UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Incident Management Policy

Policy Statement

Each business unit at the University of North Carolina at Chapel Hill that manages its own or subcontracts its information technology must:

- Establish and maintain an up-to-date Incident Management Plan. For specific elements that must be included in the Incident Management Plan, contact the Information Security Office (ISO) at 919-445-9393 or security@unc.edu.
- Designate a primary and backup Information Security Liaison. See Information Security Liaison Policy.
- Provide the Information Security Office with the names and contact information of the business unit's primary and backup Information Security Liaisons and update this information whenever it changes.

Every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus who has access to University-owned or managed information through computing systems or devices ("Users") must report Information Security Incidents (as defined below) promptly per the procedures described herein.

When deemed appropriate to protect Sensitive Information (as defined below) or Mission-Critical devices (as defined below), the Information Security Office may, in coordination with the affected University business unit, direct the incident response and investigation. The Executive Director and Information Security Officer or the Chief Information Officer has the authority to take any action deemed appropriate to mitigate the risk posed by any Information Security Incident. Depending on the scope of the investigation, ITS may request reimbursement of associated costs from the affected department(s).

Scope

This policy and the related Incident Management Procedures set forth requirements and procedures for reporting and managing Information Security Incidents.

Audience

This policy applies to all Users accessing the UNC network through computing devices owned by or managed through UNC-Chapel Hill or through permission

granted by UNC-Chapel Hill. It also applies to each business unit at the University that manages its own or subcontracts its information technology.

Compliance

Failure to adhere to this policy may put University information assets at risk and may have disciplinary consequences for employees up to and including termination of employment. Students who fail to adhere to this Policy will be referred to the Honor System. Contractors and vendors who fail to adhere to this Policy may face termination of their business relationships with the University. Violation of this policy can in some cases also carry the risk of civil or criminal penalties.

Definitions

- **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, for example, 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 Identifying 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 information 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.

Incident Management Procedures

Adherence to the procedures outlined below will streamline the handling of Information Security Incidents and minimize the timeframe during which Sensitive Information and Mission-Critical Resources are left in a vulnerable state.

Incident Reporting

Every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus who has access to University-owned or managed information through computing systems or devices ("Users") and who suspects that there may have been an Information Security Incident (ranging from a lost or stolen PDA or laptop to the virus infection of an end-user work station to a major intrusion by a hacker) must promptly report the Incident to the IT Response Center at 962-HELP. The IT Response Center is available 24 hours a day, 7 days a week, so there is no reason not to contact them immediately.

For those business units that manage their own, or subcontract, their information technology, the Security Liaison for that unit should also be notified.

If University equipment, including a University-owned laptop or PDA, has been lost or stolen, then Public Safety must also be notified at 962-8100.

If there is reason to believe that Personal Identifying Information may have been compromised, the Office of University Counsel should also be notified at 962-1219.

Each Information Security Incident will be classified by the Information Security Office accordingly to the following "levels:"

Incident Level	Examples	Investigation Type
Level 1	• Violation of UNC Acceptable Use Policy • Virus infection of end-user desktops	• Basic investigation of an incident • Remediation advice for an incident is provided • Device isolation, if necessary
Level 2	A suspected incident involving Sensitive Information stored on a system or device owned or managed by the University or hosting University Sensitive Information	Investigation of an incident *potentially* involving unauthorized access of Sensitive Information or a Mission-Critical system

Incident Level	Examples	Investigation Type
Level 3	An incident involving Sensitive Information on a University-owned or managed system or device or a system hosting such University information where the initial investigation indicates a likelihood that Sensitive Information was successfully accessed by an intruder	• Investigation of a likely or confirmed breach of a system processing/storing Sensitive Information or a Mission-Critical system • Investigation of information-technology-relevant issues performed in support of criminal or civil cases, as well as University internal investigations

In the event of a possible Level 2 or 3 Information Security Incident, the User or administrator of the potentially compromised system or device should attempt to preserve all evidence, including leaving the possibly compromised machine powered up and online, and refraining from accessing the system or machine in any way. The IT Response Center will notify the Information Security Office, who will determine how best to proceed for purposes of preserving evidence and ensuring an audit trail for the investigation of the incident. For confidentiality reasons, only contact information and minimal details regarding the Information Security Incident should be provided to the IT Response Center. An Information Security Specialist will promptly contact the reporting party at the telephone number left by the reporting party with the IT Response Center.

As appropriate, the Information Security Office will coordinate with Public Safety and the Office of University Counsel.

All external communications with the media or the public related to any Information Security Incident will be coordinated through the Office of University Relations.

If the Information Security Office determines that the affected University business unit can take the lead on the incident handling, the Information Security Office must be regularly and comprehensively updated on the progress of the incident response.

Reimbursement Rates
To assist with the reimbursement for materials and time spent by the Information Security Office in handling Information Security Incidents, the following reimbursement rates will apply when an Information Security Incident arises.

Incident Level	Reimbursement Rate
Level 1	No charge
Level 2	The Information Security Office will be reimbursed at the approved ITS Standard Technical Rate. Reimbursement will be the responsibility of the University business unit that has the primary responsibility for the incident occurrence. In the event that no University business unit can be identified based on incident occurrence, the department to which the Information Steward associated with affected information belongs will be responsible.
Level 3	ITS will be reimbursed at the ITS Standard Technical rate for any work done by the Information Security Office on the incident. In addition, ITS may seek the assistance of a third-party provider of forensics services. If this assistance is deemed necessary by the Information Security Office, reimbursement of all costs of the third-party services related to the investigation of the incident will be required of the University business unit that has the primary responsibility for the incident occurrence. In the event that no University business unit can be identified based on incident occurrence, the department to which the Information Steward associated with affected information belongs will be responsible.

On an individual case basis for level 2 or level 3 Information Security Incidents, ITS may also seek reimbursement for any specialized software and equipment materials required in support of the investigation.

Related Documents

- NC Identity Theft Protection Act of 2005
- HIPAA Security Rule
- Gramm Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Payment Card Industry (PCI) Data Security Standard
- UNC-Chapel Hill Interim Data Network Acceptable Use Policy
- The University of North Carolina at Chapel Hill Protocol for Responding to Security Breaches of Certain Identifying Information
- Definition of Sensitive Information

Contacts

Subject	Contact	Telephone	Fax
Policy Questions	University Information Security Office	919-445-9393	919-445-9488
Report a Violation	University Information Security Office	919-455-9393	919-445-9488
Report a Violation Involving Personal Identifying Information	University Information Security Office	919-455-9393	919-445-9488
	Office of University Counsel	919-962-1219	
Report Lost or Stolen University Equipment	University Information Security Office	919-455-9393	919-445-9488
	Public Safety	919-962-8100	
Request Information Security Consulting	University Information Security Office	919-455-9393	919-445-9488

History

Effective Date:
Revised Date: June 30, 2010
Next Review Date: