UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Information Security Liaison Policy

Policy Statement

Given the risks associated with information security incidents, as well as implications for the University's compliance with federal and state regulatory requirements and the terms of certain grants and contracts, it is essential that Deans and Department Heads be aware of information security issues and of their responsibilities for mitigating information security risks.

Deans or Department Heads who oversee University business units that maintain and manage their own Information Technology must designate employees as primary and back-up Information Security Liaisons, provide the Information Security Office with the names and contact information of these individuals, and update this information whenever it changes.

Each Information Security Liaison (ISL) must act as an intermediary between his/her respective University business unit and the Information Security Office (ISO) and must assist the University business unit he/she serves in implementing information security policies and information security initiatives and in responding to data breach incidents, all in close coordination with the Information Security Office.

Scope

This policy sets forth requirements for school and departmental Information Security Liaisons.

Audience

This policy applies to all Deans and Department Heads who oversee University business units that maintain and manage their own Information Technology and to the employees of those business units who are designated as primary or back-up Security Liaisons.

Compliance

Failure to adhere to this policy may result in disciplinary consequences for employees up to and including termination of employment.

Definitions

- **Data Steward:** A Senior University Official who has responsibility for managing a segment of the University's institutional data resources. By virtue of their positions, Stewards of institutional data have the primary administrative and management responsibilities for the segments of data within their functional areas. For example, the Vice Chancellor for Human Resources has stewardship responsibility for HR data. Stewards of institutional data interpret policy, define procedures pertaining to the use and release of the data for which they are responsible, and ensure the feasibility of acting on those procedures.
- **Incident Management Plan**: A plan established and maintained by a University business unit that manages its own or subcontracts its information technology and that contains procedures on how to handle Information Security Incidents, including contact information for business unit personnel with responsibility for responding to the incident, plans to contain an incident, and procedures on how to restore information, if necessary.
- **Information Security Incident:** Includes any incident that is known or has the potential to negatively impact the confidentiality, integrity, or availability of UNC-Chapel Hill's information. This can range from the loss of a laptop or PDA to the virus infection of an end-user work station to a major intrusion by a hacker.
- **ISO:** Denotes the staff of the University's Information Security Office.
- **Mission-Critical Resource:** Includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Typical mission-critical services have a maximum downtime of three consecutive hours or less. Mission-critical resources for Information Security purposes include information assets, software, hardware, and facilities. The payroll system, for example, is a Mission-Critical Resource.
- **Sensitive Information:** Sensitive Information includes all data, in its original and duplicate form, which contains:
  - "Personal Information," as defined by the North Carolina Identity Theft Protection Act of 2005. This includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or info that can be used to access a person's financial resources.
  - "Protected Health Information" as defined by HIPAA

- Student "education records," as defined by the Family Educational Rights and Privacy Act (FERPA)
- "Customer record information," as defined by the Gramm Leach Bliley Act (GLBA)
- "Card holder data," as defined by the Payment Card Industry (PCI) Data Security Standard
- Confidential "personnel information," as defined by the State Personnel Act
- Information that is deemed to be confidential in accordance with the North Carolina Public Records Act

Sensitive data also includes any other information that is protected by University policy or federal or state law from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, social security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public-safety information, information concerning select agents, information security records, and information file encryption keys.

Roles and Responsibilities

Deans or Department Heads who oversee University business units that maintain and manage their own Information Technology must designate employees as primary and back-up Information Security Liaisons, provide the Information Security Office with the names and contact information of these individuals, and update this information whenever it changes.

Each Information Security Liaison must act as an intermediary between his/her respective University business unit and the Information Security Office (ISO) and must assist the University business unit he/she serves in implementing information security policies and information security initiatives and in responding to Information Security Incidents, all in close coordination with the Information Security Office.

Information Security Liaison (ISL) roles and responsibilities include, but are not limited to:

- Serving as a single point of contact for the ISO regarding security efforts and Information Security Incidents that affect the ISL's business unit.
- Aiding the ISO in improving information security at UNC Chapel Hill by

coordinating with the ISO on security matters.
- Working with the ISO on incident management and response as well as assist the ISO, as needed, in certain activities including the ones described below.
- Acting as the primary point of contact with the ISO when handling security intrusions that affect the ISL's business unit.

Specifically, the ISL will coordinate the following with the ISO:

- Ensure proper identification and classification of computer resources storing Sensitive Information or deemed Mission Critical within their business unit.
- Advise their unit's systems development and application Data Stewards on the implementation of appropriate security controls for information on systems, from the point of system design through testing and production implementation.
- Meet periodically with the ISO staff to move forward enterprise security initiatives for their respective University business unit.
- Maintain an up-to-date list of staff with access to Sensitive Information in their working group and promptly notify the ISO of any personnel changes, including transfers within the University.
- Provide basic security advice for all assigned systems and users within their business unit. Ensure timely compliance with security awareness requirements, including appropriate refresher training and training of new employees. In consultation with the appropriate Data Steward, the ISL will work towards ensuring that the department business unit or working group is compliant with applicable state and federal laws as well as University policies regarding the confidentiality of Sensitive Data.
- Ensure that any detected vulnerabilities are remediated in a timely manner consistent with the Vulnerability Management Policy.
- Advise their University business unit and/or their respective other assigned areas of responsibility regarding the implementation of appropriate security controls consistent with the University's Information Security Policy.
- Collect incident response information and metrics, including development and maintenance of the department's or University business unit's incident response plan. The ISL must ensure a timely notification of the University's ISO regarding any Information Security Incidents for their respective University business unit consistent with the Incident Management Policy. In addition, the ISL must ensure a timely and comprehensive response to Information Security Incidents in coordination with the University's ISO.
- Report incident and incident metrics to the University's ISO consistent with the Incident Management Policy.
- Coordinate with the ISO regarding the University's information security strategic initiatives, including security improvements for the liaison's

University business unit or department. Periodically report to University Administrators/Deans/Department Heads/ISO regarding the entity's status with respect to information security initiatives and policy compliance.

Related Documents

Data Governance Policy
Incident Management Policy and Procedures
Information Security Policy
Vulnerability Management Policy

Contacts

Subject	Contact	Telephone	FAX
Policy Questions	The University's Information Security Office	919-445-9393	919-445-9488
Report a Violation			
Request Information Security Consulting			

History

Effective Date:
Revised Date: 6/30/10
Next Review Date: