

IT Security

Information Technology Systems and Services

Information Technology Security Office (ITSO) Implementation Plan

DRAFT

Brad Miller
IT Security Officer
October 20, 2005

IT Security

Information Technology Systems and Services

I. Introduction

1. This document will outline the Information Technology Security Office's implementation plan for meeting its objectives.
2. The objectives stem from the ITSO mission:
 - To work with the entire UND community to protect the confidentiality, integrity, and availability of our critical information and computer resources.
 - To implement and advance secure computing practices with sensitivity to UND's educational environment which promotes academic and intellectual freedom, diversity, privacy, and individual rights.
3. Sections II-VI provide the detail plan for the six main objectives the ITSO will strive to accomplish. These objectives are:
 - 3.1. **Security Policy, Guidelines, and Procedures**

The ITSO will work with the UND and NDUS community to recommend, develop, communicate, and implement IT security policies, guidelines and procedures.
 - 3.2. **Security Assessment/Risk Analysis**

The ITSO will work with the UND community to identify and document the information and information systems critical to UND's operation, identify threats and vulnerabilities, and develop and implement plans to minimize the risk to these systems.
 - 3.3. **Federal and State Regulation Compliance**

The ITSO will work in cooperation with the UND community and the appropriate campus compliance and safeguarding committees to provide information technology expertise in the effort to ensure compliance with all applicable Federal and State laws governing access to personal information, integrity of financial and health data, and copyright protections.
 - 3.4. **Security Education, Training, and Awareness**

The ITSO will provide information technology security information and training to users. The ITSO will promote personal responsibility for securing data and IT resources and foster a community partnership for the exchange of knowledge and information.
 - 3.5. **Incident Response**

The ITSO will work with the UND Security Incident Response Team (SIRT) to provide assistance in responding to incidents when requested. The ITSO will track incidents to be used for measuring IT security program effectiveness and to develop summary reports on the number and kind of incidents affecting UND.

IT Security

Information Technology Systems and Services

II. Security Policy, Guidelines, and Procedures

The ITSO will work with the UND and NDUS community to recommend, develop, communicate, and implement IT security policies, guidelines and procedures.

1. IT security policies and guidelines are implemented at UND in the interests of the entire community – to communicate to all users the kinds of actions that can help or hinder the availability and reliability of IT resources supporting UND's academic mission.
2. The ITSO will be responsible for developing policy, guidelines, and procedures.
 - 2.1. *Policy.* A policy is a statement of institutional direction. Adherence to a policy is expected.
 - 2.2. *Guideline.* A guideline is a statement of proposed direction. Adherence to a guideline is recommended.
 - 2.3. *Procedure.* A procedure is a plan describing how to accomplish a security task or reach a goal.
3. *Identify needs and priorities.* In order to develop effective IT security policies, guidelines, and procedures, the first step is to determine the needs and priorities of the university. This is an ongoing process dictated by campus and ITSS priorities and initiatives as well as in response to Security Assessment/Risk Analysis activities.
 - 3.1. Based on an initial assessment of the current environment, it is a priority to create a policy or guideline for the following:
 - 3.1.1. UND Student Acceptable Use
 - 3.1.2. UND Faculty/Staff Acceptable Use
 - 3.1.3. User Account/Passwords
 - 3.1.4. Host (Desktop and Server) Security
 - 3.1.5. Server Security
 - 3.1.6. Email Usage
 - 3.1.7. Wireless Security
 - 3.2. Based on an initial assessment of the current environment, it is a priority to create a procedure for the following:
 - 3.2.1. Incident Response
 - 3.3. Additional policies, guidelines and/or procedures could be developed for the following:
 - 3.3.1. Patch Management
 - 3.3.2. Blocking Network Access
 - 3.3.3. Use of Copyright Material
 - 3.3.4. Web/Internet
 - 3.3.5. Data Protection
 - 3.3.6. Network Infrastructure
 - 3.3.7. Network Protocol
 - 3.3.8. Network Bandwidth
 - 3.3.9. Firewall
 - 3.3.10. Remote Access

IT Security

Information Technology Systems and Services

- 3.3.11. DNS
 - 3.3.12. Physical Security
 - 3.3.13. Intellectual Property
 - 3.3.14. Mobile/Blackberry
 - 3.3.15. Guest Accounts
 - 3.3.16. Backup/Tape Retrieval
 - 3.3.17. Disaster Recovery
 - 3.3.18. Residence Hall Usage
 - 3.3.19. Surplus Equipment Disposal
4. *Development.* After determining priorities, policies should be created by using the following procedures:
- 4.1. A notice will be posted on the [IT Security Policy web site](#) to communicate that a policy or guideline will be created on a particular topic.
 - 4.2. For each proposed policy, the ITSO will assemble a group of Subject Matter Experts (SMEs). This group will meet face-to-face as needed, but development will primarily be done through correspondence. This group will have the following responsibilities:
 - 4.2.1. Identify the key issues and what to include in the policy/guideline.
 - 4.2.2. Determine what is most appropriate for the particular issue: a policy or a guideline.
 - 4.2.3. Collaborate to draft the language of the document.
 - 4.3. The draft document will be sent to a specific group of campus individuals for a two week review period to solicit comments. This list will include (but is not limited to):
 - 4.3.1. UITC
 - 4.3.2. Office of General Counsel
 - 4.3.3. Audit Office
 - 4.3.4. Campus IT Managers/System Administrators
 - 4.3.5. Student Services
 - 4.3.6. Office of Student Government
 - 4.3.7. Dean's Council
 - 4.4. The ITSO and SMEs will review any comments and, if necessary, modify the draft document.
 - 4.5. A copy of the draft document will then be posted on the [IT Security Policy web site](#) for one month for all members of the UND community to provide comments.
 - 4.6. If comments are not received within the above timeframes, acceptance will be assumed.
 - 4.7. The ITSO and SMEs will review any additional comments and prepare a "final" draft document.
5. *Publishing.* This strategic and political process is necessary to give legitimacy to the suggested policy or guideline.

IT Security

Information Technology Systems and Services

- 5.1. The IT Security Officer will present the “final” draft document to the University Information Technology Council (UITC) for their input and recommendations. According to UITC recommendations, a policy will be submitted to UND’s President and cabinet for approval. Guidelines recommended by the UITC will be released immediately to the campus community.
6. *Education and Awareness.* A policy or guideline is only effective if people are aware of it.
 - 6.1. The IT Security Officer will be responsible for distributing the new policy or guideline through a developed education and awareness program ([see section V](#)).
 - 6.2. Policies and guidelines will be available on the [IT Security Policy web site](#) and will be identified as “in development”, “draft”, “published”, and “under review”.
7. *Measuring Effectiveness and Adherence.* It will be necessary to develop a plan to periodically update and review the relevance of existing policies and guidance documents. Also, some measures need to be in place to monitor compliance and determine if the policy is having the desired effect.
 - 7.1. The IT Security Officer and SMEs will be responsible for setting a review date of each policy/guideline based on the sensitivity and changing nature of the issue. The ITSO will post the review schedule for each policy and guideline on the [IT Security Policy web site](#).
 - 7.2. The IT Security Officer will develop metrics (i.e., incidents, number of compromised systems, periodic audits, etc.) to measure the effectiveness of each policy/guidance.
 - 7.3. The IT Security Officer will develop procedures to periodically audit compliance to existing policy/guidance documents.

IT Security

Information Technology Systems and Services

III. Security Assessment/Risk Analysis

The ITSO will work with the UND community to identify and document the information and information systems critical to UND's operation, identify threats and vulnerabilities, and develop and implement plans to minimize the risk to these systems.

1. Conducting a security assessment and risk analysis of UND's current information systems environment is quite possibly the most critical effort to be undertaken by the IT Security Office. This process will not only assist the IT Security Office in its effort to protect critical systems and data, but will provide individual departments and the institution as a whole with invaluable insight into the risks to our critical systems and how those risks can be mitigated or even eliminated.
2. There are a number of potential options to properly conduct a security assessment/risk analysis. The main options are:
 - a) Use a highly collaborative, subjective method such as OCTAVE or STAR. These models involve such things as setting up committees and conducting multiple workshops with various groups across campus to collaborate and prioritize critical systems, identify threats and vulnerabilities, and recommend controls to mitigate security risks.
 - Pros:
 - Promotes an open discussion across campus which encourages IT security awareness and a "know thyself" outlook.
 - Since more people (and more time of those people) are required, individuals will have a greater sense of ownership and will be more committed to the effort.
 - Little or no upfront costs.
 - Cons:
 - Very labor intensive – requires a lot of time of individuals to participate in collaborative meetings.
 - Very subjective in nature – relies on the individuals opinions (i.e., "What do you think is most critical?", or "What do you think should be done to minimize this security vulnerability?")
 - Relies heavily on paper (spreadsheets, note takers, etc.). This makes analysis and follow up assessments more difficult and labor intensive
 - b) Use a collaborative method complemented by an objective third-party risk assessment software package such as RSAM, CounterMeasures, or Riskwatch. This model would involve creating a steering committee to guide the effort, but would use a third-party software package to conduct web-based surveys and to make standards-based (ISO, NIST, HIPAA, and/or GLBA) recommendations for controls to mitigate security risks.

IT Security

Information Technology Systems and Services

Pros:

- Using a software package requires much less labor and time commitment to implement – surveys are much easier for the surveyee to complete.
- Turn-around time for assessments will be quicker.
- Provides an objective, standards-based approach to evaluate security posture. (Instead of relying on subjective opinions, it asks questions like “What type of data does this system process?” and then determines criticality based on this systematic approach)
- Stores assessments in a database which can be analyzed, backed up, and used for future assessments and benchmarking.

Cons:

- Expense – most software packages run \$10-15K
- Due to the less collaborative nature of this type of assessment, there will be less commitment and ownership of the process.

- c) Outsource the security/vulnerability assessment. Contract a “white hat” vendor to conduct an internal assessment (interviews, processes, etc.) as well as vulnerability and penetration testing.

Pros:

- The least amount of labor and time commitment to implement (with the exception of the ITSO who must coordinate)
- This should provide the quickest turn-around time for an assessment.
- External assessors with an external outlook can bring credibility (or perceived credibility) that an internal assessment can not.

Cons:

- The most expensive option - \$50K+
- One time snapshot – have to pay each time an assessment is done.
- This is the least collaborative type of assessment. There will be less commitment and ownership of the process and follow up actions.

3. The recommendation of the ITSO is to start working towards option b. A “proof of concept” of this method could start with a small assessment of a critical system within ITSS. This would involve:

1. *Forming a committee.* A small committee (3-4 individuals) with a blend of management and technical people. This committee will select the critical system(s) to be evaluated, identify individuals to survey, and select survey components.

IT Security

Information Technology Systems and Services

2. *Configuring software package.* This will mostly be done by the ITSO, but may require technical assistance within ITSS to set up software on a server and implement web-based surveys.
 3. *Survey Individuals.* Use the web survey engine to survey key individuals
 4. *Technical Assessment (tentative).* Possibly use Nessus vulnerability scanner on critical system(s) to identify vulnerabilities to include in the final report.
 5. *Present results.* Use the software to generate reports and recommendations and present the results to committee and ITSS management.
-
4. If the “proof of concept” assessment goes well, the plan would be to create a long-term plan to roll this out campus-wide. The plan would include how to roll it out, i.e. one department at a time or campus-wide assessment, the timeline for conducting assessments, and how to secure the funding.
 5. Assessing the security of our critical systems is not intended to be a one-time “snapshot” of our organizational risks. This should be an on-going process with periodic reviews (possibly bi-annually) to identify changing assets, threats, and vulnerabilities.

DRAFT

IT Security

Information Technology Systems and Services

IV. Federal and State Regulation Compliance

The ITSO will work in cooperation with the UND community and the appropriate campus compliance and safeguarding committees to provide information technology expertise in the effort to ensure compliance with all applicable Federal and State laws governing access to personal information, integrity of financial and health data, and copyright protections.

1. Failure to take the necessary steps to comply with Federal and State Regulations such as FERPA, HIPAA, and GLBA could lead to an incident which may result in legal liability for negligent security as well as heavy, negative publicity which could damage the universities reputation. Management must understand the status of efforts to protect critical information and be given reassurance that the university is taking the appropriate steps to secure this information.
2. The ITSO will provide guidance and IT expertise in the effort to secure our critical data and bring our practices and systems into compliance.
 - 2.1. The ITSO will make contact with existing campus HIPAA, GLBA, and FERPA safeguarding committees (where they exist) to join and re-energize compliance efforts. The ITSO will provide IT security expertise and make recommendations to these committees as necessary. Where an organized committee or group does not exist, the ITSO will make an effort to identify and organize individuals who have a common interest in compliance issues related to a given regulation.
 - 2.2. During the Security Assessment ([see section III](#)), the ITSO will identify and make appropriate groups and individuals aware of any practices or systems which are not in compliance with HIPAA, GLBA, and/or FERPA regulations.

IT Security

Information Technology Systems and Services

V. Security Education, Training, and Awareness

The ITSO will provide information technology security information and training to users. The ITSO will promote personal responsibility for securing data and IT resources and foster a community partnership for the exchange of knowledge and information.

1. The UND ITSO supports the concept that “Security is everyone’s job”. Statistics consistently show that (1) the majority of security breaches are caused by or could have been prevented by insiders to the organization, often end-users, and (2) external attacks are increasingly targeting end-user systems.
2. Having a diverse education and awareness program is a critical component in protecting UND’s IT systems and infrastructure. Awareness should be multi-faceted to target various audiences within the university; including administration, faculty/staff, students, and IT staff.
3. The ITSO will solicit input from departmental system administrators and their supervisors in order to improve the security awareness program.
4. Below are some initial steps the ITSO will implement as part of an ongoing awareness program.
 - 4.1. IT Security website – creating of an IT Security website is critical to information sharing as it will give the ITSO a portal for sharing security policies, guidelines, initiatives, and security alerts. The ITSO will create a website and provide up-to-date and useful information to the UND community. The website will be at <http://itsecurity.und.edu> – the tentative plan can be viewed in [Appendix A](#).
 - 4.2. S.P.E.A.R.Head program– the ITSO would assemble a diverse group of technical and non-technical individuals who have an interest in IT security and could help promote security awareness in their departments. This group would be a dissemination point for awareness articles, new policies, and other information. They could also provide input and feedback to the IT Security Awareness program. The ITSO will get together with this group periodically to provide training and awareness.
 - 4.3. IT Security training module – this would most likely be a PowerPoint presentation on basic IT Security principles. It could be shared by the ITSO or others at such forums as the Intro to University Life class, student/faculty orientation, summer Getting Started program, etc.
 - 4.4. IT Security lecture series – this would be a program where the ITSO would bring in experts in IT Security to lecture to students, faculty and staff.
 - 4.5. Periodic one-on-one visits with managers – it is important for the ITSO to remain visible with department managers and leaders on campus. Periodic face-to-face visits to discuss current initiatives and address concerns would be appropriate.
 - 4.6. Acceptable Use brochures
 - 4.7. IT Security Videos
 - 4.8. UND-IT-Security mailing list

IT Security

Information Technology Systems and Services

VI. Incident Response

The ITSO will work with the UND Security Incident Response Team (SIRT) to provide assistance in responding to incidents when requested. The ITSO will track incidents to be used for measuring IT security program effectiveness and to develop summary reports on the number and kind of incidents affecting UND.

1. The UND ITSO will not be the responsible person for incident response and handling. This responsibility will remain with the UND SIRT. The ITSO will assist in responding to incidents and helping with investigations when requested by the UND SIRT team. This will usually be in response to a major incident and will involve providing oversight and communicating the incident and response efforts.
2. The UND ITSO will assist in creating policy and procedures for handling incidents in a consistent manner. The ITSO will also track and monitor incidents to be used for measuring the effectiveness of various IT Security policies, guidelines and initiatives, and to develop summary reports on the number and kinds of incidents affecting UND.

DRAFT

IT Security

Information Technology Systems and Services

Appendix A. Website Information Plan ***(<http://itsecurity.und.edu>)***

- 1) About IT Security**
 - a) Vision, plan, contact info, etc
- 2) Virus/Worm info**
 - a) Top viruses
 - b) Latest viruses outbreak
 - c) Anti-virus software download links
- 3) Spyware info**
 - a) How to prevent
 - b) Software download links
- 4) Phishing/Identity theft info**
 - a) How to prevent
- 5) Policy documents**
 - a) Policy
 - b) Guidance
 - c) Best practices
- 6) Announcements**
- 7) Awareness**
 - a) Articles, cartoons, seminars
- 8) Minimum steps to protect your computer**
- 9) Minimum steps to protect your Data – file transfer, encryption, backups, email, secure web**
- 10) Minimum steps to protect yourself**
- 11) File sharing and copyright links**
- 12) Incident Reporting procedures**
- 13) Statistics – virus/network incidents**
- 14) How-to-guides**
- 15) Tools**