக் குறியீடுகள் (! @ # $% ^ & *)

5.1.10. பயனர்கள் தமது கடவுச்சொற்களை மீட்டமைக்க அல்லது மாற்ற கடவுச்சொல் சுய சேவை Portalஇன் கடவுச்சொல் சுய சேவை வசதியைப் பயன்படுத்த வேண்டும்.

5.2 பல்காரணி முறையிலான உறுதிப்படுத்தல் (MFA)

சில செயலிகளைப் பொறுத்தவரையில், MFA ஐ கட்டாய காரணியாகக் கொண்டு அடையாளங்கள் பாதுகாக்கப்படுகின்றன. ஆதரிக்கப்படாத / மரபு சார்ந்த செயலிகள் பயன்பாட்டு கடவுச்சொற்கள் மூலம் அங்கீகரிக்கப்பட வேண்டும். பயனர்கள் தங்கள் கடவுச்சொல்லுடன் MAS வழங்கும் எந்தவொரு சேவை அல்லது MFA பாதுகாக்கப்பட்ட செயலியினுள்ளும் நுழையும்போது, பதிவுசெய்யப்பட்ட சாதனத்திலிருந்து உள்நுழைவை உறுதிப்படுத்த அவர்கள் பதிலளிக்க வேண்டும். இந்த நோக்கத்திற்காக, பயனர்கள் தங்கள் இரண்டாவது சரிபார்ப்பு முறையாக கீழே உள்ள ஒன்று அல்லது அதற்கு மேற்பட்ட சரிபார்ப்பு விருப்பத்தேர்வுகளை ஏற்படுத்த வேண்டும்.

- உறுதிப்படுத்தல் தொலைபேசி
- அலுவலக தொலைபேசி
- மாற்று உறுதிப்படுத்தல் தொலைபேசி
- உறுதிப்படுத்தல் செயலி

ஒரு பயனர் தனது கடவுச்சொல் வேறு ஆட்களுக்குத் தெரிந்துவிட்டதென அறிந்திருந்தால் அல்லது சந்தேகித்தால், அது பற்றி IT உதவிப்பிரிவுக்கு அல்லது SBU / பிரிவு IT பிரதிநிதிக்குக்கு அறிவிப்பதோடு கடவுச்சொல்லையும் உடனடியாக மாற்ற வேண்டும்.

6. மின்னஞ்சல் மற்றும் தகவல் அனுப்பல்

MAS இன் குறிக்கோள்கள் மற்றும் நோக்கங்களோடு ஒத்துழைப்பதற்கும் மேலும் மேம்படுத்துவதற்கும் வணிக மற்றும் பங்கு சார்ந்த பணிகளை நிறைவேற்றுவதற்கும் நிறுவனம் வழங்கிய மின்னஞ்சல், செய்தி மற்றும் நிறுவன சமூக வலைப்பின்னல் சேவைகளைப் பயன்படுத்த பயனர்கள் ஊக்குவிக்கப்படுகிறார்கள்.

6.1 எல்லா நேரங்களிலும், MAS இன் வழங்குநர்கள் அல்லது வாடிக்கையாளர்களின் முக்கியமான அல்லது இரகசிய தகவல்களை வெளியிடுவதைத் தவிர்ப்பதற்காக நிறுவனம் வழங்கிய மின்னஞ்சல், செய்தி மற்றும் பெருநிறுவன சமூக வலைப்பின்னல் கருவிகளில் பகிரப்படும் அல்லது வெளியிடும் எந்தவொரு உள்ளடக்கம் தொடர்பிலும் பயனர்கள் கவனமாக இருக்க வேண்டும்.

6.1.1. பயனர்கள் நிறுவனத்தின் மின்னஞ்சலை அதிகாரப்பூர்வமற்ற நோக்கங்களுக்காகவோ அல்லது அதிகாரப்பூர்வமற்ற மின்னஞ்சலை அனுப்பும் முறையாகவோ பயன்படுத்தக்கூடாது

6.1.2. பயனர்கள் நிறுவனம் வழங்கிய நிறுவனத்தின் மின்னஞ்சலினை, அதிகாரப்பூர்வமற்ற நோக்கங்களுக்காக, தனிப்பட்ட பயன்பாட்டிற்கான உள்நுழைவாகவோ அல்லது தனிப்பட்ட வலைத்தளங்களை அணுகும் முறையாகவும், பயனருக்கு சொந்தமான மற்றும் கட்டணம் செலுத்தப்படும் மொபைல் செயலியையும் எந்தவொரு நுகர்வோர் கணினியையும் பயன்படுத்தவோ பகிரவோ கூடாது.

6.1.3. **குழும நிறுவன தொடர்பாடல் பிரிவின்** வெளிப்படையான ஒப்புதல் இல்லாமல் தொழில் தொடர்பான நோக்கங்களுக்கு பொருந்தாத உள்ளடக்கம் பரப்பப்படக்கூடாது

6.2 MAS இல், நிறுவனம் மின்னஞ்சல் மற்றும் Microsoft 365இல் Microsoft அணிகள் வழங்கும் மற்றும் Yammer வழங்கும் வசதிகள் உத்தியோகபூர்வ மின்னணு தகவல்தொடர்பு முறையாக இருக்கும், மேலும் பயனர்கள் தங்கள் மின்னஞ்சல்களையும், அவர்களின் chat செய்திகளையும், Yammer இடுகைகளையும், அவர்களின் முக்கியமான சந்திப்புகள், பணிகள், செய்திகள் மற்றும் அறிவிப்புகள்

மற்றும் இற்றைப்படுத்தல்களைப் பற்றி அறிந்திருக்க, கிரமமான முறையிலும் பொருத்தமான நேரங்களிலும் சரிபார்க்க வேண்டும் என்று எதிர்பார்க்கப்படுகிறது.

6.3 ஒழுங்கமைப்பு, காப்பகம் மற்றும் அகற்றல் உள்ளிட்ட அவரவருடைய மின்னஞ்சல் நிர்வாகத்திற்கு பயனர்களே பொறுப்பாவார்கள்.

6.3.1. மின்னஞ்சல் அளவிற்கென ஓர் எல்லை உள்ளது. அது பற்றி அறிய, உங்கள் பிரிவு IT பிரதிநிதியை அணுகவும்.

6.3.2. மின்னஞ்சலானது cloud மூலம் நிர்வகிக்கப்படுகிறது. தனிப்பட்ட ரீதியில் மின்னஞ்சலைப் பராமரிக்க வேண்டுகின்ற பயனர்கள் அத்தகைய மின்னஞ்சலை நிர்வகிப்பதற்கும் காப்புப் பிரதி எடுப்பதற்கும் பொறுப்பானவர்களாக இருப்பார்கள். எனினும், உள்ளிட இயந்திரத்தில் இருக்கும் அத்தகைய தகவல்களின் உணர்திறன் மற்றும் இரகசியத்தன்மையைக் கருத்திற்கொண்டு, இந்த வழிமுறையை நாம் பரிந்துரை செய்யவில்லை.

6.4 உங்கள் மின்னஞ்சல் கணக்கை/கடவுச்சொல்லைப் பாதுகாக்கவும்

6.4.1. மின்னஞ்சல் கணக்கு மற்றும் கடவுச்சொல் மின்னஞ்சல் அமைப்பிற்கு ஒரு பயனரை தனிப்பட்ட முறையில் அடையாளம் காட்டுவதாக இருக்கும். மின்னஞ்சல் கணக்கைப் பயன்படுத்தி நிகழ்த்தப்படும் எந்தவொரு செயலும் ஒரு குறிப்பிட்ட பயனரால் மேற்கொள்ளப்படும் செயல்களாக அடையாளம் காணப்படும். எனவே, பலவீனமான அல்லது பகிரப்பட்ட மின்னஞ்சல் கணக்கைப் பயன்படுத்தி மோசடி அல்லது அனுமதியற்ற செயற்பாடு மேற்கொள்ளப்பட்டால், அந்த மின்னஞ்சல் கணக்கின் குறிப்பிட்ட உரிமையாளரே அதற்குப் பொறுப்பாதல் வேண்டும்.

6.5. MAS இல் மின்னஞ்சல் அணுகல் தனிப்பட்ட கணக்குகள் மற்றும் கடவுச்சொற்கள் மூலம் கட்டுப்படுத்தப்படுகிறது. அவர்களின் கணக்கு மற்றும் கடவுச்சொல் தகவலின் இரகசியத்தன்மையைப் பாதுகாப்பது பயனரின் பொறுப்பாகும்.

6.6. வணிகம் தொடர்பான அனைத்து மின்னஞ்சல் தகவல்தொடர்புகளிலும் பொருத்தமான கைதுறப்புகளுடன் நிறுவனத்தின் நிலையான மின்னஞ்சல் கையொப்ப வார்ப்புருவைப் பயனர்கள் பயன்படுத்த வேண்டும்.

6.7. பயனர்கள் வேறு எந்த பயனரின் மின்னஞ்சல் கணக்கையும் அந்த பயனரின் அதிகாரமளிப்பின்றி தானாகவோ அல்லது அந்தப் பயனரின் சார்பாகவோ பயன்படுத்த அனுமதிக்கப்பட மாட்டார்கள்.

6.8. பயனர்கள் அறியப்படாத அல்லது நம்பத்தகாத மூலங்களிலிருந்து பெறப்பட்ட மின்னஞ்சல்கள் மற்றும் இணைப்புகளைத் திறக்கவோ, செயல்படுத்தவோ அல்லது சேமிக்கவோ கூடாது, மேலும் அத்தகைய மின்னஞ்சல்கள் அல்லது இணைப்புகள் இருப்பதை IT உதவி பிரிவினருக்கு தெரிவிக்க வேண்டும்.

வெளியிடத்தில் உருவாக்கப்பட்ட அனைத்து மின்னஞ்சல்களும் அமைப்புக்கு வெளியில் இருந்து வந்தவை என்பதைக் குறிக்கும் வகையில் ‘‘வெளி மின்னஞ்சல்” குறிச்சொல்லைக் கொண்டிருக்க வேண்டும்.

6.9. இரகசியமான அல்லது உணர்திறன் வாய்ந்த உள்ளடக்கம் அல்லது இணைப்புகளைக் கொண்ட மின்னஞ்சல்கள் இரகசியத்தன்மைக் கொள்கைக்கு அமைவாக பாதுகாக்கப்படவும் கையாளப்படவும் வேண்டும்.

6.10. வணிக செய்தி நோக்கங்களுக்காக தனிப்பட்ட மின்னஞ்சல் சேவைகளை (Hotmail, Yahoo Mail அல்லது Gmail போன்றவை) பயன்படுத்த பயனர்களுக்கு அனுமதி இல்லை.

6.11. சமூக ஊடக வலைத்தளங்கள் அல்லது பொது Chat சேவைகளை (WhatsApp, Skype, Google talk போன்றவை) வணிக நோக்கங்களுக்காகப் பயன்படுத்தும்போது பயனர்கள் எச்சரிக்கையாக இருக்க

வேண்டும், ஏனெனில் அந்த பயனர்கள் தகவல் பாதுகாப்புக்கான அமைப்பின் விதிகளை மீறும் இடரை ஏற்க வேண்டும். மேலதிக தகவலுக்கு, **சமூக ஊடகக் கொள்கையை** பார்க்கவும்.

6.12. பொது சாதனம்-செயலிகள் மற்றும் சேவைகளைப் பயன்படுத்துவதைத் தீர்மானிப்பதற்கு முன், சமமான நிறுவனத்தினுடைய குறிப்பிட்ட சாதனம்-செயலிகள் மற்றும் சேவைகளின் கிடைக்கும் தன்மையைப் அறிந்துகொள்ள, பயனர்கள் தத்தமது IT உதவி பிரிவினரை அணுக வேண்டும்.

6.13. பயனர்கள் எந்தவொரு உள்ளடக்கத்தையும் கருத்துகளையும் தங்கள் அலுவலக மின்னஞ்சல் முகவரிகளைப் பயன்படுத்தி பொது சமூக ஊடக தளங்கள், chat சேவைகள், மின்னஞ்சல் பட்டியல்கள் அல்லது செய்தி குழுக்களுக்கு இடுகையிட அனுமதிக்கப்படுவதில்லை. வணிகக் கடமைகளின் சாதாரண போக்கில் இதுபோன்ற ஒரு இடுகை செய்யப்பட வேண்டியிருந்தால், **குழும நிறுவன தொடர்பாடல் பிரிவின்** பொருத்தமான முன் ஒப்புதல் பெறப்பட வேண்டும்.

6.14. இரகசியமான/உணர்திறன்மிக்க மின்னஞ்சல்களின் பாதுகாப்பு

இரகசியமான மற்றும் உணர்திறன் வாய்ந்த மின்னஞ்சல் உள்ளடக்கம் மற்றும் இணைப்புகளை அதிகாரமளிக்கப்படாத அணுகலில் இருந்து பாதுகாக்க பயனர்கள் தங்கள் மின்னஞ்சல் மற்றும் அலுவலக பயன்பாடுகளுடன் வழங்கப்பட்ட தகவல் பாதுகாப்பு செயல்பாட்டைப் பயன்படுத்த ஊக்குவிக்கப்படுகிறார்கள்.

பயனர்கள் MAS உடனான தொடர்பை நிறுத்தும்போது பயனர்களின் மின்னஞ்சல், செய்தி அனுப்பும் வசதி, நிறுவன சமூக வலைப்பின்னல் அணுகல் வசதி என்பனவும் நிறுத்தப்படும்.

கவனிக்கவும்: உற்பத்தித்திறன் மற்றும் வசதியை மேம்படுத்துவதற்காக, தனிப்பட்ட கணினிகள் / மடிக்கணினிகள் மற்றும் மொபைல் சாதனங்களைப் பயன்படுத்தி பயனர்கள் தமது நிறுவன மின்னஞ்சலை அணுக அனுமதிக்கப்படுகிறார்கள். இருப்பினும், நிறுவன மின்னஞ்சலை அணுகவும் பயன்படுத்தவும் பயன்படுத்தப்படும் அனைத்து தனிப்பட்ட சாதனங்களும் எல்லா நேரங்களிலும் பாதுகாக்கப்படுவதை பயனர்கள் உறுதிப்படுத்த வேண்டும் - தனிப்பட்ட முறையில் சொந்தமாக வைத்திருக்கடும் சாதனங்களில் MAS IT சேவைகளைப் பயன்படுத்துதல் பகுதியை பார்க்கவும்.

கவனிக்கவும்: தொலைந்து போன அல்லது தவறவிடப்பட்ட சாதனங்கள் இருந்தால், பயனர்கள் உடனடியாக IT உதவிப் பிரிவுக்கு அல்லது SBU யின்/பிரிவின் IT பிரதிநிதிக்கு அறிவித்து, கடவுச்சொல்லை மாற்ற வேண்டும்.

கவனிக்கவும்: நிறுவனம் வழங்கிய உதவிக் கருவிகள் அல்லது பொது வலைத்தளங்கள், சமூக ஊடக தளங்கள், மின்னஞ்சல் பட்டியல் அல்லது செய்தி குழுக்களில் MAS, அதன் வழங்குநர்கள் அல்லது வாடிக்கையாளர்களின் முக்கியமான அல்லது இரகசிய தகவல்கள் இருப்பதைப் பயனர்கள் அவதானித்தால். அவர்கள் அத்தகைய உள்ளடக்கத்தை உடனடியாக IT உதவிப் பிரிவின் கவனத்திற்குக் கொண்டுவர வேண்டும்.

7. இணையப் பாவனை

7.1 MAS இன் குறிக்கோள்கள் மற்றும் நோக்கங்களை மேம்படுத்துவதற்கும், வணிக மற்றும் பங்கு சார்ந்த பணிகளை நிறைவேற்றுவதற்கும் இணையத்தைப் பயன்படுத்த பயனர்கள் ஊக்குவிக்கப்படுகிறார்கள். இருப்பினும், அவர்கள் பரப்பிய உள்ளடக்கம் அல்லது MAS ஆல் வழங்கப்படும் இணைய சேவைகள் மூலம் அவர்கள் அணுகும் தகவல்களுக்கு பயனர்களே பொறுப்பாவார்கள்.

7.2 பயனர்கள் வணிகம் தொடர்பான செயல்பாடுகளுக்கு மட்டுமே MAS வழங்கிய இணைய சேவைகளை பயன்படுத்த வேண்டும். அத்தகைய சேவையின் சட்டவிரோத அல்லது வணிக நோக்கமற்ற பயன்பாடு அனுமதிக்கப்பட மாட்டாது.

7.3 இணையச் சேவை பதிவு மற்றும் கண்காணிப்பு

7.3.1. நிறுவனத்தினால் வழங்கப்பட்ட மடிக்கணினி மற்றும் டெஸ்க்டாப் கணினிகளில் பயனர்கள் தங்கள் இணைய அணுகல் அமைப்புகளையும் உள்ளமைவுகளையும் மாற்றவோ மாற்ற முயற்சிக்கவோ கூடாது.

7.3.2. MAS இணைய பாதுகாப்புக் கட்டுப்பாடுகளைத் தவிர்ப்பதற்கான செயலிகளை நிறுவ அல்லது பயன்படுத்த பயனர்கள் தடைசெய்யப்பட்டுள்ளனர்.

7.3.3. நிறுவனத்தினால் வழங்கப்பட்ட மடிக்கணினி மற்றும் டெஸ்க்டாப் கணினிகளில் கோப்பு பகிர்வு, peer-to-peer, அரட்டை மற்றும் செய்தியிடல் பயன்பாடுகளை நிறுவ அல்லது பயன்படுத்த பயனர்கள் தடைசெய்யப்பட்டுள்ளனர்.

7.3.4. அங்கீகரிக்கப்படாத உள்ளடக்கம் அல்லது தனிப்பட்ட உள்ளடக்கத்தைப் இணையத்திலிருந்து பதிவிறக்க அல்லது செயல்படுத்த பயனர்கள் MAS இணைய இணைப்பைப் பயன்படுத்தக்கூடாது.

7.3.5. MAS நிறுவன வலையமைப்பிற்கான அணுகல் இருப்பிட அடிப்படையிலான கம்பிமூல வலையமைப்பு இணைப்பு வழியாகவோ அல்லது இருப்பிட அடிப்படையிலான வயர்லெஸ் வலையமைப்பு இணைப்பு வழியாகவோ சாத்தியமில்லாதபோது மாத்திரம் MAS இனால் வழங்கப்பட்ட Dongle மட்டுப்படுத்தப்பட்ட அளவில் பயன்படுத்தப்பட வேண்டும்.

7.3.6. ஒன்லைன் மோசடி திட்டங்கள் மற்றும் இணைய அடிப்படையிலான பிற அச்சுறுத்தல்கள் குறித்து பயனர்கள் தொடர்ந்து தங்களை புதுப்பித்துக் கொள்ள வேண்டும். பயனர்கள் குறிப்பாக வலைத்தளங்கள் அல்லது செயலிகளை அணுகும்போது கவனமாக இருக்க வேண்டும்.

7.3.7. கணினிகள், மடிக்கணினிகள், ஸ்மார்ட் ∴போன்கள் மற்றும் டப்லெட் சாதனங்களில் MAS செயலிகள், மின்னஞ்சல் மற்றும் MAS வழங்கிய கோப்பு சேமிப்பு இடங்களை அணுகும்போது மற்றும் பரிவர்த்தனை செய்யும்போது பயனர்கள் வணிக ரீதியாக கிடைக்கக்கூடிய இலவச அல்லது கட்டண இணைய VPN செயலிகளை (உதா: OneDrive/SharePoint on Office 365) ஒருபோதும் பயன்படுத்தக்கூடாது.

7.3.8. இணையத்தை அணுகும்போது ஏதேனும் பிழைகள் அல்லது விதிவிலக்குகள் ஏற்பட்டால் பயனர்கள் IT உதவி மையத்திற்கு அல்லது SBU/பிரிவு IT பிரதிநிதிக்கு அறிவிக்க வேண்டும்.

7.3.9. பயனர்கள் MAS தொடர்பான பக்கங்கள் அல்லது சமூக ஊடக கணக்குகளை உருவாக்கக் கூடாது அல்லது சமூக தளங்கள் அல்லது வேறு எந்த இணைய எதிர்கொள்ளும் தளத்திலும் MAS தொடர்பான உள்ளடக்கத்தை இடுகையிடக்கூடாது அல்லது ஆயுளு தொடர்பான உள்ளடக்கத்தைக் கொண்டிருக்க, எந்தவொரு வலைத்தளத்தையும் சொந்தமாக வடிவமைக்கக்கூடாது, மேலும் ஒரு வணிகத் தேவை இருந்தால் , பயனர் அத்தகைய தேவைகளை **குழு நிறுவன தகவல் தொடர்பாடல்** பிரிவின் ஊடாக செயற்படுத்த வேண்டும்.

கவனிக்கவும்: அலுவலகத்திற்கு வெளியில் இருந்து இணையத்தை அணுகும்போது, நிறுவனம் வழங்கிய மடிக்கணினிகளைப் பயன்படுத்தும்போது அல்லது சொந்த கணினிகள், மடிக்கணினிகள் அல்லது பிற மொபைல் கணினி சாதனங்களைப் பயன்படுத்தும்போது கவனமாக இருக்கும்படி பயனர்கள் அறிவுறுத்தப்படுகிறார்கள். போலி வலைத்தளங்களுக்கு பயனரை கவர்ந்திழுக்க, அங்கீகரிக்கப்படாத மென்பொருளை நிறுவவும், கணினி வைரஸ்களைப் பரப்பவும், கடவுச்சொற்களைத் திருடவும் மற்றும் / அல்லது முக்கியமான நிறுவனம் மற்றும் தனிப்பட்ட தகவல்களுக்கான அணுகலைப் பெறவும் இணைய தாக்குதலை மேற்கொள்பவர் அதிநவீன நுட்பங்களைப் பயன்படுத்தக்கூடும்.

8. தொலைவிட அணுகல் சேவை (REMOTE ACCESS SERVICE)

தொலைவிட அணுகல் சேவையானது, அலுவலக வலையமைப்பிற்கு வெளியில் இருந்து மின்னஞ்சல் மற்றும் பிற வணிகப் பயன்பாடுகளை மேற்கொள்வதற்கான அணுகல் வசதியை குறிப்பிட்ட பயனர்களுக்கு வழங்குகிறது. வழங்கப்பட்ட அத்தகைய அணுகல் வசதி, வணிகத் தேவையின் அடிப்படையிலும், ஒதுக்கப்பட்ட வேலைப் பொறுப்புகளைச் செய்வதற்குத் தேவையான குறைந்தபட்ச சலுகைகளின்படியும் அமைந்திருக்கும்.

8.1. உற்பத்தித்திறனை மேம்படுத்துவதற்கும் வசதியை மேம்படுத்துவதற்கும் தொலைநிலை அணுகல் வசதிகளைப் பயன்படுத்த பயனர்கள் ஊக்குவிக்கப்படுகிறார்கள். இருப்பினும், தொலைநிலை அணுகல் சேவை ஒரு பொறுப்பான, நம்பகமான மற்றும் பாதுகாப்பான முறையில் பயன்படுத்தப்படுவதை உறுதிசெய்வது பயனர்களின் பொறுப்பாகும், இது நிறுவனத்தின் நோக்கம் மற்றும் குறிக்கோளுக்காக மட்டுமே ஆகும்.

8.2. தனிப்பட்ட அல்லது நிறுவனத்தால் வழங்கப்பட்ட வணிக செயல்பாடுகளுக்கு பயன்படுத்தப்படும் அனைத்து தொலை கணினி உபகரணங்கள் மற்றும் மொபைல் சாதனங்கள் அங்கீகரிக்கப்படாத அணுகல் அல்லது தவறான பயன்பாட்டைத் தவிர்க்க நியாயமான தொடுகை ரீதியான மற்றும் தொழில்நுட்ப பாதுகாப்பு கட்டுப்பாடுகளுடன் செயல்படுத்தப்பட வேண்டும்.

8.3. இத்தகைய கணினிகள் / சாதனங்களில் பொருத்தமான வைரஸ் தடுப்பு மென்பொருள் நிறுவப்பட்டு, இற்றைப்படுத்தப்பட்டு, திறம்படச் செயற்படுத்தப்பட வேண்டும

8.4. இத்தகைய கணினிகள் / சாதனங்களில் நிறுவனத்தால் அங்கீகரிக்கப்பட்ட தனிப்பட்ட firewall நிறுவப்பட்டு, இற்றைப்படுத்தப்பட்டு, திறம்படச் செயற்படுத்தப்பட வேண்டும்

8.5. வைரஸ் தடுப்பு மற்றும் தனிப்பட்ட Firewalls

8.5.1. கணினி / தொடர்புடைய சாதனங்கள், சாதன ஆதரவு இயக்க முறைமையின் (Device supported operating system) சமீபத்திய பதிப்பை இயக்குகின்றன என்பதை பயனர் உறுதிப்படுத்த வேண்டும். உபகரண உற்பத்தியாளரிடமிருந்து (OEM) கிடைத்தவுடன், சமீபத்திய சாதன இயக்க முறைமை இணைப்புகள் மற்றும் புதுப்பிப்புகள் பதிவிறக்கம் செய்யப்பட்டு நிறுவப்பட்டுள்ளன என்பதை பயனர் மேலும் உறுதிப்படுத்த வேண்டும். (பயனரால் இதை உறுதிப்படுத்த முடியாது என்பதால் மேற்கூறியவற்றை சரிபார்க்க, பிரிவின் IT குழுவினரால் தொடர்பு கொள்ள திட்டமிடப்பட்ட அட்டவணையின் அடிப்படையில் பயனர் தங்கள் இயந்திரத்தை சமர்ப்பிக்க வேண்டும்)

8.5.2. தொலைநிலை இணைப்பு அமைப்புகள் அல்லது உள்ளமைவுகளை பயனர்கள் மாற்ற கூடாது.
8.5.3. பயன்பாட்டில் இல்லாதபோது தொலைநிலை அணுகல் சேவையை பயனர்கள் நிறுத்த வேண்டும்.

8.6 Bluetooth & Wireless

கணினிகள் மற்றும் சாதனங்களின் எளிதான மற்றும் நெகிழ்வான தொடர்புகளை செயல்படுத்த பெரும்பாலான நவீன கணினிகள் / சாதனங்கள் Bluetooth மற்றும் வயர்லெஸ் தொழில்நுட்பத்துடன் பொருத்தப்பட்டுள்ளன. இருப்பினும், பலவீனமான பாதுகாப்பு காரணமாக, கணினிகள் / சாதனங்களுக்கான அங்கீகரிக்கப்படாத அணுகலைப் பெற இந்த தொழில்நுட்பங்கள் ஒப்பீட்டளவில் எளிதில் பயன்படுகின்றன. ஆகவே,

8.6.1. நிறுவனத்தின் வலையமைப்புடன் இணைக்கப்படும்போது பயனர்கள் தங்கள் கணினிகள் / சாதனங்கள் வேறு எந்த வலையமைப்புடனும் இணைக்கப்படவில்லை என்பதை உறுதிப்படுத்த வேண்டும்

உதா: ஒரு Broad Band Dongle உடன் இணைக்கவும், அதே நேரத்தில் MAS தனியார் நிறுவன Wifi அல்லது கம்பியாலான (LAN) வலையமைப்புடன் இணைக்கப்பட்டிருத்தல்.

8.6.2. பயனர்கள் தொலைநிலை அணுகலுக்குப் பயன்படுத்தப்படும் கணினிகள் / சாதனங்களை கவனிக்காமல் விடக்கூடாது. பயன்பாட்டில் இல்லாதபோது, அத்தகைய கணினிகள் / சாதனங்கள் சரியாக செயலிழக்க செய்யப்பட்டு பாதுகாப்பாக இருக்க வேண்டும்.

8.6.3. கணினிகள் / சாதனங்கள் தொலைந்து போதல் அல்லது தவறாக வைக்கப்பட்டால் நிலை ஏற்பட்டால், பயனர்கள் உடனடியாக IT உதவிப்பிரிவு அல்லது SBU / பிரிவு IT பிரதிநிதிக்கு அறிவித்து கடவுச்சொல்லை மாற்ற வேண்டும்.

நிறுவனத்தின் வளங்கள் மற்றும் தகவல் தொழில்நுட்ப அமைப்புகளை அணுக பயனர்கள் பொது கணினிகளை (Internet Cafeக்களில் பகிரப்பட்ட கணினிகள் போன்றவை) பயன்படுத்துவதைத் தவிர்க்க வேண்டும். வேறு நபர்கள் திரையை கவனிப்பதிலிருந்தும் ரகசிய தகவல்களைப் பார்ப்பதிலிருந்து பயனர்கள் தங்கள் கணினிகள் / சாதனங்களை பொது இடங்களில் (விமான நிலைய ஓய்வறைகள், உணவகங்கள் , போக்குவரத்தில் இருக்கும்போது போன்றவை) பயன்படுத்தும்போது கவனமாக இருக்க வேண்டும்.

9. நிறுவனத்திற்கு சொந்தமான சாதனங்களில் MAS தகவல் தொழிநுட்ப (IT) சேவையின் பாவனை

9.1 தனிப்பட்ட கணினிகள்

MAS தனிப்பட்ட கணினிகளாக, மடிக்கணினிகள் மற்றும் டெஸ்க்டாப்புகள் இரண்டையும் வழங்குகிறது, அவை அதன் அனைத்து ஊழியர்களுக்கும் சமீபத்திய தரநிலை இயக்க முறைமைகள் மற்றும் அம்சங்களை IT தரத்தின்படி இயங்குகின்றன. தொழில்நுட்ப சேவைகளால் ஒரு பயனர் IDஐ வழங்குவது, அந்த ஊழியரின் முகாமையாளரினால் நிர்ணயிக்கப்பட்ட தேவைக்கேற்ப MAS இன் வெவ்வேறு பயன்பாட்டு அமைப்புகளை அணுக தனிப்பட்ட கணினி அல்லது சாதனத்தின் ஏற்பாட்டை உடனடியாகப் பின்பற்றுகிறது.

பரந்த வளாக இணைய வசதிகளை வழங்குவதோடு, அலுவலக வளாகத்திற்கு வெளியே இந்த சாதனங்களைப் பயன்படுத்துவது, அந்த ஊழியரின் மேலாளரின் ஒப்புதலின் அடிப்படையில் அனுமதிக்கப்படுகிறது.

9.2. மொபைல் சாதனங்கள் (டப்லெட்கள் மற்றும் ஸ்மார்ட் ∴போன்கள்)

9.2.1. MAS SBU இற்கு சொந்தமான மற்றும் MAS தொழில்நுட்ப சேவைகள் குழுவால் நிர்வகிக்கப்படும் மொபைல் சாதனங்கள் மட்டுமே MAS MPLS வலையமைப்பில் சிறப்பாக வரையறுக்கப்பட்ட வயர்லெஸ் வலையமைப்புக்களுடன் இணைவதற்கு அனுமதிக்கப்படுகின்றன.

9.2.2. பொது இணையம் வழியாக App store இலிருந்து MASஇனால் அணுகக்கூடியவையென வரையறுக்கப்பட்ட Portfolioக்கு உட்பட்ட செயலிகளை மட்டுமே MASக்கு சொந்தமான மொபைல் சாதனங்களில் பயன்படுத்த முடியும்.

9.3. MAS தகவல்கள் மற்றும் அமைப்புகளை அணுகுவதற்கு அதிகாரமளிக்கப்பட்டவர்கள் தவிர்ந்த ஏனைய தரப்புக்களினால் தனது சாதனத்திலிருந்து அணுகல் மேற்கொள்ளப்படுவதை தடுக்கும் முழுப் பொறுப்பும் பயனரைச் சார்ந்தாகும்.

9.4 நிறுவனத்திற்கு உணர்திறன்மிக்க தகவல்கள் அத்தகைய தனிப்பட்ட கணினிகளில்/சாதனங்களில் சேமிக்கப்படாதிருப்பதை அல்லது பேணப்படாதிருப்பதை அல்லது தனிப்பட்ட Cloud சேமிப்பக சேவைகளின் மூலம் back-up செய்யப்டாதிருப்பதை பயனர்கள் உறுதிப்படுத்த வேண்டும்.

9.5. தனிப்பட்ட Cloud சேமிப்பக சேவைகளில் பின்வருவனவும் உள்ளடங்கும். நுகர்வோர் பதிப்புகளினால் அவை மட்டுப்படுத்தப்பட மாட்டா. :

- Dropbox
- Box
- Apple iCloud
- Google Drive
- Microsoft Personal OneDrive
- WeChat
- Smart Sheets
- WeTransfer

* Microsoft OneDrive for Business என்பதே உத்தியோகபூர்வ பாவனைக்காக அங்கீகரிக்கப்பட்டது என்பதைக் கவனத்தில் கொள்ளவும். எனவே, MAS ஊழியர்கள் மற்றும் வெளியிடத் தரப்பினருடான தகவல் பகிர்வுகள் Microsoft OneDrive for business வழியாக மட்டுமே செய்யப்பட வேண்டும்.

வேறு Cloud சேமிப்பகத்தைப் பயன்படுத்துவதற்கு, பிரதம நிறைவேற்று அதிகாரியின் இடர் ஏற்பு தேவைப்படும்.

கவனிக்கவும்: உண்மையான பாதுகாப்பு மீறல் அல்லது மீறல் பற்றிய சந்தேகம்இருந்தால், பயனர்கள் உடனடியாக IT உதவிப் பிரிவு அல்லது SBU /பிரிவு IT பிரதிநிதிக்கு அறிவிக்க வேண்டும், தகுந்த தீர்வு நடவடிக்கையை எடுக்க இது உதவும்.

10. தனிப்பட்ட ரீதியில் சொந்தமான உபகரணங்களில் MAS தகவல் தொழிநுட்ப (IT) சேவையின் பாவனை

MAS இன் தனிப்பட்ட வலையமைப்புடன் இணைப்பதன் மூலம் தனிப்பட்ட ரீதியில் சொந்தமான சாதனங்கள் பயன்படுத்தப்படுவதை BYOD என்று MAS வரையறுத்துக் கூறுகின்றது. **இச் செயற்பாடு அனுமதிக்கப்படுவதில்லை.**

இருப்பினும், கீழேயுள்ள கொள்கை விதிகளின் அடிப்படையில் பொது இணையம் வழியாக அணுகப்படும் மின்னஞ்சல் உட்பட MASஇன் தகவல் தொழில்நுட்ப பயன்பாடுகளுடன் இணைக்கப்பட்ட தனிப்பட்ட ரீதியில் சொந்தமான சாதனங்களைப் பயன்படுத்த MAS அனுமதிக்கிறது.

10.1 தனிப்பட்ட கணினிகள்

10.1.1. தனிப்பட்ட முறையில் சொந்தமான கணினிகளைப் பயன்படுத்த அனுமதிக்கப்படும் தரப்பினர்:

- ஒப்பந்த ஊழியர்கள்
- பயிற்சியாளர்கள்
- MAS இனால் பணியமர்த்தப்பட்ட முகாமையாளரின் மேற்பார்வையுடன் சில வணிக செயல்முறைகளில் ஈடுபடும் வெளிப் பங்காளிகள்.

எனினும், MAS இன் தகவல் தொழில்நுட்ப அமைப்புகள் மற்றும் சேவைகள் இணையம் வழியாக, நேரடியாகவோ அல்லது மெய்நிகர் Desktop இடைமுகம் வழியாகவோ அணுகப்பட்டால், அந்த குறிப்பிட்ட நபர்களுக்கு MAS நிறுவனத்தினால் வழங்கப்படும் தனி பயனர் ID மூலம் அங்கீகரிக்கப்பட வேண்டும்.

10.1.2.அதற்கு மேலதிகமாக, பின்வரும் விதிகள் குறிப்பிட்ட நபர்களுக்கு பொருந்தும்...

- அவர்கள் தனிப்பட்ட முறையில் சொந்தமான தனிப்பட்ட கணினிகளை IT நிர்வாகிக்கு விநியோகிக்கப்பட்ட IT தர ஆவணங்களின்படி MAS தொழில்நுட்ப சேவைகளால் அங்கீகரிக்கப்பட்ட சமீபத்திய இயக்க முறைமைகள் மற்றும் அம்சங்களுடன் மட்டுமே பயன்படுத்த வேண்டும்.

- அவர்கள் ஒருபோதும் தங்கள் தனிப்பட்ட கணினிகளில் உரிமம் பெறாத மென்பொருள் அல்லது பாதுகாப்பு மூலம் கடந்து செல்லப்பட்ட (சிறை உடைந்த) சாதனங்களை (broad band வலையமைப்பு சாதனங்கள் போன்றவை) பயன்படுத்தக்கூடாது.

- MAS வசதியை வழங்கும் பொது இணையம் வழியாக மட்டுமே இணைக்கப்பட வேண்டும், அவர்கள் நிலைநிறுத்தப்பட்டுள்ள MAS வணிக வளாகத்தின் தனியார் வலையமைப்புடன் ஒருபோதும் இணைக்கக்கூடாது.

- இந்த கணினிகள் ஒரு நிறுவனத்தால் அங்கீகரிக்கப்பட்ட வைரஸ் தடுப்பு, தனிப்பட்ட firewall மற்றும் மொபைல் சாதன மேலாண்மை மென்பொருளை நிறுவியுள்ளன, புதுப்பிக்கப்பட்டன மற்றும் திறம்பட செயல்படுகின்றன என்பதை அவர்கள் உறுதிப்படுத்த வேண்டும்.

- நிறுவனத்திற்குச் சொந்தமானதாகக் கருதப்படும் மற்றும் தனிப்பட்ட முறையில் சொந்தமான கணினிகளைப் பயன்படுத்தி இந்த வகை நபர்களால் பயன்படுத்தப்பட்ட அல்லது உருவாக்கப்பட்ட அனைத்து தரவுக் கோப்புகளும், நிறுவனம் வழங்கும் Cloud தளத்தில் சேமித்து வைக்கப்பட வேண்டும். நிறுவனத்தால் பணிபுரியும் துறை மேலாளர்கள், தனிப்பட்ட முறையில் சொந்தமான கணினிகளில் சேமிக்கக்கூடாது.

- கணினிகள், மடிக்கணினிகள், ஸ்மார்ட் தொலைபேசிகள் மற்றும் டேப்லெட் சாதனங்களில் MAS செயலிகள், மின்னஞ்சல் மற்றும் மாஸ் வழங்கிய கோப்பு சேமிப்பு இடங்களை அணுகும் போது மற்றும் பரிவர்த்தனை செய்யும் போது பயனர்கள் வணிக ரீதியாக கிடைக்கக்கூடிய இலவச அல்லது கட்டண இணைய VPN செயலிகளை ஒருபோதும் பயன்படுத்தக்கூடாது, (உதா: OneDrive/SharePoint on Office 365).

10.2. மொபைல் சாதனங்கள் (டப்லெட்கள் மற்றும் ஸ்மார்ட .ீபோன்கள்)

10.2.1. தனிப்பட்ட முறையில் சொந்தமான மொபைல் சாதனங்கள் பொது இணையம் வழியாக மட்டுமே இணைக்க அனுமதிக்கப்படுகின்றன, மேலும் இந்த சாதனங்களுக்கு MAS தனியார் வலையமைப்புக்கான இணைப்பு தடுக்கப்பட்டுள்ளது.

10.2.2. பொது இணையம் வழியாக App store இலிருந்து MAS இனால் வரையறுக்கப்பட்ட போர்ட்.்போலியோக்கு உட்பட்ட செயலிகள் மட்டுமே தனிப்பட்ட ரீதியில் சொந்தமான மொபைல் சாதனங்களில் பெற்றுக்கொள்ள முடியும்.

10.3. MAS க்காக பணிபுரியும் காலகட்டத்தில், MAS தகவல் மற்றும் அமைப்புகளை அணுக அங்கீகாரம் பெற்றவர்களைத் தவிர வேறு எந்த தரப்பினராலும் தனிப்பட்ட முறையில் சொந்தமான சாதனத்தை அணுகுவதிலிருந்து பாதுகாத்தலுக்கு பயனர்கள் மட்டுமே பொறுப்பாவார்கள்.

10.4. நிறுவனத்தின் தனிப்பட்ட தகவல்கள் அத்தகைய தனிப்பட்ட கணினிகள் / சாதனங்களில் சேமிக்கப்படுவதில்லை அல்லது பராமரிக்கப்படுவதில்லை அல்லது தனிப்பட்ட Cloud சேமிப்பக சேவைகள் மூலம் காப்புப் பிரதி எடுக்கப்படுவதில்லை என பயனர்கள் உறுதிப்படுத்த வேண்டும். ஒரு மெய்நிகர் டெஸ்க்டாப் இடைமுகம் அல்லது ஒரு நிறுவனத்தின் செயலியை வழங்குவது, பொருந்தக்கூடிய இடங்களில், மற்றும் அந்த மெய்நிகர் டெஸ்க்டாப் இடைமுகம் அல்லது செயலிக்கு மட்டுமே அணுகலை மட்டுப்படுத்துவது இந்த கட்டுப்பாட்டை உறுதி செய்யும் என்று எதிர்பார்க்கப்படுகிறது.

10.5. கணினிகள், மடிக்கணினிகள், ஸ்மார்ட் தொலைபேசிகள் மற்றும் டேப்லெட் சாதனங்களில் MAS செயலிகள், மின்னஞ்சல் மற்றும் MAS வழங்கிய கோப்பு சேமிப்பு இடங்களை அணுகும் போது மற்றும் பரிவர்த்தனை செய்யும் போது பயனர்கள் வணிக ரீதியாக கிடைக்கக்கூடிய ,லவச அல்லது கட்டண இணைய VPN செயலிகளை ஒருபோதும் பயன்படுத்தக்கூடாது, (உதா: OneDrive/SharePoint on Office 365).

* Microsoft OneDrive for Business என்பதே உத்தியோகபூர்வ பாவனைக்காக அங்கீகரிக்கப்பட்டது என்பதைக் கவனத்தில் கொள்ளவும். எனவே, MAS ஊழியர்கள் மற்றும் வெளியிடத் தரப்பினருடான தகவல் பகிர்வுகள் Microsoft OneDrive for business வழியாக மட்டுமே செய்யப்பட வேண்டும்.

கவனிக்கவும்: உண்மையான பாதுகாப்பு மீறல் அல்லது மீறல் பற்றிய சந்தேகம்இருந்தால், பயனர்கள் உடனடியாக IT உதவிப் பிரிவு அல்லது SBU /பிரிவு IT பிரதிநிதிக்கு அறிவிக்க வேண்டும், தகுந்த தீர்வு நடவடிக்கையை எடுக்க இது உதவும்.

11. நிறுவனத்திற்கு சொந்தமான தரவுகளை சேமிப்பதில் FLASH DRIVES ஏனைய அகற்றக்கூடிய சேமிப்புக் கருவிகளின் பாவனை

FLASH DRIVES மற்றும் USB Hard Disks, CDs அல்லது DVDs போன்ற அகற்றக்கூடிய தரவு-சேமிப்பு ஊடகங்கள் திருட்டு, இழப்பு மற்றும் சேதத்திற்கு உள்ளாகக்கூடும்.

எனவே, பயனர்கள் அவற்றை எவ்வாறு பயன்படுத்துவது என்பதில் கவனமாக இருப்பது முக்கியம்.

இந்த ஊடகங்கள், MAS ஊழியர்களால் பாதுகாப்பாகவும் திறமையாகவும் பயன்படுத்தப்படுவதை உறுதி செய்வதற்கு நிறுவனம் பின்வரும் விதிகளை அமைத்துள்ளது:.

11.1 தனியாருக்குச் சொந்தமான CDகள் அல்லது DVDகளை ஊழியர்களும் துணையாளிகளும் பயன்படுத்துவது அனுமதிக்கப்பட மாட்டாது. நிறுவனத்திற்கு சொந்தமான CDகள் மற்றும் DVDகள் மட்டுமே IT உதவி குழுவின் மேற்பார்வையுடன் பயன்படுத்த அனுமதிக்கப்படுகின்றன, அத்துடன், இந்த ஊடகங்கள் வியாபாரப் பிரிவின் முகாமைத்துவத்தினால் சேமிக்கப்பட வேண்டும்.

11.2. MASஇன் ஒவ்வொரு வியாபார பிரிவிலும், நிறுவனத்திற்கு சொந்தமான மற்றும் IT உதவிப் பிரிவினால் பராமரிக்கப்பட்டு விநியோகிக்கப்படும மறைகுறியாக்கப்பட்ட Flash Drives, USB disk-drives என்பவற்றின் பாவனை மட்டுமே அனுமதிக்கபபடும். இந்த இயக்கிகள், ஊழியரின் பயன்பாட்டு காலத்திற்கென வியாபாரப் பிரிவின் மூலம IT உதவிப் பிரிவு வழியாக வழங்கப்படும். காலத்தின் முடிவில் ஊழியரினால் தரவுகள் அழிக்கப்பட்டு சோதனை மற்றும் சேமிப்பிற்காக தகவல் தொழில்நுட்ப உதவிப் பிரிவிடம் ஒப்படைக்கப்பட வேண்டும்.

11.3. மேலும். பயனர் உருவாக்கிய அனைத்து தரவு அல்லது ஆவணக் கோப்புகளும், அவ்வாறு உருவாக்கப்படும் அல்லது மாற்றியமைக்கப்படும் வேளையிலேயே உரிமைகள் என்ற வகையில் பாதுகாக்கப்படுவது கட்டாயமாகும். எல்லா நேரங்களிலும், அதிகாரமற்ற நபர்களின் கைகளில் கிடைத்த பின்னரும்கூட அத்தகைய கோப்புகளின் அனுமதிக்கப்படாத அணுகல்களைத் தடுப்பதற்கு இவ்வாறு பாதுகாக்கப்பட வேண்டும்.

12. மதிப்பீடு மற்றும் கண்காணிப்பு

12.1. MAS IT அமைப்புகள் மற்றும் சேவைகளுக்கான அணுகலைப் பெறுவதற்கு முன்பு, அனைத்து பயனர்களும் இக் கொள்கையின் உள்ளடக்கங்களைப் படித்து புரிந்து கொண்டார்கள் என்பதை உறுதிசெய்வதுடன், அதன்படி நடப்பதற்கு இணங்கவும் வேண்டும்.

12.2. இந்தக் கொள்கை, தகவல் பாதுகாப்புக் கொள்கை, தகவல் தொழில்நுட்ப ஆளுகை மற்றும் முகாமைத்துவக் கொள்கை ஆகியவற்றைக் கண்காணிக்கவும் நடைமுறைப்படுத்தவும் செயல்முறை மற்றும் கருவிகள் பயன்படுத்தப்படும்.

12.3. நிறுவனத்தினால் உருவாக்கப்பட்டுப் பேணப்படும் மின்னஞ்சல்கள், உள்ளக வலையமைப்புத் தளங்கள் மற்றும் நிறுவனத்தின் தரவு சேமிப்பு வசதிகள் ஆகியவற்றிலுள்ள உள்ளடக்கத்தையும் செயலிகளிலுள்ள (SAP போன்றவை) தரவுகளையும் அணுக நிறுவனத்தினால் அதிகாரமளிக்கப்பட்ட ஏற்புடைய அலுவலர்களுக்கு உரிமை உண்டு.

13. இணக்கமின்மை

13.1 கொள்கைக்கு இணங்காத செயல் எதுவும் தெரியவந்தால் பின்வரும் ஒரு வழியில் முறைப்பாடு
செய்யுங்கள்:

- உங்கள் ஸ்தல IT அலுவலரிடம் தெரிவியுங்கள் அல்லது IT உதவி பிரிவில் முறைப்பாட்டைப் பதிவு செய்யுங்கள்
- உங்கள் SBU, பிரிவு அல்லது குழும விதிமுறை அலுவலரிடம் தெரிவியுங்கள்
- DNA உதவி பிரிவு வழியாக முறைப்பாடு செய்யுங்கள்.
- masdnahelpdesk.ethicspoint.com இல் பிரவேசித்து முறைப்பாட்டைச் சமர்ப்பியுங்கள்
- 0112 430 430 ஐ அழைத்து, ஆங்கில ஏவலின்படி 855 867 7899 ஐ டயல் செய்யுங்கள்

13.2. முறைப்பாட்டின் பதிவு மற்றும் விசாரணையுடன் சம்பந்தப்பட்ட சகலரினதும் இரகசியத்தன்மையானது, மத்திய MAS DNA அணி, ஏற்புடைய விதிமுறை அலுவலர்கள், HR பிரிவு மற்றும் பொறுப்புக்கூற வேண்டிய ஏனைய தரப்புகளினால் பேணிப் பாதுகாக்கப்படும்.

13.3. நீங்கள் மத்திய MAS DNA அணி அங்கத்தவர் ஒருவரினால் அல்லது விதிமுறை அலுவலர் ஒருவரினால் தொடர்பு கொள்ளப்படும் சந்தர்ப்பத்தில் திறந்த, நேர்மையான மற்றும் இரகசியத்தன்மையை பேணும் முறையில் நடந்துகொள்வதன் மூலம் நடைமுறையிலுள்ள விசாரணைகளுக்கு ஆதரிப்பது உங்கள் கடமையாகும்.

13.4. ஒரு நபர் புகார் அளித்தார்/அளிக்க முயன்றார், பாதிக்கப்பட்டவரை ஆதரித்தார் அல்லது விசாரணைகளில் பங்கேற்றார் என்ற காரணத்திற்காக அவருக்குப் பதிலடி கொடுப்பது MAS DNA (நடத்தை விதிமுறை) மற்றும் கொள்கைக்கு இணக்கமற்ற நடத்தையாகக் கொள்ளப்படும்.

13.5. நற்பெயர்களுக்குக் களங்கம் உண்டுபண்ணும் முகமாக, தவறான நோக்கங்களுடன் ஆதாரமற்ற பொய்யான குற்றச்சாட்டுகளை முன்வைத்தல் MAS DNAக்கு இணக்கமற்ற செயலாகக் கொள்ளப்படும்..

13.6. இக் கொள்கை குறித்து மேலதிக விளக்கம் எதையும் பெற்றுக்கொள்ள விரும்பினால், தயவுசெய்து policyinfo@masholdings.com ஊடாக DNA உதவிப் பிரிவுடன் தொடர்புகொள்ளவும் அல்லது ஸ்தல IT உதவி நிபுணருடன் தொடர்பு கொள்ளவும். அல்லது Help@masholdings.com ஊடாக IT உதவிப் பிரிவை அணுகவும்.

13.7 பயனர் ஒருவர் இக் கொள்கையை மீறினார் என்று காணப்பட்டால், பிரிவினால் அனுப்பப்படும் எச்சரிக்கைக் கடிதம் உட்பட பொருத்தமான ஒழுங்கு நடவடிக்கை எடுக்கப்படும்.

14. பொறுப்பு

நிறைவேற்று பணிகளில் ஈடுபட்டுள்ள சகல ஊழியர்களும் இக் கொள்கை பற்றிய அறிவை உடையவராதகவும் இக் கொள்கையை பின்பற்றவராகவும் இருப்பதை உறுதி செய்வது ஒவ்வொரு பிரிவுத் தலைவரினதும்/ முகாமையாளரினதும் பொறுப்பாகும். தாம் அவதானிக்கும் அல்லது தமது கவனத்திற்கு கொண்டுவரப்படும் கொள்கை மீறல்களுக்கு எதிராக அவர்கள் உடனடியான மற்றும் பொருத்தமான நடவடிக்கையை எடுக்க வேண்டும்.

15. MAS IT பாவனை கொள்கையின் செல்லுபடியாகும் காலம்

இந்தக் கொள்கை, MASஇன் ஆடைகள் சபையினால் மீளாய்வு செய்யப்பட்டு அங்கீகரிக்கப்பட்டுள்ளது.

தகவல் தொழில்நுட்ப சூழலில் ஏற்படும் மாற்றங்கள், ஏற்புடைய சட்டம், ஒப்பந்த ஏற்பாடுகள், சிறந்த நடைமுறைகள் என்பவற்றில் ஏற்படும் மாற்றங்களுக்கு அமைவாகவும் கொள்கையின் செயற்றிறனில் வீழ்ச்சி ஏற்படும் சந்தர்ப்பங்களில் அதற்குப் பதிலளிக்கும் விதத்திலும் இக் கொள்கை ஆண்டுதோறும் மீளாய்வு செய்யப்படும்.

16. வரைவிலக்கணங்கள்

வைரஸ் எதிர்ப்பு - வைரஸ்கள் போன்ற தீங்கிழைக்கும் அல்லது அங்கீகரிக்கப்படாத திட்டக் குறியீடு இணைப்பில் பரவுவதையோ அல்லது கணினி அமைப்புகளை பாதிப்பதையோ கண்டறிந்து தடுக்க பயன்படும் மென்பொருள்.

குறியாக்கம் - குறியாக்கம் என்பது algorithm ஒன்றைப் பயன்படுத்தி தகவலை மாற்றுவதற்கான செயல்முறையாகும், அந்த தகவலுக்கான அணுகல் வசதியைக் கொண்டிருப்போரைத் தவிர வேறு எவராலும் அதனை அறிந்துகொள்ள மடியாமல் செய்வதே இதன் நோக்கமாகும்.. மறைகுறியாக்கம் என்பது குறியாக்கப்பட்ட தகவலை வாசித்து அறியத்தக்கதாக மீண்டும் மாற்றும் செயல்முறையாகும்.

Firewall - நம்பகமற்ற வலையமைப்புகளிலிருந்து முக்கியமான வலையமைப்புகள் அல்லது அமைப்புகளை தனிமைப்படுத்தவும் பாதுகாக்கவும் பயன்படுத்துவதற்காக சேவையகத்தில் இயங்கும் ஒரு வன்பொருள் சாதனம் அல்லது மென்பொருள் செயலி.

ப்ராக்ஸி சேவையகம் (Proxy Server) - ப்ராக்ஸி சேவையகம் என்பது இணையத்தை அணுகும் உள்ளக பயனர்களை வெளிப்புற அச்சுறுத்தல்களிலிருந்து பாதுகாக்கப் பயன்படுத்தப்படும் ஒரு பாதுகாப்பு அமைப்பு.

MAS - MAS Holdings (Private) Limited மற்றும் அதன் உப நிறுவனங்கள், இணை நிறுவனங்கள் மற்றும் கூட்டு நிறுவனங்கள்

SBU - மூலோபாய வியாபாரப் பிரிவு, MASஇன் உப நிறுவனம் அல்லது இணை நிறுவனம்

பிரிவு - நிதி, மனிதவள, தகவல் தொழில்நுட்பம், புத்தாக்கம் போன்றவற்றை உள்ளடக்கிய (ஆனால் அவை மட்டுமல்ல) MAS SBUக்குள் அடங்கும் ஒரு பிரிவு.

மூன்றாம் தரப்பு - MASஇன் அல்லது அதன் கூட்டு முயற்சிகளின் பகுதியாக இல்லாத நிறுவனம்

IT உதவிப் பிரிவு - பயனர்களுக்கு உதவவும் பயனர்களின் கோரிக்கைகள் மற்றும் புகார்களுக்கு பதிலளிக்கவும் அமைக்கப்பட்டுள்ள தொழில்நுட்ப சேவைகளுக்குள் செயற்படும் ஒரு பிரிவு..