

Information Security Plan for the College of Information Technology at UNC Charlotte

Nov. 2000

1 Objective and scope of the plan

The objective of this document is to outline the information security plan for the College of Information Technology. Information security refers to the confidentiality, integrity, and availability of information and information systems.

This plan will be focused on the information security needs for activities within the College of Information Technology (COIT). Our plan is consistent with the overall university plan for information security and this information security plan has been developed in consultation with the university's chief information security officer. The scope of this plan specifically focuses on the following areas:

- Student academic information kept at COIT
- Student employment information kept at COIT
- Online COIT information
- Faculty and staff personnel information kept at COIT
- COIT financial information, including financial information on grants and contracts of COIT faculty and staff
- Distance education programs
- Computing and communication infrastructure that support the computing needs of COIT.

An important note is that at the present time faculty and student use one of the two possible email systems: one supported by the university computing services, or another email system supported by the college of engineering. Therefore, this plan does not address the security of email servers.

This plan does not address the risks associated with the theft of computing and communication equipment.

2 Review, update, and implementation of the plan

The Dean of the COIT is ultimately responsible for information security in COIT. The person who is responsible to coordinate the planning, design, and implementation of information security within COIT is the director of the Laboratory for Information Integration, Security, and Privacy (LIISP), here after referred to as the LIISP director. This plan needs to be reviewed at least once every academic year and updated when necessary. Working closely with the faculty of COIT and the LIISP director, the Dean of COIT is responsible for making sure that resources are available to practically implement information security within COIT according to the plans.

The computing staff of COIT is charged with the responsibility of implementing this plan for those computing and communication resources that are maintained by COIT. This plan serves as a guideline to those computing and communication resources, maintained by research labs within COIT.

For each major system operated and maintained by COIT, an information security plan that governs the management controls, operational controls, and technical controls of such a system may be warranted. The LIISP director will make recommendations of the specific systems for which such a plan is needed. Information security plans for specific systems need to address the issues outlined in this plan.

3 Management controls

In this section, we describe the management control measures that are intended to meet the security requirements of COIT. Management controls focus on the management of the computer security system and the management of risk for a system. Technical and operational controls (to be discussed in sections 4 and 5) support management controls. To be effective, these controls all must interrelate.

3.1 Risk assessment and management

The following risks have been identified and will guide the development of the information security plan:

- Unauthorized access to student academic information kept at COIT
- Unauthorized access to student employment information kept at COIT
- Unauthorized deletion/modification/addition of online COIT information
- Unauthorized access to faculty and staff personnel information kept at COIT
- Unauthorized access to COIT financial information, including financial information of grants and contracts of COIT faculty and staff
- Denial of service attacks against computing and communication infrastructure that support the computing needs of COIT
- COIT resources used by malicious users to launch denial of service attacks.

As the activities of COIT evolves, information security risks also will change. The LIISP director is responsible for coordinating reviews of the information security risks as part of the plan review and update process described in section 2.

3.2 Rules of Behavior

The use of computing and communication resources at COIT by faculty, staff, and students are governed by the appropriate policy as prescribed by the University of North Carolina at Charlotte.

3.3 Planning for security in life cycle

3.3.1 Initiation phase

When planning for the acquisition/development of any information system, information security risks must be assessed against the risks identified in this plan. For equipment to be purchased by COIT, such an assessment along with possible mitigation mechanisms, may be mandated by the equipment committee as part of the proposal to purchase, upon recommendation from the LIISP director.

3.3.2 Development/acquisition phase

During the development/acquisition phase, mechanisms to mitigate identified security risks must be fully considered. Among the questions that should be addressed are the following:

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g. Request for Proposals) include security requirements and evaluation /test procedures?
- Did the requirement permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

3.3.3 Implementation

During the implementation phase, the system's security features should be configured and enabled, the system should be tested and installed or fielded. A design review should be conducted. Among the questions that should be addressed are the following:

- Were design reviews and system tests run prior to placing the system in production? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable laws, regulations, policies, standards, and guidelines?

3.3.4 Operations/Maintenance phase

During the operation/maintenance phase, the system is almost always being continuously modified by the addition of hardware and software and by numerous other events. If the system is undergoing modifications, determine which phase of the life cycle the system modifications are in and describe the security activities conducted or planned for in that part of the system.

Each major information system, as determined by the LIISP director, operated and maintained by COIT should have an information security plan. The following high-level items should be described:

Security Operations and Administration Operation of a system may involve many security activities. Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples.

Operational Assurance Operational assurance examines whether a system is operated according to its current security requirements. This includes both the actions of people who operate or use the system and the functioning of technical controls. The LIISP director will coordinate the operational assurance process.

Audits and Monitoring The security plan must specify appropriate audit and monitoring measures.

3.3.5 Disposal phase

When computing resources are disposed. The operator of this resource must certify, in writing, that any sensitive information (e.g. those identified by this plan) has been destroyed.

3.3.6 Authorization processing

Below are the minimum-security controls that must be in place prior to authorizing a system for use. The levels of controls should be consistent with the level of sensitivity the system contains. These controls include

- Technical and/or security evaluations complete
- Risk assessment conducted
- Rules of behavior established and communicated to the users
- Contingency plan developed and tested
- Security plan developed, updated, and reviewed
- System meets all applicable laws, regulations, policies, standards, guidelines
- In-place and planned security safeguards appear to be adequate and appropriate for the systems
- In-place safeguards are operating as intended.

4 Operational controls

The operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or a group of systems). They often require technical or specialized expertise – and often rely upon management controls as well as technical controls.

4.1 Personnel security

In accordance to university policies, the COIT should make sure that user accounts and access authorities are granted appropriately. Among the questions that should be addressed by specific information systems are the following:

- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

4.2 Information back up and recovery

College of Engineering, with the collaboration of COIT, will provide back up services of the main file system (currently the Mosaic file system). It is also responsible for the recovery of data when necessary. It is the long term objective of COIT that the main file system and its back up system will reside in different physical buildings to minimize the risk of loss data due to physical environment damages.

All COIT users are encouraged to use the main file system for storage and/or back up of information. A complete security plan for the main file system will be completed in the near future coordinated by the director of LIISP.

4.3 System software update controls

Failure to timely update system software (e.g. operating systems, web servers) is one of the most common reasons for security breaches. The LIISP director shall make recommendations to the COIT IT staff to maintain a list of the critical software infrastructure components, their versions and the latest updates applied. Working in conjunction with the Computing Service, project Mosaic, and the Laboratory of Information Integration, Security, and Privacy, there should be a regular review of this list and apply the necessary upgrades and/or reconfigurations based on the latest information available (e.g. the data base of software vulnerabilities maintained by the National Institute of Standards and Technology).

4.4 Physical and environmental protection

Access control

Servers (including file servers and their storage devices, web servers, and application servers) will be housed in designated room with restricted access. The LIISP director will make sure that a process for making specific access control decisions is in place. The dean's office will help maintaining a list of those with key access to server rooms. Reviews of the access list and access control policies shall be performed at least once a year.

Fire and building safety factors

COIT will adopt the university's fire and building safety codes for housing computer and communication equipments.

4.5 Contingency planning

In close collaboration with the university's computing services, COIT will develop, in the near future a contingency plan that will permit COIT to continue essential functions if information technology support is interrupted. Such a plan should describe procedures that would be followed to ensure basic IT services if the supporting IT systems were unavailable.

- Are tested contingency plans in place to permit continuity of mission-critical functions (e.g. recovery of essential data) in the event of a catastrophic event?
- Are tested disaster recovery plans in place for all supporting IT systems and networks?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

The contingency plan must include descriptions of the following controls:

- Any agreement for backup processing?
- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup)
- Location of stored backups
- Generations of backups kept
- Coverage of back up procedures (e.g. what is being backed up).

4.6 Data integrity / validation controls

Data integrity controls are used to protect data from accidental or malicious alternation or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

The university computing service is responsible for the first line of defense again email viruses. All faculty and students are encouraged to install and update virus detection software.

4.7 Security Awareness and training

Security awareness programs are the most effective mechanism to protect COIT's sensitive information as much of the information will be under the control of faculty, staff, and students. The Laboratory for Information Integration, Security, and Privacy (LIISP) will be primarily responsible for coordinating information security awareness programs for COIT. Currently, the following types of programs are available

Self-protection resources

LIISP will maintain a live links to information resources about practical techniques to practice self-defense against common attacks in a campus setting. This information shall be made available through <http://www.sis.uncc.edu/LIISP>.

Security awareness lectures and demos

This lecture series will be presented at least twice every semester. Each lecture will highlight at least one major technique that can be used to protect information resources from unauthorized access or attacks. All lecture materials will be made available through the LIISP site.

UNC Charlotte Symposium on Information Security and Privacy

This bi-annual symposium will feature invited speakers and LIISP personnel to spot light research developments in information security and privacy. LIISP will also solicit active participation of this event by the local information security professional community. All symposium material will be made available through the LIISP site.

5 Technical controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within COIT.

5.1 Identification

Identification is the means by which a user provides a claimed identity to the system. COIT will use user ID to identify individuals.

Unique identification

Each faculty, staff, and student in COIT will have a unique user id, corresponding to the mosaic Kerberos login. COIT should work with all other related campus organizations to work towards a system where each UNC Charlotte user will have a unique user id.

Maintenance of User ID

The assignment of user ID is being tied to the personnel processes within the university. Specifically, only active employees should be assigned a user id. Only registered students will be assigned user id for the semester they have registered. Under the following situations a COIT faculty member can sponsor an individual to have a COIT user id:

- Students working on COIT computers for their program-related work, in that case, the user id shall be restricted to the particular summer session
- Visitors sponsored by a faculty member, the user id must be granted only for the duration of visit
- COIT alumnus may be assigned a user id for up to one year after his/her graduation.

Inactive user ids

User ids that are inactive on the system for longer than a year shall be removed.

5.2 Authentication

Authentication is the means of establishing the validity of a user's claimed identity to the system. Currently COIT uses password authentication. Kerberos is being used as the authentication mechanism for AFS as well as most NT systems. COIT should work closely with other units on campus to work toward a campus wide single-sign-on authentication system for all academic computing resources.

As part of the user awareness program discussed earlier, all COIT users should be educated with the proper choice and maintenance of passwords. COIT staff should do everything possible to prevent possible automatic password cracking attacks.

With the help of LIISP, COIT should work with the appropriate units on campus to review the policy and mechanisms used to assign initial passwords and make recommendations to the campus wide community.

5.3 Logical access control

Logical access controls include authorization and access controls. The primary access control mechanism used by COIT is based on operating systems and file servers. The responsibility to enforce access control relies mainly on those who administer the systems. Well defined access control policies and mechanism will be documented for those systems that are administered by COIT IT staff. Through the security awareness series, COIT will help all administrators to be more effective in protection COIT information resources from malicious attacks.

5.4 Public access control

COIT web server's provide the main public access point for COIT information. Maintaining the integrity of information served by COIT web servers is one of the most important information security objectives of COIT. The web server will be under the direct control of COIT IT staff .

COIT provides anonymous ftp service for publicly available information.

COIT also supports access by remote (including mobile) systems to gain access to its computing resources through the following protocols: telnet, ftp, smtp, imap, http, https, and gopher. Password authentication is the primary mechanism to enforce access control.

5.5 Audit trails

Working with COIT IT staff, the LIISP director will determine the type of audit trails that need to be maintained for different COIT systems and the appropriate monitoring mechanisms.