**Security Administration Procedures**

1. **Overview**

Various regulations require that organizations define responsibility and accountability for information security administration.

1. **Objective/Purpose**

These security administration guidelines make recommendations that operational leaders or their designees may use to support compliance with the UConn Health Information Security Administration policy.

1. **Scope**

These guidelines apply to all UConn Health workforce, Business Associates, Non-Workforce and all other individuals granted access to UConn Health electronic resources.

1. **Guideline**
	1. Operational leaders, or their designate data stewards shall create and maintain reasonable and appropriate procedures to comply with UConn Health policies.
		1. Procedures should take into account the size, complexity, capabilities, and technical infrastructure, hardware, and software capabilities of the operational area; the costs of security measures; and the probability and criticality of potential risks to confidential data.
	2. The ISO shall develop guidelines for the purpose of assisting departments to comply with policies and procedures.
	3. Policies, procedures and actions, activities or assessments, including but not limited to, risk analysis, evaluations, and documentation related to security incidents and their outcomes, shall be maintained for six years from the creation date or the date when it last was in effect, whichever is later.
	4. Policies, procedures, and guidelines shall be documented and stored, by the respective operational areas and the UConn Health ISO.
	5. Data Stewards shall make documentation available to anyone responsible for implementing, managing, and auditing the procedures.
	6. Data stewards shall review, update and modify documentation, as needed, if environmental or operational changes occur that affect the security of confidential data.