UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Security Officer

Responsible Office
ITS – Information Security Office

PROCEDURE

UNC-Chapel Hill Incident Management Procedure

Purpose and Background

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 exist in a vulnerable state.

The following procedures are required for all UNC-Chapel Hill affiliates unless an exception is granted by the Chief Information Officer or delegate. Please see the Incident Management Policy for policy context relevant to these procedures. Regarding incidents that involve risk to payment card information, please also see the Payment Card Industry-Incident Management Plan.

Audience

This procedure applies to all departments and Users including Users engaged in merchant activity as defined by the Payment Card Industry Data Security Standards

Procedures

INCIDENT REPORTING

Every UNC-Chapel Hill affiliate who has access to University-owned or managed information (AKA Users) and/or who suspects an Information Security Incident that might endanger any Sensitive, University-owned Information or Mission-Critical Resource must follow these steps:

1. If sensitive information is believed to be in current danger of being acquired remotely from a computing device by an unauthorized party, a User may disable or disconnect the network interface on the system. Doing so will limit the information available to Incident Handlers so Users should only disable a network interface when necessary to protect against an identified, current threat.
2. In order to preserve evidence, the potentially-compromised system should remain powered up and no one should use the system in any way until instructed otherwise by an Incident Handler.

3. Immediately report the suspected Incident to the Information Technology Response Center (ITRC), which is available 24 hours a day, 7 days a week, by calling 919-962-HELP or toll-free by calling 1-866-962-4457.
4. Ask the ITRC staff member who answers to "please create a critical Remedy ticket for Information Security."
5. Provide only a name and a telephone number at which the reporting User can be reached within the next 30 minutes.
6. Do not provide additional information to the ITRC staff member. Wait to provide detailed information about the incident until called by an Incident Handler, who will respond within 30 minutes.
7. If University equipment has been lost or stolen, the primary user of the equipment must notify UNC Department of Public Safety at 919-962-8100.

Events that do not place sensitive, University-owned information or Mission-Critical Resources at risk need not be reported, but the Information Security Office (ISO) is available to offer counsel at any time.

INCIDENT MANAGEMENT

The assigned Incident Handler may notify the appropriate campus Information Security Liaison (ISL) but the affiliate reporting the matter should also feel free to consult their ISL at any time.

UNC-Chapel Hill Incident Handlers will lead response efforts including preserving evidence and ensuring an audit trail regarding investigation of the incident.

As appropriate, the ISO will coordinate with Public Safety, the Privacy Office, the Office of University Counsel and others.

All external communications with the media or the public related to any Information Security Incident must be coordinated through University Communications AND the Office of the Chief Information Officer or their delegates.

If the University Chief Information Security Officer determines that the affected University business unit may lead the incident handling activity or a component thereof, the Information Security Office must be regularly and comprehensively updated on the progress of the incident response.

REIMBURSEMENT

Information Technology Services (ITS) will be reimbursed at the ITS Standard Technical rate for work by the Information Security Office regarding Information Security Incidents. In addition, ITS may seek the assistance of third-party forensic service providers. If third-party assistance is deemed necessary by the Chief Information Security Officer, reimbursement of costs relevant to the third-party services 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, the home department of the relevant Information Steward will be responsible for reimbursement.

On an individual case basis the department responsible for the incident will reimburse ITS for any specialized software and equipment or materials required in support of the investigation

ITS may also seek reimbursement for any specialized investigative services required by either the major card brands (i.e., Visa, Mastercard, Discover, American Express, JCB) or the Payment Card Industry Security Standards Council for investigations involving Payment Card information. In addition, the department responsible for the merchant account will also be responsible for payment of any fines, penalties, fees, or other costs resulting from a Payment Card Industry investigation.

Compliance

Failure to comply with 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 may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with UNC-Chapel Hill.

Roles and Responsibilities

- **Users:** report all incidents that involve risk to sensitive, University-owned information and/or Mission-Critical Resources as per the Incident Management Procedures linked below.

- **UNC Incident Handlers:** provide incident management, consulting, referral to Office of University Counsel (when appropriate) and other services.

Definitions

- **Information Security Incident:** Includes any event that has the potential to negatively impact the confidentiality, integrity, or availability of UNC-Chapel Hill's sensitive information (including physical files such as paper files) or mission critical resources. Examples of incidents include the loss or theft of a mobile device that has not been encrypted and that stores sensitive, University-owned information, a virus infection of an end-user work station that works with sensitive, University-owned information or the disabling of a piece of mission-critical hardware that endangers mission-critical resources.

- **ISO:** Denotes the staff of the Information Technology Services, Information Security Office.

- **ITS Standard Technical rate**: A reimbursement rate approved by the University and published on the official interdepartmental fees and charges schedule posted on the University Finance website.

- **Information Steward:** The University official responsible for management of a segment of University information resources. For example, the Registrar is the Information Steward for much of the University's student information.

- **Incident Handler:** A University employee trained in incident handling techniques.

- **Mission-Critical Resource:** Includes any resource that is critical to the mission of the University. Typical mission-critical services have a maximum downtime of three consecutive hours or less. The owning business unit determines whether a resource is mission critical. Once designated as mission critical, information security policies and standards apply in an effort to assure that the resource remains available. If a business unit does not designate a resource as mission critical, that resource may not be a priority for restoration of services in the event of an incident or outage.

- **Sensitive Information:** Sensitive Information includes information which contains:

- "Personal Identifying Information (PII)," as defined by the North Carolina Identity Theft Protection Act of 2005. In combination with name, PII 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 Data Security Standards (PCI DSS)
  - 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 information also includes any other information that is protected by University policy or law from unauthorized access. Sensitive information must be restricted to those with a legitimate business need for access.

Related Documents

1. NC Identity Theft Protection Act of 2005
2. HIPAA Security Rule
3. Gramm Leach Bliley Act (GLBA)
4. Family Educational Rights and Privacy Act (FERPA)
5. Payment Card Industry Data Security Standards (PCI DSS)
6. UNC-Chapel Hill, Payment Card Industry (PCI) Incident Management Plan
7. Incident Management Procedures
8. UNC-Chapel Hill Data Network Acceptable Use Policy
9. Definition of Sensitive Information
10. Information Classification Standard

Contacts

Subject	Contact	Telephone	Online
Policy Questions or Information Security Consulting	UNC Information Security Office	919-962-HELP	help.unc.edu
Report an incident	UNC Information Security Office	919-962-HELP	N/A
Report lost or stolen University equipment	Department of Public Safety	919-962-HELP	N/A

Document History

- Effective Date and title of Approver: 6/30/2010 VC for Information Technology and CIO
- Revision and Review Dates, Change notes, title of Reviewer or Approver:

  9/19/14 Revised template, VC for IT and CIO

  10/20/15 Revised template, CISO

  10/17/2016 Review only, link added to references, CISO