ACCEPTABLE USAGE POLICY

SECURE, SMART, AND RESPONSIBLE: YOUR TECHNOLOGY USAGE GUIDE

INLINE WITH ISO 27001:2022

MINISTRY OF
MOS
SECURITY

Document Management Information

Document Title:	Acceptable Use Policy
Document Number:	ORGANISATION-ACCEP-USE-POL
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	Name	Designation
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

Contents

1. Purpose

The purpose of the [ORG NAME] Acceptable Usage Policy is to establish clear guidelines for the appropriate use of [ORG NAME] Information Resources. This policy aims to safeguard the confidentiality, integrity, and availability of all information that is created, collected, and maintained by the organization.

2. Audience

This policy applies to any individual, entity, or process that interacts with [ORG NAME] Information Resources, including employees, contractors, vendors, and any other authorized users.

3. User Responsibilities

1. Users must utilize only company-approved technology and services for carrying out their responsibilities.
2. All enterprise assets provided to users are loaned strictly for the performance of essential job functions.
3. Upon termination of employment or contract, all company-provided IT assets, along with any associated data, must be returned.
4. Users are responsible for securing their physical workspace, including locking computers when unattended.
5. Personally Identifiable Information (PII), confidential information, and any sensitive data must not be left exposed or accessible in workspaces.
6. Users must protect all information, systems, and assets in their care from loss, damage, or unauthorized access.
    a. Any lost or damaged equipment must be reported to the IT department promptly.
7. Passwords must be stored securely, and only approved password management tools should be used for digital storage.
8. Users must only access systems, applications, files, and data to which they have been explicitly granted permission. Possessing the technical ability to access information does not imply authorization.
9. Only designated and authorized users are permitted to post content or make statements on behalf of the company on social media, blogs, or other internet platforms.
10. Information and knowledge gained during employment must remain confidential, and this obligation continues after the end of employment.

4. Personal Use

1. Users are permitted limited personal use of enterprise assets, such as browsing websites and checking personal email. a. Users may access web-based personal password managers on enterprise assets; however, local installation of a password manager requires IT approval.
    a. Enterprise passwords must not be stored in personal password managers.
    b. Users must not use browser synchronization or browser profiles that transfer browser history between personal devices and enterprise assets (or vice versa).

2. Users must not use personal accounts (e.g., Apple ID, Google Account, Microsoft Account) as device-wide accounts on enterprise devices unless explicitly authorized by the enterprise.
    a. Users must collaborate with IT to create enterprise-specific accounts for required assets or third-party services, such as creating an enterprise-owned Apple ID for an Apple device.
3. Users are prohibited from using enterprise license keys on personal devices without enterprise authorization.
4. Enterprise data must not be stored on non-enterprise personal cloud storage platforms (e.g., Google Drive, Microsoft OneDrive, Dropbox).
5. Personnel must comply with all [ORG NAME] policies when using [ORG NAME] information resources and/or during company time. If any policy requirement or responsibility is unclear, personnel should seek clarification from the Information Security Committee.
6. Personnel must promptly report harmful events or policy violations involving [ORG NAME] assets or information to their manager or a member of the Incident Handling Team. Such events include, but are not limited to:
    a. Technology incidents: Any event that may cause failure, interruption, or loss of availability of [ORG NAME] Information Resources.
    b. Data incidents: Any potential loss, theft, or compromise of [ORG NAME] information.
    c. Unauthorized access incidents: Any potential unauthorized access to a [ORG NAME] Information Resource.
    d. Facility security incidents: Any damage or unauthorized access to a [ORG NAME]-owned, leased, or managed facility.
    e. Policy violations: Any potential violation of [ORG NAME] policies, standards, or procedures.
7. Personnel must not engage in activities that:
    a. Harass, threaten, impersonate, or abuse others.
    b. Degrade the performance of [ORG NAME] Information resources.
    c. Deprive authorized personnel access to [ORG NAME] Information resources.
    d. Obtain additional resources beyond what is allocated; or
    e. Circumvent [ORG NAME] security measures.
8. Personnel must not download, install, or run security programs or utilities that expose or exploit system weaknesses. For example, personnel should not use password-cracking programs, packet sniffers, port scanners, or any other non-approved programs on [ORG NAME] Information Resources.
9. All inventions, intellectual property, and proprietary information developed on [ORG NAME] time or using [ORG NAME] Information Resources (including reports, drawings, blueprints, software codes, data, and technical information) are the property of [ORG NAME].
10. Encryption usage must be managed to ensure designated [ORG NAME] personnel can access all data promptly.
11. [ORG NAME] Information Resources are provided to facilitate business operations and should not be used for personal financial gain.
12. Personnel are expected to cooperate with incident investigations, including federal and state investigations.
13. Personnel must respect and comply with all legal protections (patents, copyrights, trademarks, and intellectual property rights) for any software or materials accessed, used, or obtained via [ORG NAME] Information Resources.

14. Personnel must not intentionally access, create, store, or transmit material that [ORG NAME] deems offensive, indecent, or obscene.

5. Prohibited Use

1. Only devices that have been explicitly approved and authorized are permitted to connect to enterprise-owned or managed networks. This includes portable devices, removable media (e.g., USB drives), and personal devices.
2. Users are prohibited from sharing their passwords or permitting others to use their accounts.
    a. Users will be held accountable for all actions taken under their assigned usernames and accounts.
3. Users must not attempt to bypass authentication controls or compromise the security of any user account or system.
4. Installation of software, hardware, or modification of system configurations on enterprise assets is strictly prohibited unless explicitly authorized as part of the user's role.
5. Engaging in activities aimed at disrupting enterprise networks or assets is strictly forbidden.
   a. Users are not permitted to engage in network monitoring, port scanning, or security scanning unless it falls within their designated job responsibilities and has been formally approved.
6. Users are not allowed to utilize enterprise resources for personal commercial gain.
7. The use of browser features such as "Remember Me" or "Remember Password" is strictly prohibited for enterprise accounts.

6. Access Management

1. Access to information is strictly granted on a "need-to-know" basis.
2. Users must use only the network and host addresses allocated by [ORG NAME] IT. Attempts to access any data or applications without proper authorization or explicit consent are strictly prohibited.
3. All remote connections to internal [ORG NAME] networks must be made using approved [ORG NAME]-provided virtual private networks (VPNs).
4. Personnel must never share access credentials, including passwords or other authentication mechanisms, with anyone who is not specifically authorized to receive them, including IT support staff.
5. Users must ensure that personal authentication credentials, including the following, remain confidential:
    a. Account passwords
    b. Personal Identification Numbers (PINs)
    c. Security tokens (e.g., Smartcards)
    d. Multi-factor authentication details
    e. Access cards or physical keys
    f. Digital certificates or similar authentication devices
6. Any access cards, security tokens, or keys that are no longer required must be promptly returned to the relevant security personnel.

7. Lost or stolen access cards, security tokens, or keys must be reported immediately to physical security.
8. A replacement fee may be charged for lost, stolen, or unreturned access cards, security tokens, or keys.

7. Authentication/Passwords

1. All personnel are responsible for keeping their personal authentication information confidential.
2. Group or shared authentication information must only be disclosed to authorized members of the group.
3. All passwords, including initial or temporary passwords, must adhere to [ORG NAME] standards, which include:
    a. Meeting minimum requirements for length, complexity, and password history.
    b. Avoiding easy-to-guess details tied to the user, such as names, birthdates, or other personal identifiers.
    c. Not reusing passwords from personal or non-business accounts.
4. Whenever possible, unique passwords should be used for each system or account.
5. User account passwords must never be disclosed to anyone, including [ORG NAME] support staff or external contractors.
6. If there is any suspicion that a password has been compromised, it must be immediately changed.
7. Password circumvention through the use of application memory, embedded scripts, or hardcoded passwords in software is not permitted.
8. Security tokens (e.g., Smartcards) must be returned when requested or upon termination of employment or contract with [ORG NAME], if they have been issued.

8. Clear Desk/Clear Screen

1. Personnel must log off from applications or network services when they are no longer in use.
2. Workstations and laptops must be logged off or locked whenever personnel leave their workspace unattended.
3. Confidential or sensitive internal information must be removed from desks or secured in locked drawers or file cabinets when workspaces are left unattended or at the end of the workday, particularly when the workspace cannot be physically secured.
4. Personal items such as phones, wallets, and keys must be stored in locked drawers or cabinets when workspaces are unattended.
5. File cabinets containing confidential information must be locked when not in use or when unattended.
6. Physical or electronic keys used to access confidential information must not be left unattended on desks or in workspaces that are not physically secured.
7. Laptops must be secured with a locking cable or stored in locked drawers or cabinets when the work area is unattended or at the end of the workday, especially if the laptop is not encrypted.

8. Passwords must never be stored in visible locations, such as on or beneath a computer or in any other easily accessible place.
9. Documents containing confidential information should be immediately retrieved from printers, fax machines, or other shared office devices.

9. Data Security

1. Approved encryption methods must be used for transmitting confidential information over public networks (e.g., the Internet).
2. Confidential information sent via USPS or other postal services must be secured in compliance with the Information Classification and Management Policy.
3. Only authorized cloud computing applications may be used to share, store, or transfer confidential or internal information.
4. Information should be shared, handled, transferred, stored, and disposed of appropriately, according to its sensitivity and classification.
5. Personnel must avoid discussing confidential information in public places, over unsecured communication channels, or in open offices and meeting areas.
6. Confidential information must be transported either by authorized [ORG NAME] employees or by couriers approved by IT management.
7. All electronic media containing confidential information must be securely disposed of in accordance with approved methods. Personnel must contact IT for assistance with the proper disposal of such media.

10. Email and Electronic Communication

1. Auto-forwarding emails or electronic messages to external systems outside the [ORG NAME] network is strictly prohibited.
2. Electronic communications must not misrepresent the sender’s identity or the [ORG NAME].
3. Personnel are responsible for the actions taken under their assigned accounts and must safeguard these accounts accordingly.
4. Accounts must not be shared without prior approval from [ORG NAME] IT, except for calendaring functions that may be shared among employees.
5. Employees are prohibited from using personal email accounts to send or receive [ORG NAME] confidential information.
6. Personal use of [ORG NAME]-provided email must not:
    a. Involve solicitation.
    b. Be associated with any political organization, except for the [ORG NAME]-sponsored Political Action Committee (PAC).
    c. Harm or potentially harm the reputation of the [ORG NAME].
    d. Forward chain emails.
    e. Contain or promote unethical or anti-social behavior.
    f. Violate local, state, federal, or international laws or regulations.
    g. Lead to unauthorized disclosure of [ORG NAME] confidential information.
    h. Violate any other [ORG NAME] policies.

7. Confidential information must only be sent via secure, approved electronic messaging solutions.
8. Personnel must exercise caution when responding to emails, clicking on embedded links, or opening attachments.
9. Out of Office or automated email responses should not disclose confidential or internal information, such as employment details, internal phone numbers, locations, or any other sensitive data.

11. Hardware and Software

1. All hardware must receive formal approval from IT Management before being connected to [ORG NAME] networks.
2. Any software installed on [ORG NAME] equipment must be pre-approved by IT Management and installed by authorized [ORG NAME] IT personnel.
3. [ORG NAME] assets that are taken off-site must remain physically secured at all times.
4. Personnel traveling to High-Risk locations, as defined by the FBI and the Office of Foreign Assets Control, must obtain IT approval prior to traveling with [ORG NAME] assets.
5. Employees must not allow family members or any other unauthorized individuals to access [ORG NAME] Information Resources.

12. Internet

6. The Internet must not be used to transmit [ORG NAME] confidential or internal information unless the confidentiality and integrity of the information can be assured, and the recipient(s) are verified.
7. Internet usage involving [ORG NAME] network or computing resources must be limited strictly to business related activities. The following unapproved activities are prohibited:
    a. Playing recreational games,
    b. Streaming media for personal use,
    c. Personal social media activity,
    d. Accessing or distributing pornographic or sexually explicit materials,
    e. Attempting or making unauthorized entry into any network or computer accessible via the Internet,
    f. Engaging in activities that violate other [ORG NAME] policies.
8. Accessing the Internet from outside the [ORG NAME] network using a [ORG NAME]-owned device is subject to the same policies that apply to Internet usage within [ORG NAME] facilities.

13. Mobile Devices and Bring Your Own Device (BYOD)

1. The use of personally owned mobile devices to connect to the [ORG NAME] network is a privilege that requires formal approval from IT Management.
2. All personally owned laptops and workstations must have approved antivirus, anti-spyware software, and active personal firewall protection.
3. Mobile devices used to access [ORG NAME] email accounts must have a PIN or other authentication mechanism enabled.

4. Confidential information must only be stored on devices that are encrypted in accordance with the [ORG NAME] Encryption Standard.
5. [ORG NAME] confidential information must not be stored on any personally owned mobile device.
6. Any theft or loss of a mobile device that has been used to create, store, or access confidential or internal [ORG NAME] information must be reported immediately to the [ORG NAME] Security Team.
7. Mobile devices must maintain up-to-date versions of all software and applications.
8. All personnel are expected to use mobile devices in a responsible and ethical manner.
9. Jail-broken or rooted mobile devices are not permitted to connect to [ORG NAME] Information Resources.
10. [ORG NAME] IT Management reserves the right to remotely wipe mobile devices without prior notice, as stipulated in the Mobile Device Email Acknowledgement.
11. In the event of a suspected security incident or breach involving a mobile device, it may be necessary to remove the device from personnel's possession as part of a formal investigation.
12. Mobile device usage related to [ORG NAME] Information Resources may be monitored at the discretion of [ORG NAME] IT Management.
13. [ORG NAME] IT support for personally owned mobile devices is limited to assisting personnel in complying with this policy. [ORG NAME] IT is not responsible for troubleshooting device usability issues.
14. The use of personally owned mobile devices must comply with all other [ORG NAME] policies.
15. [ORG NAME] reserves the right to revoke mobile device usage privileges if personnel fail to comply with the requirements outlined in this policy.
16. Texting or emailing while driving is strictly prohibited during company time or when using [ORG NAME] resources. Only hands-free communication is permitted while driving, whether on company time or when using [ORG NAME] resources.

14. Physical Security

1. The use of photographic, video, audio, or any other recording equipment, including cameras integrated into mobile devices, is strictly prohibited in secure areas.
2. Personnel are required to display their photo ID access cards at all times while within the building.
3. Personnel must badge in and out of access-controlled areas. Activities such as piggybacking, tailgating, propping doors open, or any other actions intended to circumvent door access controls are expressly forbidden.
4. Visitors entering card-controlled areas of the facilities must be accompanied by authorized personnel at all times.
5. Consumption of food and beverages is prohibited within data centers. Personnel should exercise caution when eating or drinking near workstations or information processing facilities.

15. Privacy

1. Information created, transmitted, received, or stored on [ORG NAME] Information Resources is not considered private and may be accessed by IT personnel at any time, under the direction of executive management and/or Human Resources, without the knowledge of the user or resource owner.
2. [ORG NAME] reserves the right to log, review, and utilize any information stored on or transmitted through its Information Resource systems.
3. Systems Administrators, [ORG NAME] IT personnel, and other authorized [ORG NAME] staff may have privileges that extend beyond those granted to standard business personnel. Individuals with extended privileges must not access files or information that are not necessary for the performance of their job-related tasks.

16. Removable Media

1. The utilization of removable media for the storage of [ORG NAME] information must be justified by a valid business case.
2. All use of removable media must receive prior approval from [ORG NAME] IT.
3. The use of personally owned removable media for the storage of [ORG NAME] information is strictly prohibited.
4. Personnel are not permitted to connect removable media from unknown sources without obtaining prior approval from [ORG NAME] IT.
5. Confidential and internal [ORG NAME] information must not be stored on removable media unless encryption is employed.
6. All removable media must be stored in a safe and secure environment.
7. Any loss or theft of a removable media device that may have contained [ORG NAME] information must be reported to [ORG NAME] IT immediately.

17. Social Media

1. Communications regarding social media must adhere to all applicable [ORG NAME] policies.
2. Personnel are personally accountable for the content they publish online.
3. The creation of any public social media account intended to represent [ORG NAME], or any account that may reasonably be perceived as an official [ORG NAME] account, requires prior approval from the [ORG NAME] Communications Department.
4. When discussing [ORG NAME] or matters related to [ORG NAME], personnel should:
    a. Identify themselves by name,
    b. Indicate that they are a representative of [ORG NAME], and
    c. Clearly state that their views are personal and not those of [ORG NAME], unless explicitly authorized to speak on behalf of [ORG NAME].
5. Personnel must not misrepresent their roles within [ORG NAME].
6. When publishing content relevant to [ORG NAME] in a personal capacity, a disclaimer must accompany the content. An example disclaimer is: “The opinions and content expressed are my own and do not necessarily represent the position or opinions of [ORG NAME].”

7. Content posted online must not violate any applicable laws, including copyright, fair use, financial disclosure, or privacy laws.
8. Discriminatory language, including but not limited to references based on age, sex, race, colour, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, marital status, or any other legally recognized protected status under federal, state, or local laws, regulations, or ordinances, will not be tolerated in any published content associated with [ORG NAME].
9. Confidential information, internal communications, and non-public financial or operational information must not be published online in any format.
10. Personal information pertaining to customers must not be published online.
11. Personnel authorized to post, review, or approve content on [ORG NAME] social media platforms must adhere to the [ORG NAME] Social Media Management Procedures.

18. Voicemail

1. Personnel should exercise discretion when disclosing confidential or internal information in voicemail greetings, including employment data, internal telephone numbers, location information, or any other sensitive data.
2. Personnel must not access another user's voicemail account unless explicitly authorized to do so.
3. Disclosure of confidential information in voicemail messages is strictly prohibited.

19. Incidental Use

1. As a convenience to [ORG NAME] personnel, incidental use of Information Resources is permitted, subject to the following restrictions:
    a. Incidental personal use of electronic communications, internet access, fax machines, printers, copiers, and similar resources is restricted to [ORG NAME]-approved personnel and does not extend to family members or acquaintances.
    b. Incidental use must not incur direct costs to [ORG NAME].
    c. Incidental use must not interfere with the regular performance of an employee's work duties.
    d. No files or documents may be sent or received that could potentially lead to legal action against, or embarrassment for, [ORG NAME] or its customers.
2. The storage of personal email messages, voice messages, files, and documents within [ORG NAME] Information Resources must be minimal.
3. All information stored on [ORG NAME] Information Resources is owned by [ORG NAME] and may be subject to open records requests. Such information may be accessed in accordance with this policy.

20.Enforcement

1. Policy Violations

Violation of the policy will result in corrective action from the management. Disciplinary action will be consistent with the severity of the incident, as determined by the investigation, and may include, but not limited to

- Loss of access privileges to information assets
- Termination of employment or contract.
- Other actions deemed appropriate by management, HR division, Legal division and their relevant policies

Violation or deviation of the policy shall be reported to the service desk and a security incident record has to be created for the further investigation of the incident.

2. Policy Exceptions

Any exceptions to this policy have to be formally approved by the Chief Information Security Officer. All the exceptions shall be formally documented in the standard IT exceptions request form.

The exception request shall follow the below mentioned approval matrix.

First level	**Unit Manager**
Second Level	**Information Security Officer**
Third Level	**Chief Information Security Officer**

After approval by the Chief Information Security Officer, the exception request form should be forwarded to relevant IT unit for execution.

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

MINISTRY OF
MOS
SECURITY

WWW.MINISTRYOFSECURITY.CO