UNC School of Dentistry Incident Management Plan

Introduction

Purpose of Policy
To establish how the SoD faculty, staff, students and related parties will handle Information Security Incidents, including protocol for reporting, responding, containing and restoring information.

Audience
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, including Users with access to Sensitive Information. Also, this applies to all UNC business units, including the School of Dentistry, that manage or subcontracts their information technology.

Definitions
1. Incident Management Plan – A plan established and maintained by the SoD 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.

2. Information Security Incident – Includes any incident that is known or has the potential to negatively impact the confidentiality, integrity, or availability of the SoD’s information. This can range from the loss of a laptop, smartphone or tablet, the virus infection of an end-user work station or a major intrusion by a hacker.

3. Mission-Critical Resource – Includes any resource that is critical to the mission of the SoD 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.

4. P2P – Peer-to-peer file sharing (P2P) allows users to download media files such as music, movies, and games using a P2P software client that searches for other connected computers. The "peers" are computer systems connected to each other through the Internet.

5. Sensitive Information: Sensitive Information includes all data, in its original and duplicate form as defined by the North Carolina Identity Theft Protection Act of 2005 and private health information (PHI) as defined by HIPPA Security and Privacy Standards.
UNC School of Dentistry Incident Management Plan

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.

6. Smartphone - A smartphone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone.

7. SoD email – University email used by SoD faculty and students. All SoD email is considered sensitive information.

8. SoD – UNC School of Dentistry

9. Tablet – A slate computing device which is a class of mobile computer (e.g. iPad, Android Pad, Kindle, Blackberry Playbook, Windows Slate PC, etc.) that accepts input from an electronic pen or finger input rather than from a keyboard.

10. UNC-ISO – The University Information Security Office. The University’s Information Security Office oversees the security of the University’s electronic information.

Policy

Policy Statement
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 promptly per the procedures described herein.

When deemed appropriate to protect Sensitive Information or Mission-Critical devices, the Information Security Office may, in coordination with the SoD, direct the incident response and investigation. The University’s Chief Information Security Officer (CISO) and Information Security Office (ISO) have 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).
UNC School of Dentistry Incident Management Plan

Compliance

Compliance Statement
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.

Procedures
OCIS is designated as the SoD organization responsible for creating and maintaining internal Processes and Procedures to govern and mitigate Incident Management

Incident Reporting
1. Every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus who has access to SoD-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 smartphone, tablet or laptop to the virus infection of an end-user work station or a major intrusion by a hacker) shall promptly contact the SoD Security Liaison (919-537-3485) or the IT Help Desk (919-962-4357) to report the Incident\(^1\).

2. If University equipment, such as a University-owned laptop or tablet, has been lost or stolen, then Public Safety shall also be notified at 919-962-8100.

---
\(^1\) The University IT Help Desk is available 24 hours a day, 7 days a week.
Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report a Violation</td>
<td>SoD Security Liaison</td>
<td>919-537-3485</td>
<td></td>
</tr>
</tbody>
</table>

Related Data

Policies
The following ITS Policies are incorporated by reference and made part of this Policy:

1. UNC-Chapel Hill Campus Standards for Electronic Media Disposal
2. University of North Carolina Network Acceptable Use Policy
3. E-Mail Address Policy
4. Incident Management Policy
5. Information Security Policy
6. Institutional Data Governance Policy
7. Password Policy for General Users
8. Transmission of Protected Health Information and Personal Identifying Information Policy
9. Vulnerability Management Policy
UNC School of Dentistry Incident Management Plan

Statutes

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 (PCI) Data Security Standard
6. UNC-Chapel Hill Data Network Acceptable Use Policy
7. The University of North Carolina at Chapel Hill Protocol for Responding to Security Breaches of Certain Identifying Information
8. Definition of Sensitive Information
9. UNC Incident Management Policy

Processes

1. OCIS Incident Management Process

Contacts

Questions

David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Violations

David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Consulting

OCIS Staff, 919-537-3485
UNC Help Desk, 919-962-4357
UNC Information Security Office, 919-445-9393

History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01/22/2015</td>
<td>TAD</td>
</tr>
</tbody>
</table>

Next Review Date: 01/21/2016

Authorization

Jane A. Weintraub, Dean, UNC School of Dentistry

Signature ________________________________

Date ________________________________
UNC School of Dentistry Incident Management Plan