Administrative Policy
2005-08 Information Security Risk Assessment

Title	Information Security Risk Assessment
Policy Owner and Contact Information	IT Security IT Website: https://health.uconn.edu/information-technology/
Applies To	UConn Health Workforce
Campus Applicability	UConn Health
Effective Date	June 2, 2021

PURPOSE:
To identify and mitigate Information Technology (IT) risks that could negatively impact patient safety or the confidentiality, integrity or availability of UConn Health confidential data and critical IT resources.

APPLIES TO:
This policy applies to all members of the UConn Health workforce, critical UConn Health Information Technology resources and any UConn Health system used to store, process or transmit confidential data.

DEFINITIONS:
Electronic resources are computing and telecommunications devices that can execute programs or store data which may include but are not limited to computers, mobile computing devices, servers and storage devices (USB or otherwise connected). Electronic resources may also include software, medical devices, Internet of Things (IOT), and cloud-based services.

POLICY STATEMENT:

1. The Information Security Office (ISO) is responsible for developing a process for conducting risk assessments for UConn Health's IT resources.
2. Operational leaders, or their designated data stewards, in coordination with the Information Security department are responsible for ensuring that a risk assessment is performed biennially and as needed when there is an environmental or operational change that may affect the security of electronic resources managed by their respective areas or otherwise under their control.
3. All new software applications and associated onsite equipment/hardware, or cloud-based services storing, processing or transmitting UConn Health Confidential Data must be evaluated for security vulnerabilities and potential risks to such data. Any identified risks or vulnerabilities identified must be remediated or mitigated prior to deployment in a production ready state.
4. The results of the risk assessment will be used to determine security improvements resulting in reasonable and appropriate levels of risk acceptance and compliance for each system.
5. Failure to remediate or mitigate identified risks may result in the electronic resource(s) being removed from the UConn Health network.
6. Results indicating an unacceptable level of risk shall be remediated as soon as possible, as determined by specific circumstances and the timelines decided collectively by the Information Security Officer, Data Steward(s), Dean(s), Director(s) or Department Head(s).
7. Results of all risk assessments shall be treated as confidential and stored in a secure location.

PROCEDURES/FORMS:
None

REFERENCES:
45 C.F.R. §164.308(1) (ii) (A) (B)
16 C.F.R. §314.4(b)
PCI DSS 12.2

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) 6/2/2021
UConn Health Chief Executive Officer

Kiki Nissen (Signed) 6/2/2021
Administrative Policy Committee Vice-Chair

Janel Simpson (Signed) 6/2/2021
Administrative Policy Committee Chair

POLICY HISTORY:
New Policy Approved 01/28/05
Policy Revised: 7/9/18, 6/2/21