Cybersecurity Policy for Acceptable Use

Sharing	WHITE
Classification	PUBLIC
Number	VM.PD - CSD - 001 - CPP
Status	FINAL
Version	5.0
Date	06/03/2024
Pages	15
Owner	Cybersecurity General Department
File Name	CYBERSECURITY POLICY FOR ACCEPTABLE USE

Sharing & Classification

Sharing	**White**: No sharing restrictions and the information can be published on public channels.
Classification	**Public**: Data shall be classified as “Public” if unauthorized access to or disclosure of such data has no impact.

Revision History

Version	Date	Author	Summary of Changes
1.0	03/03/2020	Cybersecurity General Department	Developed Structure and Detailed Policy Statement
1.1	18/03/2020	Cybersecurity General Department	1. Amended the wording of the initially developed policy 2. Applied comments received from Cybersecurity General Manager
1.2	25/03/2020	Cybersecurity General Department	Updated email details under section 9
2.0	25/06/2020	Cybersecurity General Department	Final Version (June 2020)
2.1	21/10/2020	Cybersecurity General Department	Pre- Publishing Review
3.0	29/12/2021	Cybersecurity General Department	Annual review and adding controls according to the requirements of the National Cybersecurity Authority
3.1	27/01/2022	Cybersecurity General Department	Reflecting stakeholders’ comments
4.0	08/02/2023	Cybersecurity General Department	Annual review and adding controls according to the requirements of the National Cybersecurity Authority and Diwan Letter
5.0	30/01/2024	Cybersecurity General Department	No part has been modified

Distribution

Name and Title	Channel
Deputy Minister for E-Health and Digital Transformation	Email
Legal Affairs General Department	Email
Deputy Minister for Human Resource	Email/Intranet
Deputy Minister for Planning & Transformation	Email

Policy Record	
Issue Number	
Modification Comments	
Date of Last Update	

Policy Title	Policy Number	Policy Issuer	Replacement of Policy Number
Cybersecurity Policy for Acceptable Use	VM.PD - CSD - 001- CPP	Cybersecurity General Department	VM.PD - CSD - 001- CPP
Policy Classification	**Date of Approval**	**Date of Implementation**	**Date of Next Revision**
■ **Corporate Policy**	10 -August-2020	03-Novermber-2020	12 –February-2025

1. Purpose

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of MoH. Therefore, this policy sets the acceptable use of Information resources and/or assets at MoH. These rules are in place to protect the user (employee, contractor,etc.) and MoH. Inappropriate use might expose MoH to risks including virus attacks, compromise of network systems and services, and legal liabilities.

2. Scope

The scope of this policy covers information resources and/or assets at MoH and applies to all types of defined users.

3. Definitions

Unless specifically defined below, definitions of the terms used in this document are consistent with National Cybersecurity Authority (NCA) and International Organization for Standardization (ISO).

- **Business Owner:** MoH employee or organizational unit that have primary responsibility for the information within a given system.
- **Technical Owner:** MoH technical employee or organizational unit given the responsibility for the technical development and maintenance of a given system.
- **User or Staff:** MoH employees includes line managers, deputy-ministers and work branches, third parties, contractors, partners, and service providers who have access to MoH information and information processing facilities.

4. Policy Content

4.1 Roles and Responsibilities

The roles and responsibilities concerning this policy are as follows:

- **Cybersecurity Advisory Board**
  - Final decisive body in case of this policy interpretation;
  - Review and approve the policy;
  - Review key violations instances against the policy.
- **Cybersecurity General Department**
  - Owning, maintaining, and communicating the policy to the intendent audience;
  - Managing policy exceptions and violations;
  - Ensuring policy compliance within MoH..
- **Users or Staff**
  - Complies with the Policy.

4.2 Acceptable Use

The objective of this section is to highlight user responsibilities towards the use of MoH information resources/assets.

4.2.1 MoH information assets are provided to the user for job related purpose and necessary system privileges are granted only where there is a legitimate business need.

4.2.2 MoH does not allow the use of its business-related information and technology assets for personal use, including repositories for personal data.

4.2.3 User should not share his/her account details with any person.

4.2.4 User is responsible to protect the confidentiality of MoH information and technology assets as per existing cybersecurity policies and requirements.

4.2.5 User will only access and use systems that are specifically authorized to him/her.

4.2.6 User should not disable any services, devices, antivirus software or security firewall protection on any of MoH technology assets and the workstations assigned to him/her.

4.2.7 User should not store, process, or transmit pornographic material into any of MoH information systems environment.

4.2.8 User should not copy or exchange any classified information in any manner, including but not limited to CD, USB drive, email attachment, etc. unless it is authorized for official purposes.

4.2.9 User should not take photos of processed information, including health records, using cameras or cameras in mobile phones without appropriate approval.

4.2.10 Any computer software which was developed by MoH staff within the scope of their employment remains the ‘Intellectual Property’ of MoH.

4.2.11 MoH reserves the right to perform a compliance review on a periodic basis to ensure compliance with this policy.

4.2.12 User shall use cross-shredding devices, to securely dispose documents, that contain data classified as “Secret” or “Top Secret”, when no longer needed.

4.3 Internet Usage

The objective of this section is to highlight user responsibilities while using the internet onto MoH information assets.

4.3.1 User shall use the internet access only to conduct business related activities within MoH in an efficient and convenient manner.

4.3.2 User should not connect any MoH device/information asset to an internet source without obtaining necessary approval from Cybersecurity General Department.

4.3.3 All information assets and equipment are owned by MoH. Hence, MoH Cybersecurity General Department may install software or hardware to monitor, record and protect all information and technology assets usage by the user, including email and web site visits, and reserves the right to record or inspect files stored on its systems and assets.

4.3.4 User must respect the audience and should not use, upload, post, share, forward, browse, and download content with ethnic slurs, discriminatory remarks, personal insults, obscenity, and political / religious passion or engage in any similar conduct that would not be appropriate or acceptable by MoH principles.

4.3.5 MoH reserves the right to configure web browsers to leave ‘footprints’ (or cookies) providing a trail of all sites visited by users.

4.3.6 MoH reserves the right to examine:

- Web browser cache files;
- Web browser bookmarks and cookies;
- Temp folders;
- Download folders;
- Logs of web sites visited.

4.3.7 MoH reserves the right to examine corresponding related logs to test user’s compliance against internal policies and assist MoH with internal investigations, if required at a later stage.

4.3.8 User should use only approved and designated software to access the World Wide Web (WWW) in order to ensure all approved security patches are incorporated.

4.3.9 User should not download or install any add-on software and scripts such as ActiveX control or Java scripts that any website may require, he/she visits, and in case his/her work requires this web site add-ons, user shall request support from IT Helpdesk.

4.3.10 User should neither store nor process sensitive, confidential or private information or documents on systems connected to the internet unless the user has a documented approval from MoH Cybersecurity General Department. Furthermore, MoH reserves the right to protect its information rights.

4.3.11 User should sign an agreement by personnel pledging to not use social media, communication applications, or personal cloud storage to create, store or share MoH's data, that is classified as "Secret" or "Top Secret" in the first stage of user's functional relationship with the Ministry and until the end of the functional relationship, with the exception of secure communication applications approved by relevant authorities.

4.3.12 User should obtain necessary approval from MoH Public Relations Department (Appointed speaker), prior to posting any relative information or documentation that was never published about MoH on the Internet and Social Media.

4.3.13 User should not release MoH business related information including but not limited to electronic protected health information, contracts, purchase orders, until the identity and authenticity of the requested individual and/or organization are verified.

4.3.14 User should carefully determine the source of the information obtained via the Internet is to ensure its trustworthy.

4.3.15 User should not hinder or prevent automatic scanning of all the files downloaded over the Internet for viruses, using approved virus detection software.

4.3.16 MoH strictly enforces and adheres to software vendor's license agreements as defined in MoH Cybersecurity Policy of Software Security. Hence, the User should not copy unauthorized software such as shareware, freeware from the Internet, that is not consistent with the vendor's license or unless the user has a documented approval from Cybersecurity General Department.

4.3.17 User should immediately notify via the established incident reporting channel if sensitive, confidential, and/or private information is suspected to be lost or disclosed to unauthorized parties.

4.3.18 User should not perform any kind of security scanning, testing, possessing or using tools for cracking software license, passwords and similar activities.

4.3.19 User should pay attention to security warnings that might appear during browsing and treat every message with caution.

4.4 Usage of Social Media

The objective of this section is to highlight user responsibilities towards the use of social Media.

4.4.1 MoH employees are brand ambassadors of the Ministry and shall be responsible for the content they publish over social media. The content posted by employees in their personal capacity may be viewed as representing MoH point of view. Therefore, user should use good judgement when engaging with social media.

4.4.2 User will ensure that his/her profile and related content is consistent with MoH code of conduct and policies while engaging with MoH on social media.

4.4.3 Social media are considered public forums, therefore, User should not perform any of the following:

- Disclose any confidential, personal, private information.
- Post material that is, or might be perceived as threatening, harassing, bullying or discriminatory towards another employee, contractor, applicant, beneficiary of MoH etc..
- Post videos and/or images of other employees, contractors, applicants, beneficiaries of MoH etc., unless formally authorized.
- Post any material that might cause harm or damage to MoH or state reputation.

4.4.4 Personal posts on social media shall not be related in any way (e.g. directly, indirectly, linkable or associated) to the non-public knowledge, gained due to the work in or services rendered for MoH.

4.4.5 User should pay special attention when using social media, not to reveal, suggest or give any impression on author’s or anyone’s else scope of duties within MoH, level of clearance or details of area of responsibility.

4.4.6 All employees working on critical jobs or systems shall not disclose their jobs and duties on social media.

4.4.7 Personal posting of any content type (e.g., audio, video, location, and any type of material) captured inside MoH facilities and events is strictly forbidden.

4.4.8 Personal usage of social media, public conferences or other internet services via official MoH accounts is strictly forbidden unless a documented approval is obtained from MoH representatives.

4.5 Physical Security

The objective of this section is to highlight user responsibilities towards MoH physical security controls.

4.5.1 User should always display his/her identity card within MoH premises in a visible manner.

4.5.2 User should not allow tailgating at MoH and he/she should be vigilant about that.

4.5.3 It is everyone’s interest to ensure that the physical access controls to MoH premises operate effectively. User shall cooperate and comply with MoH physical security measures.

4.5.4 Access to computer rooms and any other restricted areas shall be controlled and user should adhere to such controls at all times.

4.5.5 Unauthorized personnel are not allowed to gain access into MoH premises or use MoH technology assets. Hence, User should adhere to such access control measures and must not support/help in such violations.

4.5.6 MoH Information and technology assets shall not be moved out of MoH premises without appropriate approval from MoH appropriate level of management and/or owner.

4.5.7 The user should not bring unauthorized Information processing devices, such as: computer systems or Internet modems, within MoH premises or connect such devices to the MoH network without justifying the business need and obtaining a documented approval from the Cybersecurity General Department.

4.6 Desktop, Laptop and Portable Device Security

The objective of this section is to highlight user responsibilities towards the use of MoH desktop, laptop, and portable devices.

4.6.1 User is only authorized to access the allocated desktop and laptops within dedicated locations. User should not access other desktop and laptops located within MoH premises without prior approval.

4.6.2 User should lock his/her session at a short beak or log off the system before leaving the office and/or at the end of each day.

4.6.3 User should secure, store and destroy sensitive information and he/she shall not leave it on his/her desk where it can be read, copied or altered without user’s knowledge.

4.6.4 User should not install new hardware onto desktop computers without appropriate authorization from Technical owner.

4.6.5 User should not install or use illegal and/or pirated software on his/her device provided by MoH.

4.6.6 User shall only use equipment owned and authorized by MoH for business and operations.

4.6.7 Gaming software is not permitted for being used on MoH systems and network. User should not attempt to install, transfer or use any gaming software within MoH network.

4.6.8 User should immediately report the loss of his/her laptop, notebook or PDAs to Physical Security

4.6.9 While using the laptop provided by MoH, the user should ensure that any data stored on the local disk is regularly copied to the central file server for backing up. He/she shall report to IT helpdesk in case of error.

4.6.10 Laptops shall be carried as hand luggage to prevent damage and unauthorized access when travelling.

4.6.11 User should not leave his/her devices containing restricted business information unprotected or unattained in visible places (e.g. in the car's chair).

4.6.12 During teleworking user should ensure that information processed will be protected from access of unauthorized people. User should use screen privacy filters to avoid shoulder surfing.

4.7 Personally Owned Mobile Devices

The objective of this section is to highlight user responsibilities towards the usage of his/her personally owned mobile devices that processes or stores MoH related business information.

4.7.1 User should enable auto-lock feature on his/her device. (This may correspond to screen timeout setting.)

4.7.2 User should avoid using auto-complete features that remember usernames or passwords.

4.7.3 Employee personal device usage for daily work need to be Controlled and restricted based on job requirements.

4.7.4 If necessary, MoH reserves the right to remotely erase mobile devices provided by the Ministry or delete the Ministry's data on users' personal mobile devices.

4.7.5 User should disable Bluetooth "if not needed". (This will help prolong battery life and provide better security).

4.7.6 User should keep his/her mobile device and applications on the device up to date. User should use automatic update options if available.

4.7.7 User should install an antivirus or security program and configure it to scan and update automatically.

4.7.8 User should take appropriate physical security measures to prevent theft of his/her mobile devices.

4.7.9 User should not leave his/her mobile device unattended in a public area.

4.7.10 User should ensure that MoH data and information stored on his mobile device are logically separated from his personal files and encrypted as per MoH Cybersecurity Policy for Cryptographic.

4.7.11 User should immediately change his/her passwords if he/she loses her/his mobile device. User should immediately report it to MoH Cybersecurity General Department as well.

4.7.12 User should be aware regarding mobile telecom operator's and MoH cybersecurity policies (if applicable) on lost and/or stolen devices.

4.7.13 User should be familiar the steps required to take if he/she lost his/her device in addition to communicating the incident to MoH relevant personnel.

4.7.14 User should report the case to his/her Telcom network carrier as soon as possible, so that they can deactivate the device if required.

4.8 Computer Malware

The objective of this section is to highlight user responsibilities to mitigate computer malware risks within MoH network.

4.8.1 User should not open attachments from unidentifiable or suspicious sources.

4.8.2 User should not alter or disable anti-virus scan and settings.

4.8.3 User should treat emails from unknown sources as suspicious and report them to MoH Cybersecurity General Department. Similarly, regarding emails from known sources, but containing unusual, not standard requests.

4.8.4 User should immediately contact MoH Cybersecurity General Department if he/she suspect or become aware of a computer virus or malware.

4.9 Password Security

The objective of this section is to highlight user responsibilities towards managing his passwords within MoH.

4.9.1 User should not share his/her passwords with anyone.

4.9.2 User should not write down his/her passwords or any media type whether physically or electronically.

4.9.3 User should use a reasonably complex password where possible and follow relevant password controls in compliance with MoH Cybersecurity Policy for Access Control.

4.10 Email and Communications Activates

The objective of this section is to highlight user responsibilities towards email usage and communication activities within MoH.

4.10.1 MoH email system is made available primarily for work related use. User should use the email in a responsible manner and according to MoH Cybersecurity Policy for Communications Security.

4.10.2 User should not share or exchange information/data in form of files and documents that may cause legal liability or harm the reputation of MoH.

4.10.3 User should not use his/her personal emails for work related activities.

4.10.4 User should not use his/her business email provided by MoH email system for any personal use including but not limited to registering on public websites, internet services, social platforms,etc.

4.10.5 User should not send e-mails that contain offensive content (including offensive comments about gender, sexual orientation, pornography, etc.).

4.10.6 User should make proper arrangements when he/she goes on leave, including assigning a corresponding person to receive incoming emails and take authorized actions if required in accordance with respective business roles

4.10.7 User shall configure Out of Office (OoO) message while on vacation or leave. However, I acknowledge that the same shall be practiced with caution. Excess of information about one's absence can be misused by outsiders. Complete information (like returning date, phone number, etc.) shall be sent ONLY within the MoH (internal) domain. However, name and e-mail address of point of contact details can be sent to outside of MoH domain.

4.10.8 User shall promptly report all suspected security vulnerabilities or problems that he/she noticed through email to Cybersecurity General Department.

4.10.9 User shall follow and obey information classification tagging while sharing MoH business related information/data internally or externally.

4.10.10 MoH management has the authority to intercept, disclose, or assist in intercepting or disclosing email communication.

4.10.11 User should not use MoH systems to produce or distribute chain emails.

4.10.12 User should not forward or divert emails from MoH business email account to any non-MoH users email accounts.

4.11 Document Security

The objective of this section is to highlight user responsibilities towards the usage of MoH documents in a secure manner.

4.11.1 User will be responsible to take all measures as per his/her business functional role and capacity to protect document from unauthorized disclosure.

4.11.2 User should immediately collect and shred adequately his/her unused or no longer needed printouts and photocopies from printers and photocopiers.

4.11.3 User should adopt Cybersecurity Policy for Clean Desk and Screen for papers, documents and classified documents in order to reduce the risk of unauthorized access, loss of and damage to information outside business hours.

4.11.4 User should tag, label and deal with all documents containing sensitive information, as per Cybersecurity Policy for Asset Management.

4.11.5 User should follow MoH Asset Disposal Procedure to dispose documents containing confidential information that reach its retention period.

4.11.6 User should display "whenever possible" warning notices on the fax coversheets to the effect that the message is meant for the recipient only and the use of the message by any other party will be deemed unauthorized or illegal.

4.12 Incident Reporting

The objective of this section is to highlight user responsibilities towards incident reporting within MoH.

4.12.1 All MoH users including employees, third parties, and contracts are responsible to notify MoH Cybersecurity Contacts immediately of any evidence or suspicion of any security violation with regard to:

- Unauthorized access to network, telecommunications, or computer systems;
- The apparent presence of a virus on a PC;
- Apparent tampering with any file for which the user established restrictive discretionary access controls;
- Violation of this Policy or any other cybersecurity policy, or procedure by another user, employee, contractor or third-party service provider;
- MoH users shall report incidents through the appropriate channels as soon as possible. Failure to report an incident may result in adverse impact on MoH information systems and data;
- All security incidents shall be documented where possible. Users shall gather as much details as possible and provide this in their report.

4.13 Exceptions

4.13.1 If a waiver to this Policy is required without a viable and secure alternative, then the requester shall duly fill, sign, and submit the Exception Request Form to Cybersecurity General Department.

4.13.2 The requester shall include in the request a detailed description of the scope, business justification, and time period.

4.13.3 Cybersecurity General Department shall review the request, identify the risk and compensating controls in accordance with MoH risk management framework, and may require the requester to consent on the identified risks and compensating controls. Furthermore, Cybersecurity General Department may consult internal related legal, and internal and external regulatory bodies.

4.13.4 The requester shall implement the exception after approval is obtained from the Cybersecurity General Manager.

4.13.5 Cybersecurity General Department shall monitor approved exceptions and revoke them after expiration.

4.14 Compliance

4.14.1 Compliance with MoH cybersecurity policies and associated controls is mandatory on MoH business missions, staff members, contractors, partners, and services providers who have access to MoH information and information processing facilities.

4.14.2 MoH line managers shall exercise due diligence to ensure compliance through continuous enforcement and self-assessment within their area of responsibility.

4.14.3 Compliance assessments shall be regularly and independently performed by Cybersecurity General Department to measure, analyze, and evaluate MoH adherence to Cybersecurity policies and associated security controls. Cybersecurity General Department shall monitor MoH compliance and oversee the implementation of corrective actions by their respective owners.

4.15 Violations

4.15.1 Cybersecurity General Department is responsible for technical verification of violations, and Legal Department shall proceed with official disciplinary and legal actions as required.

4.15.2 Disciplinary actions shall be consistent with the severity of the violation, as determined by the investigation, and stipulated by the relevant regulations and laws.

4.16 Policy Review

4.16.1 Cybersecurity General Department shall conduct annual review and update of this document, and shall assure constant alignment with changes to requirements, best practices, regulations, and obligations.

4.16.2 If a change to this policy is required, then the requester shall duly fill, sign, and submit the Security Document Change Request Form to Cybersecurity General Department.

4.17 Communication

4.17.1 Enquiry, feedback, and incidents related to this policy can be communicated to Cybersecurity General Department through any of the following channels:

- Enquiry and feedback can be sent through email to **CS-Policies@moh.gov.sa**
- Incidents can be reported by email to **CS-IR@moh.gov.sa**

5. Procedures

Does not require.

6. KPIs

Review the National Cybersecurity Authority (NCA) publications and ensure that it is included in the policy.

7. References

7.1 Government legislation references:

- Controls for the usage of Information and Communication Technologies;
- Essential Cybersecurity Controls;
- Critical Systems Cybersecurity Controls
- Anti-Cyber Crime Law.

7.2 International references:

- ISO/IEC 27001;
- ISO/IEC 27002.

7.3 Internal References:

- Cybersecurity Policy for Access Control;

- Cybersecurity Policy for Physical and Environmental Security;
- Cybersecurity Policy for Incident Response;
- Technology Asset Lifecycle Management;
- Naming Convention Standard;
- Information Classification and Labelling Standard;
- Asset Management Standard;
- Removable Media Management Standard;
- Asset Disposal Procedure;
- Cybersecurity Human Resource Procedure.

8. Appendix

8.1 Government legislation references:

- Controls for the usage of Information and Communication Technologies;
- Essential Cybersecurity Controls;
- Critical Systems Cybersecurity Controls;
- Anti-Cyber Crime Law.

Policy Title	Policy Number	Policy Issuer	Replacement of Policy Number
Cybersecurity Policy for Acceptable Use	VM.PD - CSD - 001- CPP	Cybersecurity General Department	VM.PD - CSD - 001- CPP
Policy Classification	**Date of Approval**	**Date of Implementation**	**Date of Next Revision**
■ **Corporate Policy**	10 -August-2020	11-Novermber-2020	12 –February-2025

Preparation			
Name	Position	Signature	Date
Basem Abdullah AlAngari	General Manager of Cybersecurity General Department		11-February-2024
Reviewer			
Name	Position	Signature	Date
Suzan Assad Rasheed	General Manager of Institutional excellence		11-February-2024
Fahad Alghewenim	General Manager of Legal Affairs		12- February -2024
Approval			
Name	Position	Signature	Date
Cybersecurity Advisory Board	Cybersecurity Advisory Board		05-March-2024