Administrative Policy
2005-08 Information Security Risk Assessment

<table>
<thead>
<tr>
<th>Title</th>
<th>Information Security Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Owner and</td>
<td>IT Security</td>
</tr>
<tr>
<td>Contact Information</td>
<td>IT Website: <a href="https://health.uconn.edu/information-technology/">https://health.uconn.edu/information-technology/</a></td>
</tr>
<tr>
<td>Applies To</td>
<td>UConn Health Employees, students, residents</td>
</tr>
<tr>
<td>Campus Applicability</td>
<td>UConn Health</td>
</tr>
<tr>
<td>Effective Date</td>
<td>July 9, 2018</td>
</tr>
</tbody>
</table>

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:
None

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. 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.
3. 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).
4. Results of all risk assessments shall be treated as confidential and stored in a secure location.

PROCEDURES/FORMS:
Operational areas are responsible for ensuring that a risk assessment is performed biennially for each of the information technology resources in their respective areas. Risk assessments will also be conducted when there is environmental or operational changes that may affect the security of confidential data or critical electronic resources.

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, UConn Health Chief Executive Officer (Signed) 8/02/18
Carolle Andrews, Policy Committee Co-Chair (Signed) 7/30/18
Kiki Nissen, Policy Committee Co-Chair (Signed) 7/31/18

POLICY HISTORY:
New Policy Approved 01/28/05
Policy Revised: 7/9/2018