Employee Handbook and Policy Quick Reference

2021.1

This is an abridged version of MiCT's security policy that all workforce members are required to be familiar with and comply with.

You are assumed to have read and fully understood the corporate security and privacy policies, standards, guidelines, controls and procedures even if you haven't. So, it's probably best you still go through the whole thing at some point.

- First and foremost, as a Health IT provider, MiCT and all its employees must fully comply with HIPAA Security and Privacy regulations. All workforce members much complete the required HIPAA training.
- You are required to follow detailed procedures defined in certain policies related to your job role.

Security is everyone's responsibility. If this is not your first job, don't do anything that might get you in trouble at your previous workplace. When in doubt, stop and ask.

!!! check "Acknowledgement"

```
As a MiCT employee, I acknowledge that

* I have reviewed and will comply with company
  [security policies and procedures][1], [acceptable use][2], and [sanction policies][3].
* I accept that my work devices, including approved BYOD devices, and activities on such dev
* I will protect my work devices at remote locations and will not leave devices unattended.
* I will ensure my laptops and workstations are securely configured with whole disk encrypti
* I will follow documented policies and procedures to protect sensitive and confidential dat
* I have completed the required [HIPAA awareness training][4].
* I understand that customer data and sensitive data may only be stored in approved producti
* I understand company and regulatory requirements to protect critical data and will NOT

    * store critical data such as customer data and passwords on online file shares (such as
    * send critical data such as customer data and passwords by email, chat, or similar publ
    * post critical data such as customer data and passwords in blogs, support tickets or ot
    * discuss patient information in public.

* I understand that use of paper records and fax transmission for sensitive customer data is
* I will keep my passwords confidential and will NOT share my individual user passwords with
* I will NOT use shared/generic, guest/anonymous, emergency or temporary accounts without ex
* I will regularly back up business data on my user devices to approved data storage media/r
* I will report any incident and suspicious activity to Security and/or my manager.
```

Training

You will be prompted as part of onboarding, and periodically going forward, to complete the following security training:

- **General security policy and procedures** training, including
  - Roles, Responsibilities and Training
  - HR and Personnel Security
  - Data Classification and Handling
- **HIPAA awareness** training
- **Ongoing security awareness** training (a monthly series, currently provided by)
- **Role-based security** training
  - all members of the **Development/Engineering** team must carefully review the following policies and procedures
    - Product Security and Secure Software Development
    - HIPAA Best Practices for Software Development
    - Data Management
    - Data Protection
    - Configuration and Change Management
  - all members of the **Administrative**, **Marketing** and **Procurement** teams must review the following policies and procedures
    - Third Party Security, Vendor Risk Management and Systems/Services Acquisition
  - all members of the **Administrative** and **Senior Leadership/Executive** teams must review the following policies and procedures
    - Business Continuity and Disaster Recovery
    - Compliance Audits and External Communications
    - Risk Management
  - all members of the **HR** and **Facilities** teams must review the following policies and procedures
    - HR and Personnel Security
    - Facility Access and Physical Security
  - all team members responsible for **Product Management** and **Business Development** must review the following policies and procedures
    - Privacy and Consent

– all members of the **Security**, **Compliance** and **IT** teams must review all policies and procedures in its entirety

Acceptable use policy for end-user computing

MiCT policy requires that:

(a) Per MiCT security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of MiCT computing systems is subject to monitoring by MiCT IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that are commonly affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the MiCT Data Classification specifications and Data Handling procedures.

(j) Mobile devices are not allowed to connect directly to MiCT production environments.

(k) It is strictly forbidden to download or store any ePHI on end-user computing devices, including laptops, workstations and mobile devices.

Your responsibilities for computing devices

MiCT provides company-issued laptops and workstations to all employees. MiCT currently does not require or support employees bringing their own computing devices.

The laptops and/or workstations assigned to you are yours to configure and manage according to company security policy and standards. You are responsible to

- configure the system to meeting the configuration and management requirements, including password policy, screen protection timeout, host firewall, etc.;
- ensure the required anti-malware protection and security monitoring agent is installed and running; and
- install the latest security patches timely or enable auto-update.

IT and Security provides automated scripts for end-user system configurations and/or technical assistance as needed.

You are also responsible for maintaining a backup copy of the business files local on your laptop/workstation to the appropriate location on MiCT file sharing / team site (e.g. SharePoint). Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams
- Meeting notes/recordings
- Important records (e.g. approval notes)

!!! important

`DO NOT backup critical data such as customer data or PII to file sharing sites. If you have such critical data locally on your device, contact IT and Security for the appropriate data management and protection solution.`

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet MiCT requirements).

Getting help

Support for most of our business applications are self-service, such as password reset via Okta.

If needed, users may use our internal service desk to request IT and Security support. Common requests include:

- Password reset and access requests
- Request new software and hardware
- Technical support

- Recommend changes to policies and processes

How to report an incident or suspicious activity

You are responsible to report all suspicious activities and security-related incidents immediately to the Information Security team, by one of the following channels:

- (preferred) "Report a security incident" by creating an issue on Github and/or via the [internal help desk](](mailto:security@mict-international.org)
- For non-sensitive, non-confidential security issues and concerns, employees may post questions on MiCT's #infosec Slack channel.
- Additionally, employees may report the incident to their direct manager.
- To report a concern under the Whistleblower Policy, you may first discuss the concerns with your immediate manager, or report it directly to the CEO or COO. *See the Whistleblower Policy section in the HR Security Policy for additional details.*