
**INFORMATION
TECHNOLOGY
SECURITY PLAN**

COLLEGE OF ENGINEERING

SEPTEMBER 30, 2003

Information Technology Security Plan

College of Engineering

This page intentionally left blank.

Information Technology Security Plan

College of Engineering

Table of Contents

1	Scope.....	1
2	Responsible Personnel.....	1
2.1	College IT Security Officer.....	1
2.2	College IT Security Manager.....	2
2.3	Unit Information Technology Security Managers.....	2
2.4	Notification.....	2
3	Unit Plans	3
3.1	Requirement	3
3.2	Mandatory Topics	3
3.2.1	Plan Title	3
3.2.2	Plan Scope.....	3
3.2.3	Responsible Personnel.....	4
3.2.4	Inventory and Network Diagram.....	4
3.2.5	Host and User Identification.....	5
3.2.6	Management Responsibility.....	5
3.2.7	Optional Topics.....	5
4	Critical Resources.....	5
5	Servers.....	6
5.1	General.....	6
5.2	Official Information Servers.....	7
5.3	Support Servers.....	7
5.4	Personal Servers.....	7
5.5	Student Organization Servers	8
5.5.1	Use Discouraged.....	8
5.5.2	Discretionary Permission.....	8
5.5.3	Time Limited Authorization.....	8

Information Technology Security Plan

College of Engineering

6	E-Commerce Systems.....	8
6.1	General.....	8
6.2	Registration.....	9
7	Data Management and Security.....	9
7.1	Classification.....	9
7.2	Student Records	10
7.2.1	Confidentiality.....	10
7.2.2	Security.....	10
7.3	Record Retention.....	11
7.4	Public Records	12
8	Email Management.....	12
8.1	Scope.....	12
8.2	Retention.....	13
8.3	User Authentication.....	13
8.4	Encryption.....	13
9	Network Infrastructure and Access Control.....	14
9.1	General Security	14
9.2	Managed vs. Unmanaged Hosts	14
9.3	User Authentication.....	15
9.4	Infrastructure	16
9.4.1	Physical Plant	16
9.4.2	DHCP Servers	16
9.4.3	VPN Servers.....	17
9.4.3.1	Authorization Required.....	17
9.4.3.2	Coordination.....	17
9.4.3.4	Logging Required.....	18
9.4.3.5	Maintenance Precautions.....	18
9.4.4	Inbound Modems	18
9.4.4.1	Authorization Required.....	19

Information Technology Security Plan

College of Engineering

9.4.4.2	Coordination.....	19
9.4.4.3	Authentication Required.....	19
9.4.4.4	Logging Required.....	19
9.4.5	Wireless Access Points.....	19
9.4.5.1	Authorization Required.....	20
9.4.5.2	Coordination.....	20
9.4.5.3	Authentication Required.....	20
9.4.5.4	Encryption Encouraged.....	21
9.4.5.5	Logging Required.....	21
10	Standard Procedures.....	21
10.1	Incident Response.....	21
10.2	User Workstations.....	22
10.2.1	Critical Patches and Updates.....	22
10.2.2	Virus Protection.....	22
10.2.3	Responsibility.....	22
10.3	Business Resumption Plan.....	23
10.4	Logon Banners.....	23
10.5	Intrusion Detection and Monitoring.....	24
10.5.1	Intrusion Detection Systems.....	24
10.5.2	Filesystem Signature Tools.....	24
10.5.3	Log Reviews.....	24
10.6	Transfer of Authority.....	24
10.7	Vulnerability Scans.....	25
10.8	Software Development Standards.....	25
11	Training.....	26
12	Physical Security.....	27
12.1	General.....	27
12.2	Facilities.....	27
12.2.1	Key Locks.....	27

Information Technology Security Plan

College of Engineering

12.2.2	Environmental Control	27
12.3	Servers.....	28
12.4	Routers, Switches and Other Network Infrastructure	28
12.5	Data Confidentiality and Integrity.....	28
12.5.1	General	28
12.5.2	Student Records, Health Records, Other Confidential Records.....	28
12.5.3	Sensitive Records	29
12.6	Surplus Equipment	29
12.7	Network Ports.....	29
13	Effective Date, Revision Schedule	29
14	Definitions	30

Information Technology Security Plan

College of Engineering

1 Scope

- 1.1 This plan establishes practices intended to implement the College of Engineering Information Technology Security Policy (see <http://www.eng.ufl.edu/home/mis/security/policies.html>), and the University of Florida Information Technology Security Policy and subsidiary documents (see <http://www.it.ufl.edu/policies/security/>).
- 1.2 All units within the College of Engineering must comply with the requirements of this plan, as well as other documents that may be published by the College to facilitate implementation of this plan.
- 1.3 All units with guest presence on any network operated by or assigned to the College of Engineering must comply with this plan, unless security authority for address space used by a guest unit outside the College has been formally transferred to the guest unit by the College. See *Transfer Of Authority*, page 24.
- 1.4 In accordance with the College of Engineering IT Security Policy, this plan establishes the College of Engineering IT Security Manager (ISM) as the central point of contact in the college for the UF ISM, establishes requirements for ISMs of units within the College, and specifies required documentation that must be provided to the College ISM.

2 Responsible Personnel

2.1 College IT Security Officer

The College of Engineering IT Security Officer is

Pramod P. Khargonekar

Information Technology Security Plan

College of Engineering

Dean, College of Engineering
352-392-6000

2.2 College IT Security Manager

The College of Engineering IT Security Manager (ISM) is

Robert Johnson
Senior Systems Programmer
352-392-9217
security@eng.ufl.edu

2.3 Unit Information Technology Security Managers

Each College Unit (see page 30) must designate a person who will act as the Unit IT Security Manager (Unit ISM). This person manages IT security issues for the unit, and will act as the unit's liaison to the College ISM and provide a contact point by which the unit will be notified of IT security issues. A list of College Unit ISMs is available at <http://www.eng.ufl.edu/home/mis/security/unitismlist.html> .

2.4 Notification

Each College Unit (see page 30) must notify the College ISM of the identity of the designated Unit ISM. Notification may be made by sending email to security@eng.ufl.edu , or by letter to

IT Security Manager
ATTN: Unit ISM Notification
Engineering MIS
Box 116550
University of Florida
Gainesville, FL 32611

Information Technology Security Plan

College of Engineering

3 Unit Plans

3.1 Requirement

Each College Unit must develop an IT Security Plan in accordance with the requirements of this plan, the College of Engineering IT Security Policy, and the UF IT Security Policy, and subsidiary documents, including published procedures and best practices. The College of Engineering IT Security Policy is available at <http://www.eng.ufl.edu/home/mis/security/EngSecPol.html>, and the UF IT Security Policy is at <http://www.it.ufl.edu/policies/security/>.

3.2 Mandatory Topics

To comply with the UF IT Security Policy and supporting documents and the College of Engineering IT Security Policy, and to ensure a clearly defined reporting structure within the college, each unit IT Security Plan must address certain specific topics and require certain documentation, as follows:

3.2.1 Plan Title

The unit name must be included in the plan title.

3.2.2 Plan Scope

Each unit plan must identify the range of network addresses to which the plan applies; must identify the single parent unit from which the unit obtains IT security authority; and must specify which IT security policies and plans the unit plan is intended to implement.

Information Technology Security Plan

College of Engineering

3.2.2.1 Note regarding IT security authority: departments and independent centers obtain IT security authority from the college, subnets within a department obtain their IT security authority from their department, etc. In order to establish a clear chain of responsibility, each unit must have one and only one parent unit designated as its source of security authority, and will be responsible for complying with the IT security policies, plans, and procedures of that parent.

3.2.3 Responsible Personnel

The unit plan must identify the Unit ISM, the Unit IT Security Officer (if any is designated), and the network and system administrators for the unit.

3.2.4 Inventory and Network Diagram

In order to clarify the security issues facing the unit, and to enable identification of offending devices when reports of worms, viruses, or other problems are received, each unit must create an inventory of IT devices owned or operated by the unit, categorized by operating system, and including a network diagram. Systems with unknown embedded operating systems (e.g. directly networked printers) should be categorized by manufacturer. This inventory must be provided to the College ISM, and must be updated as changes are made to the network. In order to simplify distribution of updates, publication on a secure website is the preferred method of publishing this inventory. Additional information about what should be included is available in the UF IT Security Procedures at <http://www.it.ufl.edu/policies/security/outlines/unit-documentation-outline.html> .

Information Technology Security Plan

College of Engineering

3.2.5 Host and User Identification

The Unit ISM must maintain records of the hardware address, the host address, and the primary user for every IT resource in their unit, or have access to such records maintained by subsidiary Unit ISMs. Such records must be available to the College ISM.

3.2.6 Management Responsibility

Each plan must clearly define for each IT device owned or operated by the unit, or for each subnet or block of network addresses managed by the unit, a single person who is responsible for security management of that device or all devices attached to that address block.

3.2.7 Optional Topics

Unit plans may address additional topics not specified in this plan.

4 Critical Resources

4.1 Any unit that wishes to have an IT device designated a "critical resource" as defined by the UF IT Security Policy (<http://www.it.ufl.edu/policies/security/>) must submit to the College ISM a management plan that describes how security incidents involving that device will be handled in a timely manner. The plan must designate the individual(s) who will be available for consultation involving after-hours security incidents. After the College ISM has approved the management plan, the College ISM will submit the plan to the UF ISM for approval. The unit submitting the plan must make available a representative to answer questions about the proposed plan.

5 Servers

5.1 General

- 5.1.1 Unit plans must address security procedures for all servers operating on the unit's network. Procedures must, for each server, unambiguously define a Professional IT Administrator (see page 30) responsible for installing operating system patches, server software patches, and other maintenance necessary for the security of the server.
- 5.1.2 No server may be placed on a unit network without approval of that unit's ISM.
- 5.1.3 The Unit ISM must have contact information for the manager of each server on the unit network. Unit plans must provide for collection and maintenance of this contact information.
- 5.1.4 The term "server" is to be interpreted in a very broad sense, to include servers using HTTP, FTP, DHCP, VPN, VNC, SSH, SMTP, POP, IMAP, or other client-server model protocols, as well as peer-to-peer services such as Windows networking, Gnutella, or KaZaA.
- 5.1.5 Unit plans may allow the Unit ISM to give blanket permission to install servers for a specific protocol if there is adequate security in place to protect that protocol. For example, a department may elect to allow users to create Windows networking shares on a subnet that protects such shares from external attack. This blanket permission does not eliminate the requirement for oversight by a Professional IT Administrator.
- 5.1.6 In order to concentrate security and management resources most effectively, units should house their servers in a single physical location when feasible.

Information Technology Security Plan

College of Engineering

5.2 Official Information Servers

5.2.1 Unit plans must provide for regular review of the content of servers used to provide official information about the unit. The content provided by official information servers must be approved by the Unit Administration (see page 30) before being made available to the general public.

5.2.2 Official information must be archived in accordance with state record retention requirements. Information about retention requirements is available at <http://www.aa.ufl.edu/aa/records/> .

5.3 Support Servers

5.3.1 Support servers, i.e. servers used to support unit activities by hosting teaching web sites, providing database access, etc., are often installed and operated by non-IT personnel who are not familiar with standard security practices. Unit plans must specifically provide for proper security management of all such servers by assigning a Professional IT Administrator (see page 30) to be responsible for oversight of the operation and management of each server.

5.4 Personal Servers

5.4.1 Unit plans must ensure that servers set up and operated by individuals for personal use are properly managed. Users who set up personal servers must be reminded that they are subject to the security requirements of the UF, College, and Unit IT Security Policies, even when they are connected to the network as unmanaged hosts (see Managed vs. Unmanaged Hosts page 14).

5.4.2 Units may elect to prohibit personal servers if unit resources do not allow for proper oversight of such servers.

5.5 Student Organization Servers

5.5.1 Use Discouraged

Servers operated by student organizations present an additional management problem because of the high turnover rate of the students managing the servers. Units should discourage student organizations from operating their own servers and encourage them to use existing servers.

5.5.2 Discretionary Permission

Units may prohibit student organization servers if unit resources do not allow for proper oversight of such servers.

5.5.3 Time Limited Authorization

Unit plans must provide a means of registering any student organization servers with the Unit ISM so that the unit has contact information for the individual(s) managing them. Such registration must be renewed each semester, or the student organization server must be removed from the network until registration information is updated.

6 E-Commerce Systems

6.1 General

E-commerce (i.e. systems that collect payment from the Internet) is a particularly important source of liability for the College and the University. University of

Information Technology Security Plan

College of Engineering

Florida policies for E-commerce (see <http://admin.ufl.edu/handbook/default.asp?doc=2.4.6.1>) require that all credit card transactions be processed via a central server operated by the UF Division of Finance and Administration (the IPAY system). Units wishing to operate E-commerce systems must contact the Division of Finance and Administration for instructions on how to proceed.

6.2 Registration

E-commerce systems must be registered with the College ISM. Units must provide the College ISM a description of the purpose of the system, contact information for both a technical contact and an administrative contact for the system, and a copy of the approved business plan that was filed with the Division of Finance and Administration.

7 Data Management and Security

7.1 Classification

Each unit must perform a review of all electronically stored data and assign each data collection a level of confidentiality which will be used to determine the appropriate level of security to be applied to that data. Suggested levels are:

7.1.1 "Routine" for data collections that are believed to contain only data that would be released if requested in a public information request;

7.1.2 "Sensitive" for data collections that are likely to be granted exemption from public disclosure because of the sensitive nature of the data. An example

Information Technology Security Plan

College of Engineering

would be details of unit security plans.

7.1.3 "Confidential" for data collections that are required by statute or rule to be exempt from public disclosure requirements. This includes student records (including records of network use or involvement in security incidents), and health care information subject to HIPPA privacy requirements.

7.1.4 Units may use other classification systems if appropriate.

7.2 Student Records

7.2.1 Confidentiality

Unit Information Technology workers are reminded that most information about individual students is considered confidential under Federal law, and may not be released to unauthorized personnel without permission from the student. This includes records of a student's network or computer activity, involvement in security incidents, and similar information.

7.2.2 Security

Student records must be protected by a level of security commensurate with their confidentiality. Student records should not be maintained on publicly accessible systems, even if the public is not normally allowed to access that particular data. Exceptions to this prohibition must be documented and justified in the unit's security plan.

Information Technology Security Plan

College of Engineering

7.3 Record Retention

7.3.1 All electronic records must be retained in accordance with State law and UF policy and procedures.

7.3.1.1 Many types of electronic records will fall under the classification of "archive until obsolete, superseded, or administrative value is lost" (OSA), and may be routinely discarded as provided by law. All other data must be retained as required by law, and disposal of such data must be in accordance with state law and UF policy and procedures.

7.3.1.2 The UF IT Security Policy

(<http://www.it.ufl.edu/policies/security/index.html>) requires that system logs which record usage (e.g. user logon and logoff, web page access, DHCP records, etc.) be retained for three years as [General Records Schedule GS1-S Item 104](#) material.

7.3.2 Records of archived data, and of the disposal of such data, must be maintained as required by state law and UF policy and procedures. Each unit plan must specify how such records will be maintained. Units are encouraged to integrate records of electronic data archives into their existing records for paper archives.

7.3.3 Information about record retention requirements is available at <http://www.aa.ufl.edu/aa/records/>. IT staff should contact their unit's Records Manager for assistance in developing record management procedures.

7.3.4 All archives must be stored on a medium, and in a manner, which will provide reliable storage for the retention period of the archive. For example, an active hard drive on a user's workstation should not be used to store three-year archives unless also backed up to a long term backup medium.

Information Technology Security Plan

College of Engineering

7.4 Public Records

7.4.1 Public records are by definition available to the public on request.

Despite this classification, all public records must be reviewed for confidential content before release to the public. Thus, material classified as "public record" (or equivalent) must still be protected by reasonable security measures.

7.4.2 Before such screening, access to such records must be limited to those personnel with a need to access the records as part of their official UF responsibilities. Adequate security must be in place to ensure that such public records can not be deleted or altered by unauthorized personnel, and that such records are archived as required by law.

7.4.3 IT staff must be trained in proper procedures for handling requests for release of public records. UF policy requires that all public record requests be referred the appropriate department chair or administrative supervisor. If there is any doubt about the public record status of a particular item, or how to handle a particular public record request, the question should be referred to the UF Office of News & Public Affairs (392-0186), who will consult with the Office of General Counsel as appropriate.

8 Email Management

8.1 Scope

All email generated or received as part of the normal operation of the university is potential public record. Unit plans must address the public record and record retention aspects of email.

8.2 Retention

- 8.2.1 All email must be retained in accordance with applicable law and university policies and procedures. Because retention requirements vary depending on message content, a unit may either use the longest applicable retention period for all email, or classify email for archive on a message by message basis.
- 8.2.2 Units may meet retention requirements by making individual users responsible for proper retention of their own email, but unit plans must then specify an education program to train users on proper retention procedures.
- 8.2.3 "Spam" messages (unsolicited commercial advertising or bulk distributed messages that do not involve official University business) are not considered to be related to the normal function of the University and need not be retained as public record.

8.3 User Authentication

Email systems must require user authentication to send or receive email messages. IP numbers may be used to authenticate access to SMTP hosts to send outgoing mail, although more reliable authentication methods are encouraged.

8.4 Encryption

Units are encouraged to use encrypted protocols for both sending and receiving email. In particular, units should educate users about the need to use encrypted protocols when sending or receiving email via wireless connections, or when the email has sensitive content.

9 Network Infrastructure and Access Control

9.1 General Security

All networks in the college must be operated in a manner which can be reasonably expected to prevent unauthorized access to network resources.

9.2 Managed vs. Unmanaged Hosts

9.2.1 Unit plans must distinguish between "managed hosts", i.e., systems managed by the unit's professional administrators, and "unmanaged hosts", i.e. systems, such as personal laptops, PDAs, and vendor-supplied equipment, that are not managed by the unit's professional administrators (see definition of Professional IT Administrator , page 30).

9.2.2 For each managed host attached to the unit network, the unit must designate a professional IT administrator who will be responsible for proper management of the host.

9.2.3 Unmanaged hosts may only be connected to network ports designated for that purpose by the Unit ISM. It is the responsibility of the Unit ISM to ensure that ports so designated are managed in a manner that protects other networks from poor security practices on the unmanaged host. Such measures might include operation on a subnet other than the normal unit subnet, ability to identify and disconnect the host from the network immediately if it is found to be a source of network disruption, frequent scanning of unmanaged host addresses for evidence of compromise by worms or trojan horse programs, preventative scanning of unmanaged hosts before they are connected to the unit's network, user training, or any other measures deemed appropriate by the Unit ISM.

9.3 User Authentication

9.3.1 Units must establish criteria for issuing and revoking accounts, including guest accounts. Users must read and agree to the UF Acceptable Use Policy (<http://www.it.ufl.edu/policies/aupolicy.html>) and be required to sign a user agreement before being granted access.

9.3.2 All users must be required to authenticate before obtaining network access.

9.3.3 User authentication must be logged, and the logs must be retained for at least three years in a form that can identify which user account was using a given IP number (or other network address in the case of non-IP protocols) at a given time.

9.3.4 Devices that are by design used as pooled resources without user accounts (e.g. printers) must be tracked in a manner that allows the device using a given network address at a given time to be identified.

9.3.5 Time stamps in user authentication logs must be synchronized to a reliable time reference and must be accurate to the nearest second.

9.3.6 Exceptions to user authentication and logging requirements must be approved by the College ISM.

9.3.7 Unit plans must specify procedures for user authentication and authentication log retention.

9.4 Infrastructure

9.4.1 Physical Plant

9.4.1.1 Network physical plant (cables, switches, and other devices on the network side of the network port or "wallplate") must be installed and configured so as to prevent unauthorized access to the network.

9.4.1.2 Unused network ports (wallplates) accessible to unauthorized users must be disconnected or disabled at a local switch or router.

9.4.1.3 Ports are not considered "accessible to unauthorized users" if they are in an area with controlled access, such as faculty and business offices that are locked when not occupied, provided that the normal occupants of the area have received training in the requirement that access to network ports must be limited to authorized personnel.

9.4.2 DHCP Servers

9.4.2.1 DHCP servers must be managed in a manner which allows the Unit ISM to identify the specific user that is using an IP number at any given time, except for devices (e.g. printers) that do not have logged in users.

9.4.2.2 In order to facilitate overall management of the University of Florida networks, DHCP servers must be coordinated with UF/CNS Network Services. Units contemplating offering DHCP services are urged to contact Network Services to determine their management requirements before purchasing equipment or setting up service.

9.4.2.3 Printers and other devices that do not have logged in users must be tracked so that the device using a given network address at a given time

can be identified.

9.4.2.4 Records of these associations must be retained for at least three years.

9.4.2.5 Unit plans must explicitly provide for compliance with these requirements.

9.4.3 VPN Servers

VPN servers provide a means for outsiders to access a network. In addition, because VPN connections are encrypted, they circumvent the normal intrusion detection methods employed on the campus core network. Thus, VPN servers must be operated in accordance with procedures designed to address these issues.

9.4.3.1 Authorization Required

Local VPN servers may not be operated without the permission of the college ISM. Units are required to document procedures for management of the VPN, and must provide contact information for the IT staff that will be administering the VPN. Requests should be sent to security@eng.ufl.edu.

9.4.3.2 Coordination

Local VPN servers must be coordinated with UF/CNS Network Services. Units considering local VPN services are encouraged to contact Network Services for information about their management requirements before purchasing or installing VPN equipment or software.

9.4.3.3 Authentication Required

VPN Servers must be configured so as to require user authentication before allowing access to the local network. All VPN access must be traceable to a responsible user.

9.4.3.4 Logging Required

VPN servers must be configured to record all connections in sufficient detail to identify the user or user account used to authenticate the connection. Records must be retained for at least three years.

9.4.3.5 Maintenance Precautions

Particular care must be taken to ensure that VPN servers are actively maintained. All appropriate security updates and patches must be applied promptly. Unit plans that permit VPN servers must specify procedures to ensure such maintenance.

9.4.4 Inbound Modems

Dial-up modem servers provide a means for outsiders to access a network. They also bypass the normal intrusion detection methods employed on the campus core network and at the Internet feeds. Thus, inbound modem servers (including PCAnywhere, personal RAS servers, and similar products) must be operated in accordance with procedures designed to address these issues.

9.4.4.1 Authorization Required

Inbound modem servers may not be operated without authorization from the College ISM. Units are required to document procedures for management of the modem server, and must provide contact information for the IT staff that will be administering the modem service. Requests should be sent to security@eng.ufl.edu.

9.4.4.2 Coordination

Inbound modem services must be coordinated with UF/CNS Network Services. Units contemplating inbound modem services are urged to contact Network Services to determine their management requirements before purchasing equipment or setting up service.

9.4.4.3 Authentication Required

Modem servers must be configured so as to require user authentication before allowing access to the network. All inbound modem access must be traceable to a responsible user.

9.4.4.4 Logging Required

Modem servers must be configured to record all connections in sufficient detail to identify the user or user account used to authenticate the connection. Records must be retained for at least three years.

9.4.5 Wireless Access Points

Wireless access points provide a means for outsiders to access a network. In

Information Technology Security Plan

College of Engineering

addition, traffic through wireless links can be easily monitored by unauthorized individuals. Thus, wireless access points must be operated in accordance with procedures designed to address these issues. Units contemplating establishment of wireless networking services should familiarize themselves with the requirements of the UF Wireless Networking Policy (see <http://www.it.ufl.edu/policies/wireless.html>).

9.4.5.1 Authorization Required

Wireless access points may not be operated without authorization from the College ISM. Units will be required to document procedures for management of the access point, and must provide contact information for the IT staff that will be administering the access point. Requests for authorization should be emailed to security@eng.ufl.edu.

9.4.5.2 Coordination

Wireless Access Points must be coordinated with both Network Services and the College ISM. In order to minimize interference with existing access points, any unit contemplating installation of a Wireless Access Point should contact the College ISM for guidance before purchasing or installing network equipment.

9.4.5.3 Authentication Required

Wireless access points must be configured to require user authentication before allowing network access. User authentication may be accomplished by using Ethernet MAC address filtering, although more robust techniques are encouraged.

9.4.5.4 Encryption Encouraged

It is recommended that wireless access points be configured to require encryption of over-the-air data. If that is not feasible, users should be encouraged to use encrypted protocols for all activities. The UF VPN service is a suitable method for accomplishing this in many cases (see http://net-services.ufl.edu/provided_services/vpn/).

9.4.5.5 Logging Required

Wireless access points must be configured to record all connections in sufficient detail to identify the user or user account used to authenticate the connection. Records must be retained for at least three years.

10 Standard Procedures

10.1 Incident Response

10.1.1 Unit plans must specify procedures for investigating and reporting network security incidents. Specified procedures must designate an individual who is responsible for coordinating the investigation. Such designation may vary by subnet or other unit subdivision.

10.1.2 Significant incidents must be reported to the College ISM. The College will publish further guidance regarding incident reporting criteria and procedures.

Information Technology Security Plan

College of Engineering

10.1.3 Responses to any incident notifications received from UF/CNS Network Services or Network Incident Response Team (NETIRT) must be copied to the College ISM (security@eng.ufl.edu).

10.2 User Workstations

Unit plans must specify procedures for management of user workstations including user peripherals (e.g. network printers), to include at least the following:

10.2.1 Critical Patches and Updates

Unit plans must specify procedures designed to ensure that critical or security patches and updates are applied in a timely manner to all user workstations and network peripherals in the unit.

10.2.2 Virus Protection

Unit plans must specify procedures designed to ensure adequate protection against viruses and other "malware" in user workstations. Plans should require the use of virus scanners on user workstations, including laptops or other personal systems, and should specify procedures designed to ensure that virus scanner databases are regularly updated. Units should consider additional strategies such as encouraging the use of Ad-Aware, Spybot, or similar anti-spyware tools.

10.2.3 Responsibility

As specified in section 3.2.6, each unit plan must clearly specify for each workstation or group of workstations, an individual who is responsible for security management of that workstation or workstations. It shall be the responsibility of that individual to ensure that specified procedures for patches, updates, virus scanning, and other security requirements are performed in a timely manner.

Information Technology Security Plan

College of Engineering

10.3 Business Resumption Plan

10.3.1 Units are required by UF policy to maintain an updated Business Resumption Plan (a.k.a. Disaster Recovery Plan). See <http://www.it.ufl.edu/policies/security/outlines/unit-brp-outline.html> for more information about required Information Technology Business Resumption Plans.

10.3.2 Unit IT Business Resumption Plans must be made available to the college ISM on request.

10.4 Logon Banners

10.4.1 Unit plans must require that users logging in to computers be, whenever feasible, presented with an appropriate logon banner that warns them of the following:

- Users are required to comply with the UF Acceptable Use Policy (<http://www.it.ufl.edu/policies/aupolicy.html>).
- Unauthorized use of the system (or network) is prohibited and may be punishable as a criminal violation.
- Use may be monitored, recorded, or revealed to law enforcement or other third parties when appropriate.

10.4.2 When feasible, required logon banners must be presented before the user has been granted network access.

10.4.3 Logon banners may be presented as part of the logon process, or may be displayed as fixed signs posted on or near the computer.

10.5 Intrusion Detection and Monitoring

10.5.1 Intrusion Detection Systems

Units are encouraged to implement procedures or devices that aid in the detection of unauthorized use of computers or network resources, including (but not limited to) automated intrusion detection systems, automated log reviews, routine network scans for suspicious services offered by computers on the network (i.e. open TCP ports or similar indications), and routine scans for unauthorized hosts operating on the network.

10.5.2 Filesystem Signature Tools

Unit plans must encourage the use of file signature recording tools such as Tripwire or Aide to detect unauthorized changes to system files and to assist in investigation of suspected or known system intrusions.

10.5.3 Log Reviews

Unit plans must require weekly (or more frequent) inspection of system logs as an aid in detecting compromises, misconfigured devices, and equipment failures.

10.6 Transfer of Authority

Units that wish to transfer security authority for part of their assigned address space, whether to a unit in the College of Engineering or to an outside unit, must send a request for such transfer of authority to security@eng.ufl.edu. If the transfer is approved, the College ISM will notify both the ISM of the hosting unit and the ISM of the guest unit of the transfer. The College ISM may require

Information Technology Security Plan

College of Engineering

documentation of the security measures that will be implemented by the guest unit.

10.7 Vulnerability Scans

10.7.1 The College ISM is authorized to conduct scans for vulnerable systems on any college network. When conducting such scans, the ISM shall notify UF Network Services and the Unit ISM for the network being scanned, so they can be prepared for alerts generated by their Intrusion Detection Systems.

10.7.2 Unit ISMs are encouraged to conduct vulnerability scans of their unit's networks on a regular basis. Prior to conducting any scans, email notification should be sent to the UF ISM, College ISM, other Unit ISM or other appropriate personnel in any units which will be affected by the traffic, e.g. UF/CNS Network Services (net-services@ufl.edu) should be notified when scan traffic will traverse a UF core network router.

10.7.3 Unit ISMs may authorize other personnel to conduct vulnerability scans within their unit.

10.7.4 Unit ISMs may request results of vulnerability scans performed by the College ISM by sending email to security@eng.ufl.edu.

10.8 Software Development Standards

10.8.1 In order to comply with requirements of the Family Educational Right to Privacy Act (FERPA - the "Buckley Amendment"), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and other applicable state and federal laws, development of applications that will access, store, or manipulate student records, health records, financial information, or other sensitive data, must be developed using practices

Information Technology Security Plan

College of Engineering

designed to assure the security of the resulting application(s).

10.8.2 Development of such applications that will be accessible via network connections must use development procedures and processes approved by the Unit ISM. It shall be the responsibility of the developers to demonstrate to the Unit ISM that the proposed development procedure will provide an appropriate degree of confidence in the security of the resulting application(s). Developers and Unit ISMs should refer to the University of Florida Secure Application Development Guidelines (tentatively available at <http://nslog.nerdc.ufl.edu/security/policy/app-dev.html>, this address may change) for guidance.

10.8.3 Evaluation of proposed development procedures for such applications shall consider the sensitivity of the information involved, the methods of access that may be available to unauthorized persons, the experience and skill of the individual developers involved, and any other factors that may be significant.

10.8.4 Units developing software that will operate on any UF network should become familiar with the requirements of the UF Application Development Policy (to be published Fall 2003).

10.8.5 Questions related to proposed development procedures and practices should be referred to the ISM of the parent unit, or to the UF ISM.

11 Training

11.1 Units must ensure that IT employees have training and skill appropriate to their duties, and receive additional training as necessary to maintain competence.

11.2 Units must ensure that IT employees attend mandatory orientation sessions. See http://net-services.ufl.edu/security/orientation/it_staff.shtml for more

information about orientation sessions.

- 11.3 Units should take advantage of the many on-campus training opportunities available to faculty and staff. The UF Computer Challenge (<http://www.it-train.ufl.edu/>) and Information Technology Security Awareness Day (<http://www.itsa.ufl.edu/>) are examples of such training.

12 Physical Security

12.1 General

All unit plans must include a description of physical security measures used to protect equipment and data from access or alteration by unauthorized personnel. Unit plans should not include confidential details of security systems such as passwords, combinations to locks, etc.

12.2 Facilities

12.2.1 Key Locks

When possible, facilities housing servers or network infrastructure equipment should use auditable key locks, i.e. "smart card" or other key locks that record the identity of individuals entering the facility.

12.2.2 Environmental Control

In order to improve reliability and reduce maintenance costs, equipment should be housed in appropriate environmentally controlled environments.

12.3 Servers

Whenever feasible, physical access to servers must be restricted to include only the administrators of each server. If such restriction is not feasible, access must be limited to a known list of personnel.

12.4 Routers, Switches and Other Network Infrastructure

Whenever feasible, physical access to network infrastructure equipment must be restricted to include only individuals who maintain, install, or manage the equipment. If such restriction is not possible, access must be limited to a known list of personnel.

12.5 Data Confidentiality and Integrity

12.5.1 General

All unit plans must provide for physical security of data commensurate with the level of confidentiality assigned to that data.

12.5.2 Student Records, Health Records, Other Confidential Records

Confidential records must be physically secure from access, deletion, or modification by unauthorized personnel. Systems containing such records must be protected against physical access by unauthorized personnel.

Information Technology Security Plan

College of Engineering

12.5.3 Sensitive Records

Sensitive records may include records of security plans and procedures, or other information that can be exempted from classification as a public record. All sensitive records must be physically protected at a level consistent with the sensitivity of each individual data collection.

12.6 Surplus Equipment

12.6.1 All surplus equipment must be sanitized of any data that is not public record before being distributed to any individual or unit that is not authorized to have access to that data.

12.6.2 Each unit plan must specify procedures to ensure proper erasure of such data, to include at a minimum overwriting the sensitive data. It is not sufficient to merely delete sensitive files or repartition a hard drive.

12.7 Network Ports

12.7.1 Network ports (e.g. Ethernet, wireless) must be managed in a manner that prevents unauthorized personnel from connecting to the network.

13 Effective Date, Revision Schedule

13.1 This plan, and any changes thereof, will be considered officially adopted when approved by the Dean of the College of Engineering.

13.2 Unit ISMs must be appointed, and the College ISM notified, within two weeks of official adoption of this plan.

Information Technology Security Plan

College of Engineering

- 13.3 Unit IT Security Policies and Plans, including necessary supporting documentation, must be established, and copies provided to the College ISM, within two months of adoption of this plan, and whenever modified thereafter.
- 13.4 The College ISM must review this plan at least once each year, soliciting input from Unit ISMs, and recommend changes as judged appropriate.
- 13.5 Suggestions or requests for changes to this plan should be sent to the College ISM. Such suggestions may be emailed to security@eng.ufl.edu.

14 Definitions

BRP - *Business Resumption Plan*, also known as a *Disaster Recovery Plan* or a *Continuity of Operations Plan*.

College Unit - A Department, or equivalent Center, Institute, Program, or Laboratory (i.e. GERC, GCATT, ERC, FCSHWM, INSPI, IPPD, MICROFABRITECH, and SUCCEED) which reports to the College rather than to a Department within the College.

IT - Information Technology

Professional IT Administrator - A professional IT administrator (or manager) is a person who is hired by a unit to perform system or network administration, and whose job description specifies duties that include installing and configuring operating systems; applying operating system patches or upgrades; installing, configuring, and maintaining network infrastructure devices and servers; investigating IT security issues; or monitoring and correcting network performance; and who has training commensurate with these duties.

Unit Administration - Department Chair, Director of a Center, Institute, Program,

Information Technology Security Plan

College of Engineering

or Laboratory, or authorized designee.

Unit IT Security Manager (Unit ISM) - An individual appointed by the Unit Administration to manage information technology security issues for the unit, and to act as liaison to the College of Engineering IT Security Manager.

Unit IT Security Officer - An individual appointed by the Unit Administration to oversee the work of the Unit ISM.