Administrative Policy
2021-01 Informational Technology Physical Security

Title	Information Technology Physical Security
Policy Owner and Contact Information	Information Technology Security itsecurity@uchc.edu / UConn Health Service Desk 860-679-4400
Applies to	All UConn Health workforce members, including employees, faculty, staff, students, residents, volunteers and other individuals.
Campus Applicability	UConn Health
Effective Date	3/3/21

PURPOSE:
To establish requirements for the management, control, monitoring, and removal of physical access to UConn Health facilities containing Information Technology (IT) Electronic Resources.

APPLIES TO:
This policy applies to all UConn Health workforce members, including employees, faculty, staff, students, residents, as well as volunteers and other individuals with access to UConn Health restricted/controlled areas containing IT Electronic Resources.

DEFINITIONS:
Restricted/Controlled Area – Any area not open to the public containing IT Electronic Resources

Physical Security - Security measures designed to deny unauthorized access to facilities containing IT Electronic Resources and protect personnel and property from damage or harm.

IT Electronic Resource – Any computing system used for the ongoing operations of institutional activities including workstations, laptops, removable storage, networking equipment and other technologies.

POLICY STATEMENT:

Physical Security

1. All facilities containing IT Electronic Resources must be physically protected relative to the importance of the function or purpose of the managed area.
2. Access to facilities containing IT Electronic Resources will be granted only to personnel whose job responsibilities require access. Electronic access control systems shall be used to manage access to facilities containing IT Electronic Resources, where available and appropriate.
3. Access rights to facilities containing IT Electronic Resources shall be based on the individual's role or function in the organization.
4. Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft or unauthorized physical access to confidential data.

Facility Access Key Cards

1. Access cards and/or keys for access to restricted/controlled areas containing IT Electronic Resources must not be shared or loaned to others.

2. Lost or stolen access cards and/or keys must be reported immediately to UConn Public Safety.

Facility Access

1. A log of access to restricted/controlled areas containing IT Electronic Resources must be maintained, by the responsible unit/department, to provide a physical audit trail of access to facilities, computer rooms and data centers where sensitive information is stored or transmitted.
    a. For individuals without electronic badges a paper log will be used and shall document the individuals name, organization represented, and the UConn Health representative authorizing physical access, where applicable.
2. Any individual accessing restricted/controlled areas containing IT Electronic Resources shall wear a UConn Health badge or other identification. Non-workforce members will be issued a temporary badge that expires and that visibly distinguishes the individual from UConn Health workforce members. Badges must be visible at all times while in restricted/controlled areas containing IT Electronic Resources.
    a. All electronic badges must be worn so that both the picture and information on the badge are clearly visible.
3. Non-workforce members without a badge compatible with an electronic badge reader must be escorted at all times within restricted/controlled areas where IT Electronic Resources are located.

PROCEDURES

An annual review of physical access rights to restricted/controlled areas containing IT Electronic Resources shall be performed to determine the appropriateness of facility access and controlled zones.

The Division of Public Safety is responsible for adding approved access to all Identification Badges. Facilities Development and Operations is responsible for issuing keys.

Requests for access shall come from the applicable manager in the area where the data/system/ equipment resides.

Revocation of all facility access shall occur immediately upon termination including the collection of keys, access cards, and/or any other asset used to enter restricted areas.

Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration.

REFERENCES:

45 C.F.R. §164.310

RELATED POLICIES:

2002-43 Confidentiality

ENFORCEMENT:

Violations of this policy or associated procedures may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, the University of Connecticut Student Code, other applicable University Policies, or as outlined in any procedures document related to this policy.

APPROVAL:

Andrew Agwunobi (Signed)	3/3/2021
UConn Health Chief Executive Officer	Date
Kiki Nissen (Signed)	3/3/2021
Administrative Policy Committee Vice-Chair	Date
Janel Simpson (Signed)	3/3/2021
Administrative Policy Committee Chair	Date

POLICY HISTORY:

New Policy Approved: 3/3/21
Replaces: 2005-04 HIPAA Security Facility Access Control Policy