وزارة الصحة
Ministry of Health

Cybersecurity Policy for IP and Copyright Compliance

Sharing	WHITE
Classification	PUBLIC
Number	VM.PD - CSD - 025 - CPP
Status	FINAL
Version	5.0
Date	06/03/2024
Pages	12
Owner	Cybersecurity General Department
File Name	CYBERSECURITY POLICY FOR IP AND COPYRIGHT COMPLIANCE

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	Initial draft
1.1	06/03/2024	Cybersecurity General Department	1. Reflecting stakeholders' comments
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
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
Innovation Center	Email

Policy Record	
Issue Number	
Modification Comments	
Date of Last Update	

Policy Title	Policy Number	Policy Issuer	Replacement of Policy Number
Cybersecurity Policy for IP and Copyright Compliance	VM.PD - CSD - 025- CPP	Cybersecurity General Department	VM.PD - CSD - 025- CPP
Policy Classification	**Date of Approval**	**Date of Implementation**	**Date of Next Revision**
[redacted]Corporate Policy	10 -August-2020	03-Novermber-2020	12 –February-2025

1. Purpose

In creating and maintaining the Cybersecurity Management System (CSMS), it is essential to understand the various IP and copyright requirements that apply to MoH and its entities. IP and copyrights compliance checks should be conducted to ensure that MoH continues to meet its obligations and avoid exposure to the risk of Intellectual Property (IP) criminal prosecution or liability.

The purpose of this Policy is to set out compliance requirements for licensing software, intellectual property and copyright.

2. Scope

The scope of this policy covers MoH both original and acquired material and software used on technical and non-technical assets, and applied 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.
- **Copyright:** It is a legal term that describes the rights granted to innovators in respect of their literary and artistic works and covers a wide range of books, music, oil paintings, computer sculptures, databases, advertisements, geographical maps and technical drawings. Copyright is obtained automatically without registration and generally apply for 50 years after the creator's death.

- **Industrial Design:** Is a collection of two-dimensional lines or colors, or a three-dimensional form that gives any industrial product or product of traditional crafts a special appearance, provided that it is not merely for a functional or technical purpose, including textile designs. The industrial design is protected by a protection document called “industrial design certificate”.
- **Integrated Circuit:** An integrated circuit is a product in its final or intermediate form in which the elements, at least one of which is active and some or all of the interconnections are integrally formed in or on a piece of material and the purpose of this is to perform an electronic function.
- **Patent:** patents provide protection for inventions and are generally granted for 20 years. They must be applied for and granted in individual countries and can be sold or licensed to others.
- **Technical Owner:** MoH technical employee or organizational unit given the responsibility for the technical development and maintenance of a given system.
- **Trademark:** A trademark is a sign or symbol that is associated with a particular individual or organization and has been registered as such. When registered, MoH can claim the exclusive right to use that symbol and can prevent others from doing so through the courts. The term of a trademark is 10 years with possibility of extension.
- **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 (CSAB)**
  - Final decisive body in case of this Policy interpretation;
  - Monitors exceptions and violations;
  - Accepts key exceptions;
  - Provide areas of improvements and insights to be considered in the policy.
- **Cybersecurity General Department**
  - Ensures policy implementation and compliance;
  - Reviews and accepts exceptions and violations;
  - Escalates exceptions and violations considered as key to Cybersecurity Advisory Board;
  - Reviewing MoH usage of software to ensure correct licensing.
- **Users or Staff**
  - Complies with the Policy.
  - Ensuring compliant usage with IP copyright terms.

4.2 General

4.2.1 Prior to using any software, MoH shall obtain the necessary licenses or acquisition of IP rights based on sizing and identifying its business and operational requirements.

4.2.2 The software owner and MoH shall ensure that all usage activities with regard to the IP are compliant with their licenses and copyright terms or other terms on using and/or disposing such IP.

4.2.3 Employees shall be made aware of the following:

- MoH IP, that needs to be protected from infringement;
- Legal requirements for protecting IP and the implications of breaching them.

4.2.4 Employees shall use software received from approved and legal sources only, in compliance with manufacturer requirements and guidelines, and MoH Cybersecurity Policy of Acceptable Use and Cybersecurity Policy of Software Security.

4.2.5 All employees are required to report any non-compliance with intellectual property rights that they are aware of, in accordance with MoH Cybersecurity Policy of Incidents Response.

4.2.6 The software is obtained from a source licensed by the copyright holder. It is always necessary to obtain and maintain proof of purchase.

4.2.7 MoH is required to obtain software approval details including:

- Type of license (e.g. general, lenient, modifiable rights, etc.);
- The date of purchase;
- The expiry date of the license;
- Scope of licensed use (number of users, workstations, accounts, bandwidth, etc.);
- License keys.

4.2.8 MoH shall retain the following for legal purposes:

- Receipt of the purchase;
- License agreement;
- Acceptance or receipt;
- Evidence of payment of license fees.

4.2.9 The technical authority responsible for open source software in the MoH ensures that all user activities related to free and open source software comply with the provisions of their licenses. In the event that there are any doubts regarding the legitimate use of this software, the technical official must clarify all doubts, and seek possible support from the legal or other department if necessary.

4.2.10 The installation and use of software on the MoH systems is subject to regular monitoring (for example annually) to ensure that it complies with the requirements of this policy.

4.2.11 The process of acquiring the software should be consistent with MoH Cybersecurity Policy of System and Application Acquisition, Development and Maintenance.

4.3 Proprietary Software License

The objective of this section is to ensure that MoH is granted the permission it needs to use the software under the End User Licensing Agreement (EULA) and is compliant with it.

4.3.1 MoH shall obtain the license (a right to use) or shall acquire necessary IP right to the proprietary software:

- Directly from the copyright;
- Other IP right holder;
- Through an authorized reseller.

4.4 Obtaining Software

The objective of this section is to ensure that MoH usage of any software other than proprietary one, including free or open-source software, is compliant with its license.

4.4.1 All software used within MoH shall comply with Cybersecurity Policy of Software Security and shall be on the approved software list.

4.4.2 Software shall only be obtained from a source authorized by the copyright holder. Purchase evidence shall always be obtained and preserved.

4.4.3 MoH shall obtain the details of software approval, that includes:

- Type of license (e.g. public, permissive, copyleft, etc.);
- Date of purchase;
- License expiry date;
- The scope of usage licensed licenses (number of users, workstations, accounts, bandwidth etc.);
- License keys.

4.4.4 MoH shall keep, for the legal purposes:

- Purchase receipt;
- License agreement;
- Receipt of acceptance or delivery;
- Royalties' payment evidences.

4.4.5 MoH technical owner of the open-source software shall ensure that all user activities concerning free and open-source software are compliant with the terms of its license. In case of any doubts towards legitimate use of this software, it is the Technical Owner to clarify all the doubts, getting possible support of e.g. Legal or other Departments, if necessary.

4.4.6 Installation and use of software on MoH systems shall be a subject to regular monitoring (e.g. annual) to ensure compliance with this Policy's requirements.

4.4.7 Obtaining software shall be conducted in line with MoH Cybersecurity Policy for System and Application Acquisition, Development and Maintenance.

4.5 Re-using Licenses

The objective of this section is to ensure full utilization of the software license.

4.5.1 If a user no longer requires a license (e.g., due to employment termination or reassignment) the license of the software shall be reused if permissible under license terms and, where applicable, the software shall be redeployed to a new user.

4.6 Software Licensing Compliance Reviews

The objective of this section is to ensure that all software in use is correctly licensed for MoH.

4.6.1 Cybersecurity General Department shall regularly review (e.g. annually) installed software against recorded licenses to ensure that all the software in use within MoH is correctly licensed and used in accordance with relevant license terms.

4.6.2 The review report shall highlight:

- Licenses with close expiry date;
- Opportunities for license re-use;
- Requirements for additional licenses to be purchased.

4.6.3 If a license could not be obtained within a reasonable time, then the unlicensed software shall be immediately removed from MoH IT infrastructure.

4.7 Other types of IP

The objective of this section is to ensure MoH compliance with other types of IP copyrights.

4.7.1 MoH shall ensure that copyrights are understood and not infringed by the employees. IP may be included in:

- Training videos;
- Audio played in works locations and offices;
- Books;
- Courses;
- Procedural documentation;
- Manuals;
- Product documentation;
- Presentations;
- Photographs used on presentations, internal mail, intranet and websites;
- Logos on marketing materials;

- Etc.

4.7.2 If the employees have any doubts about compliance with the right to use IP, they should confirm it with IP business or technical owner and - if necessary – with Legal Affairs Department.

4.7.3 If the license (the right to use) does not cover the need, then a clearance shall be obtained from the copyright holder in a legally acceptable format and kept in a safe location. This clearance shall include the format of the medium involved and the distribution intended (e.g., public or internal within MoH).

4.8 Protecting MoH Intellectual Property

The objective of this section is to protect MoH IP copyrights.

4.8.1 IP rights for MoH materials shall be defined, established and carried out as part of its business process (e.g. submitting an application for patents to SAIP).

4.8.2 MoH should protect its identity from impersonation by using brand protection service.

4.8.3 Employees generating material out of the formal business processes, shall take into consideration the following requirements:

- Ensure that a claim to copyright is included on all works that are intended for outside distribution;
- Remain vigilant for instances where MoH copyrights, patents, trademarks or industrial designs are being used without permission;
- Report all suspected infringements to the legal team;
- Consider licensing terms when sending items that might be termed IP to others outside the organization;
- Make sure that everyone understands the law concerning MoH IP.

4.8.4 Any products developed by MoH employees during their contracted work and/or using MoH assets are by default considered IP of MoH, unless different arrangements between the author(s) and MoH were made prior to performing the work.

4.9 Exceptions

4.9.1 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.

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

4.9.3 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 and external related legal and regulatory bodies.~~ consult internal related legal, and internal and external regulatory bodies.

4.9.4 The requester shall implement the exception after approval is obtained from the Cybersecurity General Manager of Cybersecurity General Department.

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

4.10 Compliance

4.10.1 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.

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

4.10.3 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.

4.11 Violations

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

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

4.12 Policy Review

4.12.1 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.

4.12.2 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.

4.13 Communication

4.13.1 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 Regulatory references:

- Essential Cybersecurity Controls;
- Critical Systems Cybersecurity Controls;
- Anti-Cyber Crime law.

7.2 International framework references:

- ISO/IEC 27001;
- ISO/IEC 27002;
- ISO/IEC 27799;
- HIPAA;
- HITECH;
- HITRUST.

7.3 Internal references:

- Cybersecurity Policy for System and Application Acquisition, Development and Maintenance;
- Cybersecurity Policy for Incidents Response;
- Cybersecurity Policy for Software Security;
- Cybersecurity Policy for Acceptable Use;
- Cybersecurity Policy for Physical and Environmental Security.

8. Appendix

8.1 Government legislation references:

- Essential Cybersecurity Controls;
- Critical Systems Cybersecurity Controls;
- Anti-Cyber Crime Law.

Policy Title	Policy Number	Policy Issuer	Replacement of Policy Number
Cybersecurity Policy for IP and Copyright Compliance	VM.PD - CSD - 025- CPP	Cybersecurity General Department	VM.PD - CSD - 025- CPP
Policy Classification	**Date of Approval**	**Date of Implementation**	**Date of Next Revision**
■ **Corporate Policy**	10 -August-2020	03-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