MAS Capital

ISO 27001 Policies & Controls A.5.10: Acceptable use of information and other associated assets

Exported on 02/11/2026 at 06:18

Organizational controls

A.5.10: Acceptable use of information and other associated assets

IT Usage Policy

Latest Note updated by Sasiru Hettiarachchi on 02/11/2026 at 06:16

MAS Group Technology

IT Usage Policy

Document Number: MAS-GT-IS-PO-002

Classification: Internal

Owner: Chief Digital Officer (CDO)

Version: 3.3

Effective Date: 02-Nov-2026

Document History:

Release Date	Revision No	Author(s)	Description	Reviewed & Approved By	Next review date

15-Sep-2021	1.0	ISO	Approved Document	GTRC	Sep-2022
15-Sep-2022	1.0	ISO	Annual Review	GTRC	Sep-2023
04-Sep-2023	2.0	ISO	Amendments were made to the Use of MAS IT services on personally owned devices	GTRC	Sep-2024
01-Mar-2025	3.0	ISO	Amendments done as per new requirements of the standard	GTRC	Sep-2026
01-Mar-2026	3.1	ISO	Updated to ISMS Online	GTRC	Mar-2027
09-July-2026	3.2	ISO	Updated enforcement and compliance section. Introduced MAM	GTRC	Sep-2027
02-Nov-2026	3.3	ISO	Restricted use of public messaging and expanded personal device restrictions on premises (BYOD)	GTRC	Nov-2027

Table of contents

1. Introduction
    - 1.1. Purpose
    - 1.2. Scope
    - 1.3. Roles and Responsibilities
    - 1.4. Laws and Regulations
    - 1.5. Distribution
    - 1.6. Enforcement
    - 1.7. Compliance
    - 1.8. Review and Revision
2. What Is Information Security
3. Information System Usage
4. Authentication

4.1. Password Protection

4.2. Multi-Factor Authentication (MFA)

5. E-Mail And Messaging

6. Internet Usage

6.1. Internet Service Logging and Monitoring

7. Remote Access Service

7.1. Anti-virus and Personal Firewalls

7.2. Bluetooth & Wireless

8. Use of MAS-GT services on company-owned devices

8.1. IT Devices

8.2. Mobile Devices

9. Use of MAS-GT services on personally owned devices

9.1. Personal Computers

9.2. Mobile devices

9.3. Mobile Application Management (MAM)

10. Use of removable media for storage of company-owned data

11. Incident Reporting

11.1. Evaluation and Monitoring

1. Introduction

1.1. Purpose

MAS Holdings Group Technology (hereafter referred to as MAS-GT) provides its employees and authorized third parties with access to its information systems and IT services, based on the job/engagement requirements in a secure, effective, and efficient manner. The IT services provided include (but are not limited to) access to computing devices, access to print services, access to corporate email services, access to business applications and data, access to the Internet and cloud storage, and access to intranet and file shares. This policy establishes a clear, reasonable, secure, and fair standard for the acceptable usage of such information systems and IT services provided by MAS to its employees and third-party users.

1.2. Scope

This MAS IT Usage Policy shall apply to the following parties/groups:

All permanent (including fixed term / contractual employees), and non-permanent employees, which shall include consultants and interns engaged with MAS under contractual terms or letters of engagement (“Employees”).

Advisors, non-executive directors and advisory board members (“Advisors”).

All corporate and individual visitors to MAS premises (“Visitors”).

All suppliers, sub-contractors, and their agents MAS deals with (“Suppliers”).

All MAS customers and their agents MAS engages with (“Customers”) who in the course of their engagement with MAS, have been provided access to MAS information systems and IT services. For easy reference, all the above shall be referred to as 'Users'.

MAS information system users and relevant third parties must read, understand, and formally accept this IT Usage Policy before accessing MAS information systems and IT services.

MAS information system users and third parties having access to MAS Holdings information systems and IT assets shall, at all times, comply with the Information Security Policy and this IT Usage Policy.

1.3. Roles and Responsibilities

Chief Digital Officer (CDO): Shall be accountable for the effective review, approval, communication, implementation, and adoption of this document.

Head of IT Security: Shall own and be accountable for the accuracy and maintenance of this document as well as its effective communication and implementation.

Information Security Officer (IS Officer): Shall own and be responsible for the accuracy and maintenance of this document as well as its effective communication and implementation.

All Users: Including but not limited to temporary employees, third parties contracted and all parties defined in the scope section must read, understand, and formally accept this IT Usage Policy before accessing MAS information systems and IT services.

1.4. Laws and Regulations

This policy shall conform to the legal and regulatory requirements of Sri Lanka and any other country where MAS Holdings conducts business operations. Compliance includes, but is not limited to, The Computer Crimes Act 24 of 2007 of Sri Lanka and any other applicable laws, regulations, or industry standards that govern cybersecurity, data protection, and the safeguarding of organizational information assets.

1.5. Distribution

This document must be shared with all users and intended parties determined by the Information Security Officer (IS Officer). Interested parties can obtain the latest version of this document from ISMS Online.

1.6. Enforcement

All stakeholders including (staff and third-party vendors) having access to MAS-GT information systems shall comply with the Information Security Policy. Such personnel shall be required to execute an agreement with MAS-GT agreeing to abide by this policy.

Prior to being granted access to MAS-GT information systems, employees must have a valid Letter of Appointment (LOA) or Contract of Employment in place.

1.7. Compliance

Systems and services provided by MAS-GT are the property of MAS-GT. This gives MAS-GT the right to monitor all activities performed using these resources.

Users shall maintain continued compliance with all MAS-GT policies, procedures, guidelines, rules, and administrative orders while using MAS-GT systems, facilities, and/or services.

The CDO shall designate persons to perform periodic reviews and provide relevant feedback on the design and operating effectiveness of this policy.

Failure to comply with these guidelines may lead to serious legal and operational consequences. Your cooperation is essential to safeguard the organization and maintain compliance with licensing agreements.

Confidential

Any non-compliance with or breach of policy may lead to investigation and action in line with the organizational A.6.4: Disciplinary process and shall be recorded and responded to through the Incident and Problem Management guideline and audit framework.

Report non-compliance of the policy via one of the following channels.

- Contact the Group Corporate Communications Team
- Speak to your SBU, Value Stream, or Group Code Officer
- Lodge a complaint via the DNA Helpdesk – masdnahelpdesk.ethicspoint.com
- Lodge a complaint via the DNA Hotline – 0723005005 (Hutch), 0758005005 (Airtel), 0117395005 (Dialog)

The MAS Ethics Committee and other accountable parties will maintain the confidentiality of all parties involved in the recording and investigation of the complaint.

It is your responsibility to support ongoing investigation by being open, honest and maintaining confidentiality, in the event you are contacted by a member of the MAS Ethics Committee.

Retaliation against an individual for lodging/ attempting to lodge a complaint, supporting a victim, or participating in investigation amounts to non-compliance of the MAS DNA (Code of Conduct) and the policy.

Reporting unfounded false allegations with wrongful intentions of malice, in a bid to tarnish reputations, amounts to non-compliance of The MAS DNA.

For any clarifications, email policyinfo@masholdings.com, or contact the Site IT Support Specialist or the IT Service Desk (Help@masholdings.com).

1.8. Review and Revision

This policy shall be periodically reviewed and updated to reflect changes in the organization, operating environment, local laws and regulations, industry best practices, and recommendations provided by consultants, advisors, internal and external auditors, and regulatory bodies. The policy shall be reviewed and revised at least once per year or more frequently if required due to significant changes in threat landscapes, regulatory requirements, or organizational operations.

2. What Is Information Security

Information security is the process and practice of protecting the company’s sensitive and business-critical information assets, in electronic or physical form, from unauthorized access, use, disclosure, disruption, modification, interception, recording, or destruction.

The main goals of information security at MAS are to ensure:

Confidentiality of information - Sensitive Customer, Supplier, and MAS information shall only be accessible to those authorized to access such information.

Integrity of information - Business Critical Customer, Supplier, and MAS information shall remain accurate, error-free, and without omissions.

Availability of information - Authorized users shall have access to critical business information when required.

Non-repudiation of electronic transactions – Users shall be held accountable for their actions in electronic transactions.

An information asset is a definable piece of information, stored in any manner, which is recognized as 'valuable' to the company.

3. Information System Usage

Users must take due care to protect MAS-GT systems and information assets from tampering and/or accidental damage.

All MAS-owned, rented, or otherwise managed assets, including information and information systems such as desktops, laptops, mobile devices, printers, networks, servers, and applications, shall be used only for their intended and authorized business purposes.

Users are not permitted to use MAS Information Systems for illegal or unlawful purposes.

Illegal or unlawful use of IT systems includes, but is not limited to copyright infringement, fraud, defamation, plagiarism, harassment, intimidation, obscenity, forgery, impersonation, gambling, computer tampering (e.g. spreading computer viruses, etc.), or unauthorized computer access.

The installation or use of software on company devices without prior approval from MAS-GT is strictly prohibited. Unauthorized software usage, including use on company devices may result in individuals being held directly liable by the respective software providers, in addition to other organizational implications.

To ensure compliance, always seek prior approval for any Software/ App installation. Use only whitelisted and licensed software provided or approved by the MAS-GT. Reach out to the IT Service Desk for assistance with any software-related requests or questions.

Users with administrative rights must not disable or bypass any controls such as, but not limited to antivirus software, proxy servers, and firewalls, implemented to protect MAS networks and information assets.

Users must not post sensitive or confidential information about MAS, its Suppliers, or Customers, on publicly accessible Internet sites, such as social media sites, chat services, mailing lists, blogs, or public newsgroups.

Any User intending to post information about MAS, its Suppliers, or Customers, on publicly accessible Internet sites, must first obtain approval from Group Corporate Communications.

Users shall obtain appropriate intellectual property rights/copyrights or contractual clearances before using any proprietary material.

Users shall not transmit sensitive or confidential information, over the network, without adequate protection controls. If required, the user must first obtain approval from Group Corporate Communications.

Users shall apply due care to avoid falling victim to social engineering attempts, including but not limited to phishing, business email compromise, corporate espionage, and competitive intelligence gathering conducted through electronic media.

Users must not post any sensitive or confidential information about MAS, its suppliers, or customers on Artificial intelligence platforms such as, but not limited to, ChatGPT, Grok AI, Gemini.

Users are strongly advised not to store personal data or personal information on MAS-provided computing devices. MAS shall not be responsible for any breach, loss, or compromise of such personal information stored on MAS-GT devices. Where personal information has been stored and a request is made for its retrieval or extraction, MAS-GT may facilitate such requests at its discretion and convenience, subject to applicable security and operational considerations.

Periodically, MAS shall conduct information security awareness and training sessions. All users are required to participate in such training when invited.

Users must exercise caution when printing confidential information using shared printers, which are designated solely for official purposes.

It is the user's responsibility to ensure that company workstations are adequately secured and that no third party can intentionally or unintentionally view the work carried out on these computing devices.

If a User needs support in communicating sensitive or confidential information, he or she must contact the IT Service Desk or the SBU/division IT representative.

4. Authentication

Authentication is the process by which the organization verifies the identity of the person accessing MAS systems. MAS shall, at its discretion, introduce different solutions that help to increase the protection of critical data across the organization. These tools give real-time visibility and control over access and activities performed by users within each application. Identities shall get blocked if any suspicious activity is detected and, in such instances, users must contact IT Service Desk to unblock the account.

4.1. Password Protection

Users are personally accountable for all events that occur under their login accounts. Therefore, users are responsible for keeping their passwords confidential.

Under no circumstance shall Users give, tell, share, or hint at their password to another person (including IT staff, service providers, superiors, other co-workers, friends, or family members).

Users shall not use the “remember password” feature of applications (such as Web Browsers, email programs, etc.).

Users shall change their passwords every 60 days. Once changed, the user shall need to wait 24 hours before it may be changed again.

Users must use new passwords that they would be able to easily remember but which would be difficult for anyone else to guess.

Clear text passwords shall not be transmitted over public internet connections.

Users must not use dictionary words or combinations as passwords.

Users must not use the same passwords they use for personal purposes (such as accessing Hotmail, Gmail, Skype, or Internet Banking) to access the company network.

Users must use long passwords containing a mix of alphanumeric and special characters. Passwords shall not be based on well-known or easily accessible personal information (such as spouse name, pet name, middle name, child’s name, etc.).

Complex Password Requirements:

Passwords must be at least 12 characters long.

uppercase and lowercase alphanumeric characters (A-Z, a-z), numbers (0-9), and special characters (!@#$%^&).

Users must use the Password Self-Service facility to reset or change their passwords through the password self-service portal.

Users are strictly prohibited from recording their passwords on sticky notes, books, or other printed materials. Additionally, passwords must not be stored in plain text format.

4.2. Multi-Factor Authentication (MFA)

Identities are protected with MFA for certain applications as a compulsory factor. Any unsupported/legacy applications must be authenticated with App passwords.

When users sign into any service or MFA-protected application offered by MAS with their password, they shall also be required to respond to confirm the login from a registered device. For this purpose, the users must set up one or more of the below verification options as their second verification method.

- Authentication Phone
- Office Phone

- Alternate Authentication Phone
- Authenticator App

If a User either knows or suspects that his / her password has been compromised, it must be reported to IT Service Desk or the SBU / division IT representative, and the password shall be changed immediately.

5. E-Mail And Messaging

Users are encouraged to use company-provided email, messaging, and corporate social networking services to collaborate and further the goals and objectives of MAS as well as to fulfil business and role-oriented tasks.

At all times, Users must be mindful about any content shared or posted on the company-supplied email, messaging, and corporate social networking tools to avoid disclosure of MAS, its Suppliers' or Customers' sensitive or confidential information.

Users must not use company email for non-official purposes or as a method of sending non-official email.

Users must not use or share the company email ID provided by the company, for non-official purposes, either as a login for personal use or as a method of accessing personal websites and any consumer PC or mobile/PC application that is owned and paid for by the user.

Content not relevant to work-related purposes must not be circulated without explicit approval from Group Corporate Communications.

At MAS, the provided email and the facility provided by Microsoft Teams in Microsoft 365 shall be the formal mode of electronic communication and users are expected to check their emails and their Team-chat messages, in a consistent and timely manner so that they are aware of important appointments, tasks, messages, announcements, and updates.

Users are responsible for their respective mailbox management, including organization, archival, and clearing.

There is an Email size limit. Users shall consult the IT Service Desk for further information on email size limits.

The email account and password shall uniquely identify a User to the email system. Any actions performed using the email account shall be indicated in the system as actions carried out by a specific User. Therefore, in case of fraudulent or unauthorized activity committed using a compromised or shared email account, it shall be attributed to the specific owner of that email account.

Email access at MAS is controlled through individual accounts and passwords. It is the user's responsibility to protect the confidentiality of their account and password information.

Users shall use the organization's standard email signature template with appropriate disclaimers in all business-related email communications.

Users are not permitted to use any other user's email account by him/her or on behalf of that user unless authorized to do so.

Users shall not open, execute, or store emails and attachments received from unknown or untrusted sources and shall report the presence of such emails or attachments to the IT Service Desk. All externally originated emails prepend the tag "[External Email]" to indicate that the message has arrived from outside the organization.

Emails containing confidential or sensitive content or attachments must be protected and handled in line with the Confidentiality Policy.

Users are not permitted to use personal email services (such as Hotmail, Yahoo Mail, or Gmail) for business messaging purposes.

MAS-provided email and Microsoft Teams are the approved channels for business communication. The use of public messaging and chat services including but not limited to WhatsApp, Skype, Viber, Telegram, and similar

platforms, for MAS business communication is discouraged and shall not be used as a substitute for approved channels.

MAS information of any classification other than Public shall not be shared, forwarded, or discussed over public messaging or chat services, including WhatsApp. This restriction applies to messages, attachments, images, screenshots, and voice notes, and applies equally on MAS-provided and personally owned devices.

Sharing MAS information classified as Confidential-Internal, Confidential-External and MAS Only via WhatsApp or any other public messaging service constitutes a breach of this policy and shall be handled accordingly.

The users are required to continually reach out to their IT support team to check on the availability of equivalent enterprise-specified apps and services before deciding on using the public device apps and services.

Users are not permitted to post any content or comments, using their office email addresses, to public social media sites, chat services, mailing lists, or news groups. If in case such a posting is required to be performed in the normal course of business duties, appropriate pre-approval must be sought from Group Corporate Communications.

Users are encouraged to use the Information Protection functionality provided with their email and Office applications to protect confidential and sensitive email content and attachments from unauthorized access.

Users' email, messaging, and corporate social networking access shall be terminated when the Users terminate their association with MAS.

Users are prohibited from using email in a manner that is disruptive, harmful, or offensive to others. This includes accessing, displaying, or transmitting politically sensitive material or obscene content, such as pornographic or abusive material, and using ethnic slurs or engaging in any activity that may be construed as harassment or disparagement of others.

Users are strictly prohibited from misrepresenting themselves as another user or attempting to modify or gain access to email messages, mailboxes, or archive files that do not belong to them.

The forwarding of chain emails, junk mail, jokes, politically sensitive material, non-business executable files, non-business-related slideshows, videos, images, music files, and any other unsolicited emails or materials deemed a threat to MAS systems and reputation is strictly forbidden.

If an email or an attachment appears suspicious, users shall refrain from responding to the message and promptly notify the IT Service Desk.

Users are permitted to access their corporate email using personal computers/laptops and mobile devices to enhance productivity and convenience. However, Users must ensure that all personal devices used to access and use corporate email are protected at all times.

In case of lost or misplaced devices, users must immediately notify the IT Service Desk or the SBU.

If in case Users notice MAS, its Suppliers' or Customers' sensitive or confidential information present in company-supplied collaboration tools or publicly accessible websites, social media sites, mailing lists, or news groups, such Users must promptly report such content to the IT Service Desk.

6. Internet Usage

Users are encouraged to use the Internet to further the goals and objectives of MAS as well as for fulfilling business and role-oriented tasks. However, Users are solely accountable for the content they disseminate or information they access through the Internet services provided by MAS.

Users must only use MAS-provided Internet services for business-related activities. Illegal or non-business use of such service is not permitted.

Users are prohibited from using the Internet in a manner that is disruptive, harmful, or offensive to others. This includes accessing, displaying, transmitting, or downloading politically sensitive material or obscene content, as well as using ethnic slurs or engaging in any activity that may be construed as harassment or disparagement of others.

Users must exercise caution to avoid violating laws, including the Computer Crimes Act, copyright laws, intellectual property rights, licensing agreements about material obtained from the Internet, and any other applicable laws.

All internet sites accessed through the company networks shall be recorded. The information recorded by the monitoring system includes but is not limited to username, source IP address, destination address, date and time, applications, and service. MAS-GT shall restrict access to specific internet websites and protocols deemed unsuitable for MAS's corporate environment.

Users may access blocked sites or services with permission if deemed appropriate and necessary for business-related purposes.

To request access to a blocked site, users must submit a request specifying the website URL to the IT Service Desk, providing details of the business requirement, along with approval from their immediate supervisor and/or department head.

Users are advised to be careful when accessing the Internet from outside the office, using company provided Laptops, or using the user's own personal computers, laptops, or other mobile computing devices. A knowledgeable attacker can use sophisticated techniques to lure the User to bogus websites, install unauthorized software, spread computer viruses, steal passwords, and/or gain access to sensitive company and personal information.

6.1. Internet Service Logging and Monitoring

All user activity performed using the MAS Internet service is recorded, maintained, and analysed to identify exceptions and unauthorized activity, and to take remedial or disciplinary actions against non-compliance.

Users must not alter or attempt to alter their Internet access settings and configurations on the company-provided devices.

Users are prohibited from installing or using applications that bypass MAS Internet security controls.

Users are prohibited from installing or using file sharing, peer-to-peer, chat, and messaging applications on the company-provided devices.

Users must not use the MAS Internet connection to download or execute unauthorized content or personal content from the Internet.

Use of MAS-provided dongles is strictly limited to be used, only when access to the MAS company network is not possible.

Users shall regularly update themselves about online fraud schemes and other Internet-based threats. Users must be careful and exercise reasonable skepticism when using the Internet, especially when accessing websites or applications.

Users shall never use commercially available free or paid Internet VPN applications on PCs, laptops, mobile phones, and tablet devices when accessing and transacting with MAS Applications, Email, and MAS-provided file storage locations (eg. OneDrive/SharePoint on Office 365).

Users must notify the IT Service Desk or the SBU / division IT representative in case of any errors or exceptions observed while accessing the Internet.

Users must not create MAS-related pages or social media accounts or post MAS-related content on social sites or any other internet-facing site or design any website on their own, to contain MAS-related content, and, in case there is a business requirement, the user shall route such requirements through Group Corporate Communications.

7. Remote Access Service

The remote access service provides identified Users access to email and other business applications from outside the office network. Such access granted shall be based on the business need and according to the

Confidential

least privileges necessary to carry out assigned job responsibilities. For users requiring remote access, a formal request to the IT Service Desk with appropriate approval and justification is required.

Users are encouraged to use the remote access facilities to enhance productivity and improve convenience. However, it is the User's responsibility to make sure that the remote access service is used in a responsible, reliable, and secure manner, only for the purpose and intention of the company.

All remote computer equipment and mobile devices used for business activity, whether personal or company-provided, must be implemented with reasonable physical and technical security controls to avoid unauthorized access or misuse.

Such computers/devices must have a company-approved personal firewall installed, updated and effectively operating.

Users are prohibited from making any modifications to the remote access connection without the explicit approval of the SOC.

Remote users must immediately report any incident or suspected incident of unauthorized access or disclosure of company resources, databases, networks, or information (refer to section Incident Reporting).

Users must avoid using public computers (such as shared computers at Internet Cafes) to access company resources and IT systems. Users must also be careful when using their computers/devices in public places (airport lounges, coffee shops, while in transit, etc.) to avoid perpetrators from observing the screen and capturing confidential information.

7.1. Anti-virus and Personal Firewalls

Computer/device operating systems support anti-virus technologies and personal firewalls. The anti-virus and personal firewalls shall monitor the system and connections for abnormal behaviour and block / raise alerts.

The user must ensure that the computers/devices are running the latest version of the computer / device-supported operating system. Users must further ensure that the latest device operating system patches and updates are downloaded and installed, as soon as they are available from the Original Equipment Manufacturer (OEM).

Users must not defer or repeatedly postpone operating system and security updates (e.g. selecting 'Update later' / 'Remind me later'). Updates must be applied promptly once available.

Users must not tamper with or change the remote connection settings or configurations.

Users must switch off the remote access service when not in use.

7.2. Bluetooth & Wireless

Computers/devices are equipped with Bluetooth and Wireless technology to enable easy and flexible interconnection of computers and devices. However, due to weak security, these technologies are relatively easily compromised to gain unauthorized access to computers/devices.

Users must ensure that their computers/devices are not connected to any other network while connected to the Company network. E.g. connect to an Internet Dongle, whilst connected to the MAS private corporate WIFI or wired (LAN) network.

Users must not leave computers/devices used for remote access unattended. When not in use, such computers/ devices must be properly locked down and secured.

In case of lost or misplaced computers/devices, users must immediately notify the IT Service Desk or the SBU / division IT representative and change the Password.

8. Use of MAS-GT services on company-owned devices

Users are solely responsible for safeguarding their device from access by any party other than those authorized to access MAS information and systems.

Users must ensure that MAS data is not backed up through personal cloud storage services.

Personal Cloud Storage Services include and are not limited to consumer versions of Dropbox, Box, Apple iCloud, Google Drive, Microsoft Personal OneDrive.

Users are not authorized to modify any device security settings. If there is a business justification for such changes, users may contact IT Service Desk with necessary approvals to request the necessary modifications to the device.

Users must be aware that such devices contain company data and take appropriate action to protect the device from being lost or stolen. If an IT Device is lost or stolen the user must immediately notify the IT Service Desk.

Devices shall be returned to the MAS-GT for repairs, replacement, disposal, or exchange. Users are not permitted to hand over the device directly to a vendor or any third party for any purpose without prior approval from the MAS-GT.

User shall ensure that data on their devices is regularly backed up. Backups of MAS data shall be stored only in Official OneDrive.

Users are strictly prohibited from using devices in a manner that is disruptive, harmful, or offensive to others and/or in any way that violates local or international laws.

Company-provided mobile devices shall not be altered or augmented in any way, such as upgrading the hard disk, adding additional RAM, or installing a flash card reader, without prior approval from MAS-GT. Furthermore, any such modifications must be only carried out by the Group Technology.

Company-provided mobile devices are designated for official use only. Users are strictly prohibited from allowing these devices to be used by friends or family members, or from loaning them to any other party.

General use and care guidelines for mobile devices include:

- Ensure that the virus guard is updated with the latest definition files.
- Do not leave the mobile device unattended in public areas (e.g., restaurants, meeting rooms, airports, or a hotel lobby, etc.).
- Avoid leaving the mobile device in view in an unattended vehicle, even for a short period.
- Store the mobile device in locations that do not expose it to extreme heat or cold (e.g., inside a vehicle).
- Avoid exposing the mobile device to excessive vibration or shocks or placing objects on top of it.
- Exercise caution when displaying sensitive information in public spaces and position the screen to prevent others from viewing it whenever possible.
- Be mindful of shoulder-surfing.
- Use a protective carrying case when traveling with a mobile device.
- It is the sole responsibility of the user to take proper care of the allocated mobile devices.

Sharing of information with MAS personnel as well as external parties shall only be done via Microsoft OneDrive for business.

In case of any security breach, suspected or actual, Users must immediately notify the IT Service Desk or the SBU / division IT representative so that appropriate remedial action can be taken.

8.1. IT Devices

MAS provides IT devices, both laptops and desktops, that run the latest standard operating systems and patches as per the IT standards, to all its employees. The provisioning of a user ID by MAS-GT immediately follows the provision of a personal computer or device to access MAS's different application systems as per the requirement set by the Manager of that employee.

Users must confirm and acknowledge the receipt of IT devices.

8.2. Mobile Devices

This section covers mobile devices including, but not limited to Tablets and Laptops owned and managed by MAS-GT. All users are allowed to connect to specially defined Wireless networks within the MAS Network.

Only the MAS-defined portfolio of Applications accessible from the App Store over the Public Internet shall be available for consumption by MAS-owned mobile devices.

9. Use of MAS-GT services on personally owned devices

MAS defines BYOD as the usage of personally owned devices by connecting to the Private Network of MAS. This is not allowed.

No personally owned electronic device shall be brought onto MAS premises by MAS employees without prior written approval from the respective line manager. For the purpose of this section, "device" includes but is not limited to laptops, desktops, tablets, portable storage media, external drives, cameras and recording equipment and networking devices. Exclusion of this will only apply to personal mobile phones. The usage of USB flash drives is prohibited unless an exception is granted via relevant approval and shall be handled in line with the USB Access Management Guideline.

Usage of MAS IT services on personally owned mobile devices is limited for Microsoft applications under MAS Login only with the objective of increasing the productivity. All users (except for any users group approved by the management) are requested to use MAS IT and application services through MAS-GT provided devices only. Any breach arising from the use of a personal device including but not limited to data breaches is the responsibility of the user.

Users are solely responsible to safeguard their personally owned device from access by any party other than those authorized to access MAS information and systems, during the period they work for MAS.

Users must ensure that company sensitive information is not stored or maintained on such personal computers / devices or backed-up through personal cloud storage services. The provision of a Virtual Desktop Interface or a Company App, wherever applicable, and locking access only to that Virtual Desktop Interface or App is expected to ensure this control.

Users shall never use commercially available free or paid Internet VPN applications on mobile phones and tablet devices, when accessing and transacting with MAS Applications, Email and MAS provided file storage locations (e.g. OneDrive/SharePoint on Office 365).

9.1. Personal Computers

In the event that the approval has been granted for the use of personally owned computers, users shall comply with the following requirements:

Users must use personally owned personal computers only with the latest operating systems and patches.

Users must refrain from using pirate software, pirate licenses or security-by-passed (jail-broken) devices appended (such as broad band network devices) to their personal computers. If any data breach or security breach happens through a personal device which has a pirate software or pirate licenses installed, the individual must take the responsibility.

User must connect only via the public Internet for which MAS shall grant that facility and must never connect to the private network of the MAS Business Premises they are stationed at.

All data files deemed to be owned by the company and used or created by this class of individuals using such personally owned computers, must be stored in the cloud-storage locations provided by the company with due rights-protection set by the supervising functional or department managers employed by the company, and shall not be kept stored in the personally owned computers.

Users shall never use commercially available free or paid Internet VPN applications on PCs and Laptops, when accessing and transacting with MAS Applications, Email and MAS provided file storage locations (e.g. OneDrive/SharePoint on Office 365).

User shall never install or use torrent on the personal computers which access MAS applications, email and MAS provided file storage locations.

9.2. Mobile devices

Personally owned mobile devices are allowed to connect only via the public internet and connection to the MAS Private Network is blocked for these devices.

Users must keep MAS business applications including but not limited to Microsoft Teams, Outlook on the latest available version on personally owned mobile devices.

The MAS defined portfolio of Applications are accessible from the App store over the Public Internet and shall be made available for consumption by personally owned mobile device users through the MAS-approved MAM solution. Installation of the MAM solution is mandatory based on user groups selected by MAS management for such access (refer to Section 9.3).

9.3. Mobile Application Management (MAM)

Where MAS IT services or applications are accessed on personally owned mobile devices, installation and continued use of the MAS-approved Mobile Application Management (MAM) solution is mandatory based on user groups selected by MAS management. MAM secures MAS business applications and data on the device. Exceptions shall be assessed and approved by the Data Protection Team on a case-by-case basis. Access may be withheld or revoked where MAM is not installed or is removed.

Because personally owned devices are not subject to the full device-level controls applied to MAS-owned devices, MAM is used to secure MAS business applications and data at the application level, enabling MAS to enforce data protection, control corporate data within approved apps, and remove MAS data from a personal device where necessary (for example, on loss, compromise, or termination), without affecting the user's personal data.

10. Use of removable media for storage of company-owned data

Flash drives and other removable data-storage media such as USB hard disks, CDs or DVDs are susceptible to theft, loss, and damage.

Therefore, users must be mindful of how to use them. The company sets the following rules to ensure that these media are used safely and effectively by its employees. Refer to the USB Access Management Guideline for further guidance.

The usage of privately owned CDs and DVDs by employees and associates is not allowed. Only company-owned CDs and DVDs are allowed for use with IT support team supervision, and the media must be stored by the management of the Business Unit.

Additionally, it is strongly recommended that all user-created data or document files are rights-protected at the point those files are created or modified by the user.

11. Incident Reporting

Users bear the responsibility of promptly reporting any suspicious events in the company's information security and any instances of potential misuse or violation of this policy to their respective unit head and the SOC through service desk ticket or e-mail: SOC@masholdings.com.

An information security incident is any event that threatens the confidentiality, integrity, or availability of company information or information systems. Examples include but are not limited to unauthorized access to data or systems, data breaches or leaks, loss or theft of company devices or data, malware or ransomware attacks, phishing attempts and any activity that compromises network security.

All users must report suspected information security incidents immediately upon discovery.

All incident reports shall be treated as confidential. The company shall take appropriate steps to protect the identity of the user reporting the incident.

Adherence to this policy is mandatory. Failure to report suspected incidents promptly may result in disciplinary action.

11.1. Evaluation and Monitoring

Prior to gaining access to MAS IT systems and services, all Users shall review and provide confirmation that they have read and understood the contents of this policy and they shall comply accordingly.

Process and tools shall be deployed to monitor and enforce compliance to this policy, Information Security Policy.

The relevant authorized personnel appointed by the CDO shall have the right to access the content in email, intranet sites and data-storage facilities of the Company, created and maintained by users, and the data content in applications (such as SAP) to which a User is given access to.

Due: 02/11/2027