Administrative Policy
2011-03 Systems Access Control

Title	Systems Access Control
Policy Owner and Contact Information	Information Technology Security itsecurity@uchc.edu / UConn Health Service Desk 860-679-4400
Applies to	UConn Health faculty, staff, others as defined below
Campus Applicability	UConn Health
Effective Date	2/3/2020

PURPOSE:
To define the requirements for managing the authentication, authorization, and administration of access to UConn Health's Confidential Data (2002-43 Confidentiality) and electronic resources.

APPLIES TO:
This policy applies to all computing equipment and software owned, leased, operated or contracted by UConn Health that is used to process and/or store Confidential Data (electronic resource), as well as, all users (workforce, business associates and non-workforce members) requiring access to and/or administering or having managerial authority of that data and those systems.

DEFINITIONS:
Service account – an account that provides applications/services (not a person) access to required resources.
Elevated privileges – privileges that exceed those assigned to a standard user account.

POLICY STATEMENT:
General Access Controls

The use and access of UConn Health's electronic resources is restricted to appropriately identified, validated and authorized individuals or automated processes for valid business purposes only.

UConn Health electronic resources shall require the use of a unique identifier in conjunction with a password or other form of authentication that has been approved by the Information Security Officer.

Passwords must be minimally configured in accordance with established UConn Health's password standards.

Procedures for requesting, authorizing and documenting additions of or modifications to user access to UConn Health electronic resources shall be maintained by the Data Steward (Data Roles and Responsibilities) and/or UConn Health IT, as appropriate.

Any type of account (service, workforce, business associates and non-workforce members) used to access any UConn Health electronic resource must have an account sponsor, who is knowledgeable of the account holder's access requirements and/or is responsible for managing the service or relationship between UConn Health and the user.

Minimum necessary access will be assured such that access to systems, assigned views or roles, and remote access ability will be consistent with the authorized user's valid business purpose only.

Users will not share their password or other authentication devices.

Users will not use another user's identifier and/or authentication data or devices to access UConn Health electronic resources.

Service Accounts

The use of service accounts are permitted on authorized devices that satisfy the following criteria:

- The electronic resource needs to remain logged onto the UConn Health network throughout the day to facilitate individual users gaining speedy access to clinical systems using their own individual log on credentials
- The account is required to support the functionality of a system process, device or application.

Service accounts will only have access to a pre-defined set of UConn Health electronic resources and will not have access to email or internet services.

Service accounts must have a designated account owner responsible for the management and use of the account.

Anonymous access, including the use of guest and public accounts, to any UConn Health electronic resource is prohibited.

Any account with elevated privileges shall not be used for routine activities.

Use of shared accounts on UConn Health electronic resources is prohibited.

DEFINITIONS:
Service account – an account that provides applications/services (not a person) access to required resources.
Elevated privileges – privileges that exceed those assigned to a standard user account.

PROCEDURES/FORMS:

- The Data Steward, account sponsor and/or UConn Health IT shall periodically review user privileges to electronic resources for continued need, as appropriate.

- User managers and/or account sponsors shall evaluate access rights when an account holder's access requirements to UConn Health's electronic resources change (e.g., job assignment change, change to remote access agreement).

- User accounts which have been inactive for 365 consecutive days will be marked for deletion.

- Users must manage their passwords in accordance with the UConn Health password standards or their account will be marked for deletion.

- User managers and/or account sponsors shall be responsible for making appropriate and timely requests for UConn Health systems account deactivation.

- User managers and/or account sponsors will ensure appropriate clearance and authorization (background checks, Business Associate Agreements, etc.) to access UConn Health electronic resources is obtained prior to submitting or approving access requests.

REFERENCES:
45 C.F.R. §164.308(3)(i)
45 C.F.R. §164.308(4)(i)
45 C.F.R. §164.312(d)
45 C.F.R. §164.312 (a) (1)
45 C.F.R. §164.312 (a) (2)
Password Standards

RELATED POLICIES:
2002-43 Confidentiality
Data Roles and Responsibilities (UConn Storrs)
2019-01 Acceptable Use, UConn Health

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) 2/11/2020
UConn Health Chief Executive Officer

Kiki Nissen (Signed) 2/10/2020
Administrative Policy Committee Co-Chair

Janel Simpson (Signed) 2/10/2020
Administrative Policy Committee Co-Chair

New Policy Approved: 2/8/2011
Revisions: 5/13/2014, 2/3/2020
Replaces Policy #2005-05 UCHC HIPAA Security Information – Systems Access Control