

RESEARCH. EDUCATION. HEALTHCARE. STATEWIDE.



# UMDNJ Information Security Plan

## 2007

# Table of Contents

- Table of Contents ..... 2
- Introduction..... 3
- Contact ..... 4
- Risk Assessment..... 5
- Plan Components ..... 6
  - Awareness..... 7
  - Policy and Procedure ..... 9
  - Security Enhancement ..... 10
  - Monitoring and Audit ..... 12
  - Enforcement ..... 14
  - Oversight ..... 15
- Timeline..... 16

## Introduction

In order to ensure the safety of University information and data, and to comply with a number of laws at the state and federal level, UMDNJ's Information Services and Technologies division along with the Office of Ethics and Compliance, and Internal audit have created an Information Security Plan. This plan responds to requirements established by the [Health Information Portability and Accountability Act \(HIPAA\)](#), the [Gramm-Leach-Bliley Act \(GLB\)](#), the [Family Educational Rights and Privacy Act \(FERPA\)](#), and others calling for the safeguarding of both sensitive information as defined by law, and information critical to the institution. The plan also recognizes that best practice in the area of information security will also continue to evolve and that the University will need to remain vigilant with regard to processes, behaviors, and tools, which can help to ensure a safe and secure environment.

Recognizing the distributed nature of UMDNJ's assets, locations, and functions, this plan places responsibilities for ensuring the protection of information at all levels and within all roles at the University. It is consistent with the University's [Sensitive Electronic Information Policy \(SEI\)](#) which designates anyone coming into possession of sensitive data as a "Data Custodian" having both rights and responsibilities associated with that role. However, recognizing that information security breaches can have a far-reaching impact on the University, the University's Information Security Officer will assume overall responsibility for the security of all network/computing assets, whether or not a part of the managed environment; and the University's Privacy & Security Officer will oversee compliance with established information security policies.

## **Contact**

Questions and comments regarding this plan can be directed to:

**Michael Clarke, Esq.**

**Vice President, Office of Ethics and Compliance**

**65 Bergen St, 13<sup>th</sup> Floor**

**Newark, NJ 07101**

**973-972-8094**

**James Rowan**

**Chief of Staff and Vice President, Internal Audit**

**65 Bergen St , 15<sup>th</sup> Floor**

**Newark, NJ 07101**

**973-972-4400**

**Wayne Thompson**

**Vice President Information Services & Technologies**

**65 Bergen St , 14<sup>th</sup> Floor**

**Newark, NJ 07101**

**973-972-3800**

## Risk Assessment

The University recognizes that some level of risk will always exist within the institution and that the challenge is to ensure that the level of risk does not exceed that required by law or that expected by the institution. Risks of unauthorized use of or access to Sensitive Information exist, including, but not limited to:

- Unauthorized access of Sensitive Information by someone other than the owner of the Sensitive Information
- Compromised system security as a result of system access by an unauthorized person
- Interception of Sensitive Information during transmission
- Loss of Sensitive Information integrity
- Physical loss of Sensitive Information in a disaster
- Physical loss/theft of Sensitive Information contained on portable media
- Errors introduced into the system
- Corruption of Sensitive Information or systems
- Unauthorized access of Sensitive Information by employees
- Unauthorized requests for Sensitive Information
- Unauthorized access to Sensitive Information through hardcopy files or reports
- Unauthorized transfer of Sensitive Information through third parties

The University recognizes that this list is not exhaustive. New risks of unauthorized use or access to Sensitive Information are created regularly because our information and the individuals who need access to it are constantly evolving. As a result, periodic monitoring of our environment forms a fundamental component of this plan.

## **Plan Components**

The key components of this plan include the following :

- Awareness
- Policy/Procedure
- Security Enhancement
- Monitoring/Audit
- Enforcement
- Oversight

Each of these areas is treated in its own section within the plan. These sections are subject to at least annual review, but may be altered more frequently if required via the process outlined in the oversight section of the document.

## **Awareness**

Components of this plan addressing awareness will include the following :

- An annual publication on information security jointly compiled by IST, the Office of Ethics & Compliance (OEC), Internal Audit, Administration, and Legal Services. The intent is to raise awareness by including tips, resources, policy excerpts, and perspectives from the participating entities. The publication will be made accessible to all electronically.
  - Publish first edition July 2007
- Periodic presentations to Deans, E/S/VPs, and CEOs at established forums, or special meetings.
  - Initial discussion of draft plan with Deans March 2007
  - Followup discussion Fall 2007
- A Website dedicated to Safe Computing
  - Revise/enhance existing website and deploy in my.umdj.edu
- Posters placed strategically throughout the University when deemed appropriate.
  - Develop new poster
  - Replace remaining HIPAA posters.
- Inclusion of selected information security content within orientation materials.
  - Analyze existing content
  - Revise/replace materials
- Periodic emphasis by the President and chief executives.

- Meet with incoming president and review plan
  - Develop message
- Recurring training classes for faculty staff and students.
  - Replace training staff member
  - Develop curriculum and schedule
- Conduct periodic assessments of awareness
  - Create an information security awareness web survey
  - Conduct initial survey in FY2008

## ***Policy and Procedure***

The University conducts an annual review of policy, and it is expected that desired or required changes in the area of information security will follow that process. It is recognized that individual units may need to create or adjust their own policies and procedures accordingly. Initially, our University policies in this area will be adjusted so that there is a discreet section or standalone policy to cover the areas below. Other relevant policy areas such as 3<sup>rd</sup> Party access, Authorization, and any new policy areas will be addressed in ongoing review of this arena :

- Sensitive Electronic Information (SEI), including the proper use and security of portable media
  - Complete review of SEI policy with the Privacy & Security Officer
- Access Management
  - Joint task force with HR and OEC to review procedures for staff transfer and termination
- Risk Remediation
  - Develop draft policy and review with IST Governance committees
- Server Creation
  - Develop draft policy and review with IST Governance committees

## ***Security Enhancement***

The University recognizes that regulatory requirements, accreditation requirements, best practice, and threats, will continue to evolve. As such, enhancements to security will be an ongoing need. Initially, our efforts will concentrate on the following areas :

- Ensuring appropriate perimeter protections
  - Hire analyst for proactive management of intrusion detection/prevention systems
  - Apply additional rule restrictions to the Tipping Point Intrusion Protection System and the Firewall Rules Base
  - Implement the Security Information Management System (SIMS) and begin to correlate event log data captured at our perimeter firewalls
- Ensuring that access to resources requires strong and current credentials
  - Review systems where strong passwords are not possible and discuss solutions with vendors
- Application of best practices as identified by industry organizations such as Educause, and AAMC
  - Collect white papers and research available and distribute to IST Governance
- Maintaining staff with appropriate skills and certifications
  - Identify staff roles where certifications are essential
  - Create staff development plans as appropriate

- Ensuring the availability and use of threat protection tools for all UMDNJ assets
  - Increase awareness of available Anti-Virus and threat-protection tools
  - Use monitoring tools to identify and report deficiencies
  - Increase the percentage of machines that are in the fully managed environment where prudent
  - Explore the feasibility of deploying data encryption technology
- Establishing interim Data Center Space, and the launch of the long term solution for Data Center space
  - Establish interim solution
  - Build long term solution

## ***Monitoring and Audit***

The University recognizes that ongoing monitoring and audit of our network/computing assets, whether or not a part of the managed environment, is essential for both operational reasons, and to satisfy regulatory and audit requirements. Monitoring can also allow the University to be proactive in the identification and prevention of threats. Routine audit of the environment is an expectation of annual internal and external audit functions. Initially, our efforts will concentrate on the following areas :

- Utilizing existing tools to monitor external threats
  - Hire Analyst to monitor and act on output from University-level Tipping Point
  - Deploy additional Tipping Point appliances for healthcare entities eg: UBHC
- Deployment of enhanced tools to monitor internal threats
  - Deployment of Core Impact software
  - Use of Nessus for targeted monitoring/assessment
- Monitoring outbound traffic/utilization and providing reports to management
  - Implement Surf Control and deploy intuitive filters
  - Define standard reports and begin distribution
- Periodically scanning the environment for risks
  - Quarterly scan of UMDNJ network
  - Periodic 3<sup>rd</sup> party penetration audits

- Focused scanning of new assets and suspected problem areas
  - Utilize Core Impact and Nessus for new servers and audit/compliance issues
- Deployment of a Security Information Management system (SIMS)
  - Purchase SIMS
  - Hire SIMS Analyst
  - Deploy SIMS

## ***Enforcement***

The University recognizes that different levels of risk demand different levels of enforcement and penalty. Accordingly, our efforts will concentrate on the following areas :

- Define security risk classifications
  - Procure Gartner reference materials
- Risk-based response to violations
  - Highest risk accounts or devices will be disabled and referred for possible further actions
  - Moderate risk accounts or devices will be disabled and referred for possible further action if not remediated within prescribed time periods
  - Low risk accounts or devices will be identified on reports to the owner/administrator with requested remediated within prescribed time periods
- Pre-Emptive Tools
  - Increase awareness of existing data encryption tools
  - Ensure maximum prudent usage of the fully managed environment
  - Deploy monitoring agents on servers

## ***Oversight***

The Information Security Plan will be administered by the Information Security Officer and the Privacy & Security Officer. Changes to the plan, and quarterly reports on progress will be submitted to IST Governance Committees and Executive Leadership for review and approval.

