Responsible University Officer
VC for Information Technology and CIO

Responsible Office
Information Technology Services

POLICY
UNC-Chapel Hill Incident Management Policy

.

Policy Statement

Each department at the University of North Carolina at Chapel Hill must:

- 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 the contact information when it changes.

Every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus (AKA Users) who has access to University-owned or managed information through computing systems or devices (including physical files containing payment card holder information) must report Information Security Incidents (as defined below) immediately per the procedures described in the Incident Management Procedures and Payment Card Industry (PCI) Incident Management Plan linked at the end of this document.

To protect Sensitive Information (as defined below) or Mission-Critical Resources (as defined below), the Information Security Office shall direct the incident response and investigation, in coordination and collaboration with the affected department(s). The Chief Information Security Officer and the Chief Information Officer have the authority to take any action appropriate to mitigate risk posed by any Information Security Incident. Information Technology Services (ITS) is entitled to obtain reimbursement of associated costs from appropriate department(s) relevant to incident investigation and resolution.

Purpose and Background

Protection of sensitive, University-owned information and Mission-Critical Resources of the University.

Audience

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

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 malicious disabling of a piece of hardware that endangers Mission-Critical Resources.

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

- **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 Resources 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

Please see the Incident Management Procedures document regarding specific procedures for reporting an incident. Please see the Payment Card Industry (PCI)

Incident Management Plan for details regarding any incident that involves risk to payment cards information.

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

  10/13/2015 Review only, CISO

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