Facility Access and Physical Security

`2021.1`

It is the goal of MiCT to provide a safe and secure environment for all employees. Access to the MiCT facilities is limited to authorized individuals only.

MiCT works with Subcontractors (e.g. property management companies and facilities management) to assure restriction of physical access to systems used as part of the MiCT Platform.

Physical Access to all of MiCT facilities is limited to only those authorized in this policy. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to MiCT's facility.

MiCT and its Subcontractors control access to the physical buildings/facilities that house these systems/applications, or in which MiCT workforce members operate, in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. In an effort to safeguard ePHI from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with escorts for unauthorized persons.

Policy Statements

MiCT policy requires that

(a) Physical access to MiCT facilities is restricted.

(b) All employees are required to wear employee badges at secure facilities (such as server rooms, data centers, labs).

(c) All employees must follow physical security requirements and procedures documented by facility management.

(d) On-site visitors and vendors must be escorted by a MiCT employee at all times while on premise.

(e) All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to MiCT's facility.

(f) Retain a record for each physical access, including visits, maintenance and repairs to MiCT production environments and secure facilities.

- Details must be captured for all maintenance and repairs performed to physical security equipment such as locks, walls, doors, surveillance cameras; and
- All records must be retained for a minimum of seven years.

(g) Building security, such as fire extinguishers and detectors, escape routes, floor warden responsibilities, shall be maintained according to applicable laws and regulations.

Controls and Procedures

Physical Security

Access Requirements Overview

- Physical access is restricted using badge readers and/or smart locks that track all access.
  - Restricted areas and facilities are locked when unattended (where feasible).
  - Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
  - Access and keys are revoked upon termination of workforce members.
  - Workforce members must report a lost and/or stolen key(s) or badge(s) to his/her manager, local Site Lead, or the Facility Manager.
  - The Facility Manager or designee is responsible to revoke access to the lost/stolen badge(s) or access key(s), and re-provision access as needed.
  - The Facility Manager or designee facilitates the changing of the lock(s) within 7 days of a physical key being reported lost/stolen.
- Enforcement of Facility Access Policies
  - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
  - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
  - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from MiCT.
- Workstation Security
  - Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
  - All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
  - All workstations purchased by MiCT are the property of MiCT and are distributed to users by the company.

Building Standards per Location All entry points are secured by card readers and have cameras for additional monitoring as needed.

- **Indianapolis, IN** Office
  - The building is unlocked Monday-Friday from 9am-4pm
  - After hours the building is secured and requires an access card for entry

  - The main entry to our office suite is open during normal business hours (M-F 8am-5pm)
  - MiCT office space is secured and requires an access card for entry for after hours access
  - All server rooms are secured 24/7 and require an access card for entry

- **Morrisville, NC** Office
  - The building is unlocked with free access Monday–Friday 7am-7pm and Saturdays from 9am-1pm
  - After hours the building is secured and requires an access card for entry
  - MiCT office suite is secured 24/7 and requires an access card for entry

Facility Access Data Storage The security server that houses our security configuration for our electronic key card system is securely located in the server room of the prospective office that it manages; Indianapolis, IN and Morrisville, NC.

dnaFusion (Indianapolis office) stores all access control logs indefinitely.

mySonitrol (Morrisville office) stores all access control logs for 90 days.

Camera footage is stored on cameras and footage is accessed through **Meraki**. Footage is stored for a minimum of 30 days.

Facility Access Control Process Access cards are stored in a locked cabinet until they are activated and issued.

New Hires New Hire access cards are assigned based on new hire notice issued through Github.

- New Hire access is typically activated the day prior to start date
- Once activated the access card is stored in a locked cabinet until issued to new hire.

Separations Separation notices are issued through Github.

- Immediate separation notices are processed when issued
- Future separation notices are pre-scheduled for deactivation prior to termination date

Special Access Requests Special access areas require additional approvals for access. If documented approver is unavailable, COO may act as approver.

Maintenance & Repairs All maintenance, repairs and modifications to our access control system will be handled by the local vendor that supports our system.

All documents regarding maintenance, repair or modification will be stored in the physical security folder located on the MiCT SharePoint site.

Reporting and Auditing All access control records are audited on an annual basis.

Special access is audited and reviewed with approver quarterly.

Records are owned and maintained by the Facility Manager. Records are kept in the Physical Security folder on SharePoint and will be retained for a minimum of 7 years.

Data Center Security

Physical security of data centers is ensured by the cloud infrastructure service provided, AWS.

Clean Desk Policy and Procedures Employees must secure all sensitive/confidential information in their workspace at the conclusion of the work day and when away from their workspace. This includes both electronic and physical information such as:

- computer workstations, laptops, and tablets
- removable storage devices including CDs, DVDs, USB drives, and external hard drives
- printed materials

Computer workstations/laptops must be locked (password protected) when physically unattended. Portable devices such as laptops and tablets should be taken home at the conclusion of the work day.

Removable storage devices and printed documents must be treated as sensitive material and locked in a drawer or similar when not in use. Printed materials must be immediately removed from printers or fax machines. Passwords must not be written down or stored physically.

Keys and access cards used for access to sensitive or restricted information/areas must not be left unattended anywhere in the office.