Status:	☐ Working Draft	☒ Approved	☐ Adopted
Document Owner:	MFA Information Security Committee		
Last Review Date:	August 2023		

Acceptable Use Policy

Purpose

The purpose of the MFA Information Resources Acceptable Use Policy is to establish acceptable practices regarding the use of MFA Information Resources **Information Resources** in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Audience

The MFA Information Resources Acceptable Use Policy applies to any individual, entity, or process that interacts with any MFA Information Resources **Information Resource**.

Contents

Policy

Acceptable Use

- Personnel are responsible for complying with MFA Information Resources policies when using MFA Information Resources information resources and/or on MFA Information Resources time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.
- Personnel must promptly report harmful events or policy violations involving MFA Information Resources assets or information to ***their manager or a member of the Incident Handling*** Team. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to MFA Information Resources
    - Data incident: any potential loss, theft, or compromise of MFA Information Resources information.
    - Unauthorized access incident: any potential unauthorized access to a MFA Information Resources **Information Resource**.
    - Facility security incident: any damage or potentially unauthorized access to a MFA Information Resources owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other MFA Information Resources policies, standards, or procedures.
- Personnel should not purposely engage in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of MFA Information Resources
    - deprive authorized MFA Information Resources personnel access to a MFA Information Resources
    - obtain additional resources beyond those allocated.
    - or circumvent MFA Information Resources computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, MFA Information Resources personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any MFA Information Resources **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on MFA Information Resources time and/or using MFA Information Resources **Information Resources** are the property of MFA Information Resources.
- Use of encryption should be managed in a manner that allows designated MFA Information Resources personnel to promptly access all data.
- MFA Information Resources **Information Resources** are provided to facilitate company business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using MFA Information Resources **Information Resources**.

- Personnel should not intentionally access, create, store, or transmit material which MFA Information Resources may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "need to know".
- Personnel are permitted to use only those network and host addresses issued to them by MFA Information Resources IT and should not attempt to access any data or programs contained on MFA Information Resources systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal MFA Information Resources networks and/or environments must be made through approved, and MFA Information Resources-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their (personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Access cards and/or keys that are no longer required must be returned to physical security personnel.
- Lost or stolen access cards, security tokens, and/or keys must be reported to physical security personnel as soon as possible.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following MFA Information Resources rules:
    - Must meet all requirements including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone. MFA Information Resources support personnel and/or contractors should never ask for user account passwords.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.

- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with MFA Information Resources, if issued.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing **confidential information** should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access **confidential information** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing **confidential information** should be immediately removed from printers and fax machines.

Data Security

- Personnel should use approved encrypted communication methods whenever sending **confidential information** over public computer networks (Internet).
- **Confidential information** transmitted via USPS or other mail service must be secured in compliance with the Information Classification and Management Policy.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- **Confidential information** must be transported either by an MFA Information Resources employee or a courier approved by IT Management.
- All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.

Email and Electronic Communication

- Auto-forwarding electronic messages outside the MFA Information Resources internal systems is prohibited.
- Electronic communications should not misrepresent the originator or MFA Information Resources.

- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from MFA Information Resources IT, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive MFA Information Resources **confidential information**.
- Any personal use of MFA Information Resources provided email should not:
    - Involve solicitation.
    - Be associated with any political entity, excluding the MFA Information Resources sponsored PAC.
    - Have the potential to harm the reputation of MFA Information Resources.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of MFA Information Resources **confidential information**.
    - Or otherwise violate any other MFA Information Resources policies.
- Personnel should only send **confidential information** using approved secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing **confidential** or **internal information** in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to MFA Information Resources networks.
- Software installed on MFA Information Resources equipment must be approved by IT Management and installed by MFA Information Resources IT personnel.
- All MFA Information Resources assets taken off-site should be physically secured at all times.
- Personnel traveling to a High-Risk location, as defined by FBI and Office of Foreign Asset control, must contact IT for approval to travel with corporate assets.
- Employees should not allow family members or other non-employees to access MFA Information Resources **Information Resources**.

Internet

- The Internet must not be used to communicate MFA Information Resources **confidential** or **internal information**, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with MFA Information Resources networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
    - Recreational games,
    - Streaming media,
    - Personal social media,

  - Accessing or distributing pornographic or sexually oriented materials,
  - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
  - Or otherwise violate any other MFA Information Resources policies.
- Access to the Internet from outside the MFA Information Resources network using a MFA Information Resources owned computer must adhere to all of the same policies that apply to use from within MFA Information Resources facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- MFA Information Resources does not allow **personally owned mobile devices** to connect to the MFA Information Resources corporate internal network.
  OR
- The use of a **personally owned mobile device** to connect to the MFA Information Resources network is a privilege granted to employees only upon formal approval of IT Management.
- All **personally owned** laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access MFA Information Resources email must have a PIN or other authentication mechanism enabled.
- **Confidential information** should only be stored on devices that are encrypted in compliance with the MFA Information Resources Encryption Standard.
- MFA Information Resources **confidential information** should not be stored on any personally owned **mobile device**.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to the MFA Information Resources Security Team immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- **Jail-broken** or rooted devices should not be used to connect to MFA Information Resources **Information Resources**.
- MFA Information Resources IT Management may choose to execute "**remote wipe**" capabilities for **mobile devices** without warning (see Mobile Device Email Acknowledgement).
- In the event that there is a suspected **incident** or breach associated with a **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to MFA Information Resources **Information Resources** may be monitored, at the discretion of MFA Information Resources IT Management.
- MFA Information Resources IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. MFA Information Resources IT support may not assist in troubleshooting device usability issues.
- Use of **personally owned** devices must be in compliance with all other MFA Information Resources policies.
- MFA Information Resources reserves the right to revoke **personally owned mobile device** use privileges if personnel do not abide by the requirements set forth in this policy.

- Texting or emailing while driving is not permitted while on company time or using MFA Information Resources. Only hands-free talking while driving is permitted, while on company time or when using MFA Information Resources.

Physical Security

- Photographic, video, audio, or other recording equipment, such as cameras and cameras in **mobile devices**, is not allowed in secure areas.
- Personnel must display photo ID access card at all times while in the building.
- Personnel must badge in and out of access-controlled areas. Piggy-backing, tailgating, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
- Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on MFA Information Resources **Information Resources** are not private and may be accessed by MFA Information Resources IT employees at any time, under the direction of MFA Information Resources executive management and/or Human Resources, without knowledge of the user or resource owner.
- MFA Information Resources may log, review, and otherwise utilize any information stored on or passing through its **Information Resource** systems.
- Systems Administrators, MFA Information Resources IT, and other authorized MFA Information Resources personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

Removable Media

- The use of **removable media** for storage of MFA Information Resources information must be supported by a reasonable business case.
- All **removable media** use must be approved by MFA Information Resources IT prior to use.
- **Personally, owned removable media** use is not permitted for storage of MFA Information Resources information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the MFA Information Resources IT.
- Confidential and internal MFA Information Resources information should not be stored on **removable media** without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a **removable media** device that may have contained any MFA Information Resources information must be reported to the MFA Information Resources IT.

Security Training and Awareness

- All new personnel must complete an approved **security awareness** training class prior to, or at least within 30 days of, being granted access to any MFA Information Resources **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the MFA Information Resources Information Security Policies before they are granted to access to MFA Information Resources **Information Resources**.
- All personnel must complete the annual security awareness training.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable MFA Information Resources policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent MFA Information Resources, including accounts that could reasonably be assumed to be an official MFA Information Resources account, requires the permission of the MFA Information Resources Communications Departments.
- When discussing MFA Information Resources or MFA Information Resources -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an MFA Information Resources representative, and
    - Make it clear that you are speaking for yourself and not on behalf of MFA Information Resources, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at MFA Information Resources.
- When publishing MFA Information Resources-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; "The opinions and content are my own and do not necessarily represent MFA Information Resources's position or opinion."
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with MFA Information Resources will not be tolerated.
- **Confidential information**, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on MFA Information Resources social media sites must follow the MFA Information Resources Social Media Management Procedures.

VoiceMail

- Personnel should use discretion in disclosing **confidential** or **internal information** in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.

- Personnel should not access another user's voicemail account unless it has been explicitly authorized.
- Personnel must not disclose **confidential** information in voicemail messages.

Incidental Use

- As a convenience to MFA Information Resources personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:
    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to MFA Information Resources approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to MFA Information Resources.
    - Incidental use should not interfere with the normal performance of an employee's work duties.
    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, MFA Information Resources or its customers.
- Storage of personal email messages, voice messages, files and documents within MFA Information Resources **Information Resources** must be nominal
- All information located on MFA Information Resources **Information Resources** are owned by MFA Information Resources may be subject to open records requests and may be accessed in accordance with this policy.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 6, 7, 8, 9, 11, 12, 13, 16, 18
- NIST CSF: PR.AC, PR.AT, PR.DS, DE.CM, DE.DP, RS.CO
- Asset Management Policy
- Encryption Management Policy
- Encryption Standard
- Identity and Access Management Policy
- Incident Management Policy
- Information Classification and Management Policy
- Mobile Device Acknowledgement
- Personnel Security and Awareness Policy
- Physical Security Policy
- Social Media Management Procedure

Waivers

Waivers from certain policy provisions may be sought following the MFA Information Resources Waiver Process.

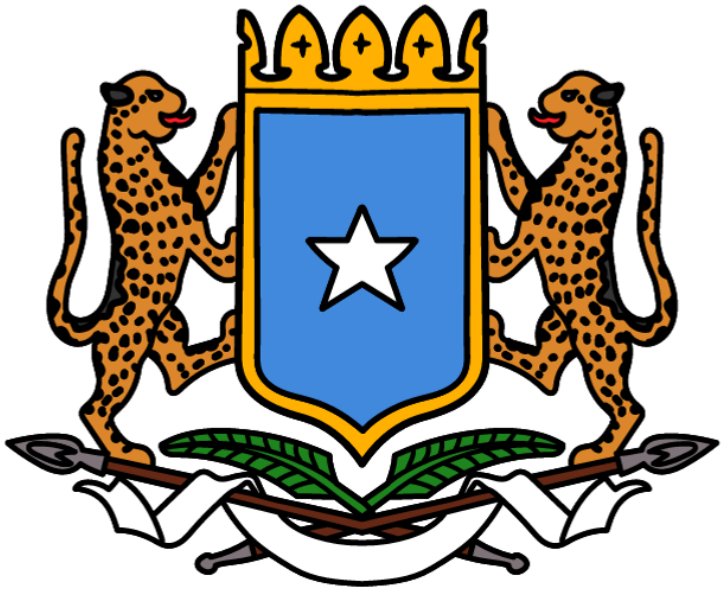
Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	August 2023			Document Origination



Ministry of Foreign Affairs & International Cooperation
Federal Republic of Somalia