**Data/Security Incident Management Plan**

1. **PURPOSE:** The purpose of the Information Security Incident Response Procedure is to

define the department’s procedures for handling 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. This procedure supplements the University’s Incident Management Policy.

2. **SCOPE:** This procedure applies to UNC Gillings School of Global Public Health hosted servers and Instructional and Information Systems employees that access/maintain the servers. A security incident includes any incident that is known or has

the potential to negatively impact the confidentiality, integrity, or availability of UNC-Chapel

Hill information.

3. **GENERAL:** Note: When there is an identifiable risk to sensitive information, departmental

personnel will issue a critical ticket to the ITS-Security Remedy group prior to performing any

system scanning or cleanup actions.

4. **PROCEDURES**

**Preparation Stage of Incident Management**

1. **Inventory** -- An inventory of systems that host/process/access sensitive data

or are critical to the university mission (sensitive/critical) will be maintained

2. **System Hardening, Profiling, and Backups** – Patches, backup, and logging will be maintained at the highest possible levels on all servers. Any situations that require an exception to the patch level management will be documented for said server.

3. **Vulnerability Management** – Qualys scans are maintained for all servers. Windows servers are connected to the WSUS server internal to campus and RedHat servers are connected to the RHN / Yum system to maintain patch levels. CLAMAV and Symantec are maintained on appropriate servers. SPLUNK alerts are set for various web intrusion checks.

4. **Communication protocol**

a. Primary contact for Linux servers is Marcus Summers. Primary contact for Windows servers is Caitlyn Hill. Primary contact for Oracle services is Tim Madden. Primary contact for Website services is Marcus Summers. Primary ISL is Bryan Andregg; Backup ISL is Caitlyn Hill. Lew Binkowski should be alerted as project manager for department.

b. All breaches identified by ISO, cujo, or external sources should be alerted to the IIS staff through Remedy or by calling the on-call cell phone provided to the ITS-CONTROL-CENTER

**Process:**

**Identification:**

1. Incident is identified
   1. Either we are informed by an external entity or internal investigation that there is unauthorized access or changes made to one of our servers
2. Affected system is removed from production/access
3. Incident is verified as to whether it impacts sensitive data

**Communication:**

1. Ticket is put into security in regards to the incident
2. **If the incident does impact sensitive data, all further activities must be coordinated through the ISO, to avoid compromising useful forensic data**
3. Department ISL and representative for the affected clients are alerted of the breech

**Actions**

1. If the incident does not impact sensitive data, steps are taken to identify:
   1. Impact
   2. Data loss concerns
   3. Related security compromises
   4. Exploit that allowed compromise
2. The exploit is discovered and closed
   1. If the exploit cannot be closed, evaluate alternative options for securing the system, such as changing VLANS, removing services, or altering services
3. All related passwords are changed
4. All impacted data is evaluated for changes
5. If necessary, the affected system is rebuilt from last known-good backup and the exploit is disabled before the system is brought back online
6. Fill out a post mortem for the incident, detailing the timeline, the steps taken to resolve the issue, and actions taken to prevent further incidents.