وزارة الصحة
Ministry of Health

IP and Copyright Compliance Policy

Sharing	AMBER
Classification	RESTRICTED
Number	CSMS_Policy_25
Status	Final
Version	2.1
Date	26/10/2020
Pages	10
Owner	Cybersecurity GM
File Name	CSMS_Policy_25 IP and Copyright Compliance Final 2.1

Sharing & Classification

Sharing	**Amber**: Restricted sharing and recipient may share information only with intended recipients inside MoH and with recipients who are required to take action related to the shared information.
Classification	**Restricted**: Disclosure causes minor embarrassment or minor operational inconvenience.

Revision History

Version	Date	Author	Summary of Changes
1.0	03/03/2020	Cybersecurity Department	Initial draft
1.1	26/10/2020	Cybersecurity Department	Reflecting stakeholders' comments
2.0	25/06/2020	Cybersecurity Department	Final Version (June 2020)
2.1	21/10/2020	Cybersecurity Department	Pre- Publishing Review

Distribution

Name and title	Channel
e-Health	Email
Legal Affairs	Email
Human Resources	Email/ Intranet

Approvals

Name	Position	Signature	Date
Abdullah A Aleid	Cybersecurity Governance		20 Dhu alhuja 1441 10 August 2020
Basem Abdullah AlAngari	General Manager Cybersecurity GD		20 Dhu alhuja 1441 10 August 2020
Cybersecurity Advisory Board			20 Dhu alhuja 1441 10 August 2020

Contents

1. Introduction

Intellectual property (IP) is commonly understood to be a “creation of mind.” It is a property that has an individual intellect involved in creating it. Therefore, the individuals retain some degree of control and ownership over its use in the form of IP right.

The national and international legal frameworks protect IP as included i.e. in article 27 of the universal declaration of human rights, the agreement on trade-related aspects of intellectual property rights and other. The World Intellectual Property Organization (WIPO) provides guidance and administration of many of the applicable international treaties that have been agreed between countries to enforce the protection of IP worldwide.

In Saudi Arabia, IP control and ownership is governed and regulated by the Saudi authority for Intellectual Property (SAIP). SAIP aims to organize, support, sponsor, protect and promote intellectual property in the Kingdom following global best practices.

MoH recognizes the importance of protecting intellectual property in all forms, such as:

- Books;
- Documents;
- Software and source code;
- Designs;
- Logos;
- Music;
- Inventions;
- Designs;
- Trademarks and tradenames;
- Topographies of integrated circuits;
- Recordings;
- Digital media;
- Photographs;
- Films / movies and videos;
- Plays;
- Know-how.

MoH also recognizes the following mechanisms for the protection of intellectual property:

- Patent;
- Protective right for the utility model;
- Protective right for the trademark;
- Protective right for the geographic indication;
- Registration right for the industrial design;
- Protective right for the topographies of integrated circuit;
- Copyright and related rights.

1.1. 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.

1.2. Scope

This Policy applies to MoH both original and acquired material and software used on technical and non-technical assets. Furthermore, it applies to processes and people, including employees, external service providers, suppliers and other third parties who have access to MoH systems. In addition, it covers inventions, designs, tradenames, trademarks, topographies of integrated circuits as well as know-how.

2. 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 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;
- **Line managers, including deputy-ministers**
  - Complies with the Policy and ensures compliance of staff members, contractors, partners, and service providers in their jurisdictions.
- **Software owners within MoH**
  - Ensuring compliant usage with IP copyright terms.
- **Users**
  - Deliberate copyright infringement will be a subject to disciplinary action by the MoH.

3. Policy

3.1. General

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.

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

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

3.2. 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.

3.2.1. 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.

3.3. 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.

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

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

3.3.3. 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.

3.3.4. MoH shall keep, for the legal purposes:

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

3.3.5. 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.

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

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

3.4. Re-using Licenses

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

3.4.1. 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.

3.5. Software Licensing Compliance Reviews

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

3.5.1. Cybersecurity 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.

3.5.2. The review report shall highlight:

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

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

3.6. Other types of IP

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

3.6.1. 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.

3.6.2. 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.

3.6.3. 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).

3.7. Protecting MoH Intellectual Property

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

3.7.1. 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).

3.7.2. 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.

3.7.3. 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. 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).

- 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.
- 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.
- 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.
- 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.

5. Exceptions

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

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

5.3. Cybersecurity 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 Department may consult internal and external related legal and regulatory bodies.

5.4. The requester shall implement the exception after approval is obtained from the head of Cybersecurity Department.

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

6. Compliance

6.1. Compliance with MoH cybersecurity policies and associated controls is mandatory on MoH offices, hospitals, healthcare institutions, staff members, contractors, partners, and services providers who have access to MoH information and information processing facilities.

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

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

7. Violations

7.1. Violations shall be investigated by Cybersecurity Department and shall expose the violator to disciplinary and legal actions according to MoH cybersecurity policies and Saudi laws.

7.2. Disciplinary actions shall be consistent with the severity of the violation, as determined by the investigation, and may include, not being limited to:

- Loss of access rights to information assets;
- Completing cybersecurity awareness;

- Financial penalties;
- Employment termination.

8. Policy review

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

8.2. 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 Department.

9. Communication

Enquiry, feedback, and incidents related to this Policy can be communicated to Cybersecurity 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**

10. Reference to Legislation and Documents

10.1. Regulatory references:

- Essential Cybersecurity Controls[1];
- Anti-Cyber Crime law;

10.2. International framework references:

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

10.3. Internal references:

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

[1] *Essential Cybersecurity Controls*. Riyadh: National Cybersecurity Authority, 2018. PDF. <https://www.ncsc.gov.sa/>.