Physical Access to Restricted IT Areas Policy

Section 1. PURPOSE AND SCOPE

Anyone with access to an IT managed space has a responsibility for keeping it protected. The granting, controlling, and monitoring of physical access facilities is extremely important to an overall security program.

The purpose of this policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Clark University ITS managed facilities.

This policy applies to all individuals that use Clark University Information Resources.

Section 2. DEFINITIONS

- **IT Secure Areas:**

  Any University communications, telecommunications closet, network distribution facility, data center, or space that contains restricted IT equipment. Examples of IT Secure Areas include, but may not be limited to:

  - Unshared telecommunications closets that contain only IT equipment
  - Shared telecommunications closets that contain IT equipment and other non-IT equipment, such as electrical panels, fire alarms, door control devices, etc.
  - Locking cabinets or cages containing IT equipment in shared spaces (the cabinet or cage is the IT Secure Area)
  - Exceptions may apply to certain equipment and enclosures including Audio-Video (AV) cabinets, lecterns, or closets, or spaces containing wireless access points or other intentionally public IT equipment.

- **Master Access List (MAL):**

  The list of personnel who are authorized to enter IT Secure Areas.

Section 3. PROCEDURES AND ENFORCEMENT

Information Technology Services (ITS), in cooperation with other University authorities and administrators, will enforce this Policy, and establish standards, procedures, and protocols in support of the policy.

Any violation of this policy by a University student is subject to the Student Code of Conduct in the Student Policy Handbook.

For employees, violation of this policy will be subject to consideration as “misconduct” under Faculty and Staff policies (faculty and non-faculty) and “unacceptable personal conduct” under Employee policies, including any appeal rights stated therein.

If a violation of this policy also results in a violation of law, it may also be referred for criminal or civil prosecution.

Additionally, violations of this policy may result in termination or suspension of access, in whole or in part, to University information systems at the discretion of ITS where such action is reasonable to protect the University or the University's information infrastructure. Failure of the University to carry out this policy effectively could endanger compliance with various local, state and federal laws and agreements surrounding security.

Section 4. ROLES AND RESPONSIBILITIES

- **Chief Information Security Officer**

  is responsible for providing interpretation of this and other related policies and disseminating related information.

- **Information Technology Services**
  is responsible as the managing unit for IT Secure Areas.

- **Staff, Faculty, and students who are authorized to enter IT Secure Areas**

  are responsible for the application of this and related policies to the systems, information, and other information resources in their care.

- **Application Administrators of the University's electronic access control systems**

  are responsible for the application of this and related policies to the systems, information, and other information resources that process, store, or transmit University data.

- **Third-party Affiliates with access to University Facilities, including IT Secure Areas**
  are expected to abide by the University's information security and privacy policies.

Section 5. POLICY

- **Physical Characteristics of IT Secure Areas**

  - New or renovated IT Secure Areas must be isolated in dedicated (non-shared) access-controlled space.
  - Physical access controls for IT Secure Areas will include one or more of the following: multi-factor authentication, key-card access, biometric access controls, or limited access key.
  - The University recognizes that some pre-existing IT Secure Areas do not meet these criteria because no reasonable remediation path exists to isolate the IT

equipment or to accommodate electronic access control equipment. Deviations from physical and environmental controls identified in the University Design and Construction Guidelines for new or renovated IT Secure Areas require written approval by the Director of IT Infrastructure.

Physical Entry

- Only authorized personnel as defined in the MAL shall place equipment or wiring in any IT Secure Area according to their department's jurisdiction over the area. Any individual or department outside of the above provision must obtain written permission from the CIO, Director of IT Infrastructure, or exclusively authorized jurisdictional department as defined in the MAL.
- Access to IT Secure Areas will be controlled and restricted to authorized personnel who require ongoing access. Authorization for access is granted based on the principle of least privilege and follows the "minimum necessary" standard by which users are given the minimum amount of access necessary to perform their job functions.
- Information Technology Services will maintain the Master Access List (MAL) of personnel who are authorized to enter IT Secure Areas. Only named individuals on the MAL can obtain keys, key cards, fobs, or other credentials that enable physical entry to IT Secure Areas.
- Temporary access to IT Secure Areas such as Data Centers may be requested for educational purposes to students. If this is the case, and a request for access has been submitted and approved, each student must complete a Non-Disclosure Agreement. Each NDA must be shared with the Information Privacy and Compliance Analyst as well as the Office of the Executive Vice President.
- The MAL and other access lists are subject to regular review (at a maximum interval of 6 months) to ensure that IT Secure Area access is limited to only those with a business need for physical access to the IT Secure Area.
- Physical access to IT Secure Areas for non-authorized personnel or visitors will be granted on a case-by-case basis by the Vice President for Information Technology Services and CIO and/or designee(s) when a clear University business need merits exception. Non-authorized personnel who have been granted temporary access by exception must be escorted by authorized personnel.
- Police, fire, and other emergency responders (including Facilities Management) may enter IT Secure Areas to respond to incidents that threaten public safety, health, and welfare as needed without prior authorization. ITS should be notified if an area is entered without prior authorization.

Logging

- Card access will be used as a means to authorize entry to secure spaces. Exceptions must be approved by the CIO.
- Access to IT Secure Areas by non-authorized personnel or visitors must be logged for entry time, exit time, purpose, and workforce member who allowed (enabled) the entry.

- Access by police, fire and other emergency responders must be logged for entry time, exit time and purpose after the causative incident has been fully resolved.

Related Policies and Regulations

Admin and Staff Handbook

Student Policy Handbook

History/Revision Information

Responsible Office/ Division: ITS

Effective Date: February 26, 2024

Last Amended Date: August 27, 2024

Next Review Date: February 26, 2027