

IT Security and Computer Regulations Policy

Department of Civil and Coastal Engineering

University of Florida

February 9, 2004

Revised 1/14/09

Table of Contents

1. Scope
2. Responsible Personnel
 - 2.1 Level 2 College IT Security Administrator
 - 2.2 Level 2 College IT Security Manager
 - 2.3 Level 3 Unit IT Security Administrator
 - 2.4 Level 3 Unit IT Security Manager
 - 2.5 Notification of ISA or ISM changes
3. Inventory and Network
4. Critical Resources
5. Subunit Servers
6. E-Commerce Systems
7. Data Management and Security
8. E-Mail Management
9. Network Infrastructure and Access Control
 - 9.1 General Security
 - 9.2 Managed vs. Unmanaged Hosts
 - 9.3 User Authentication
 - 9.4 Physical Plant
 - 9.5 Department Servers
 - 9.5.1 DHCP Servers
 - 9.5.2 VPN Servers
 - 9.5.3 Mail Servers
 - 9.5.4 Web Servers
 - 9.5.5 Data Servers
 - 9.6 Inbound Modems
 - 9.7 Wireless Access Points
10. Standard Procedures
11. Training
12. Physical Security
13. Effective Date, Revision Schedule
14. Definitions
15. Personal Laptop and Desktop Computers
16. Computer Software Applications
17. IP Subnets
18. Computer Support

1. SCOPE

This plan establishes practices intended to implement the Department of Civil and Coastal Engineering Information Technology Security and Computer Policy.

The Department of Civil and Coastal Engineering must comply with the requirements of this policy, as well as other documents that may be published by the Department of Civil and Coastal Engineering to facilitate implementation of this policy as described by University IT Security Policy (<http://www.it.ufl.edu.edu/policies/security>) and College IT Security Policy (<http://www.eng.ufl.edu/home/mis/security/policies.html>).

All units with guest presence on any network operated by or assigned to the Department of Civil and Coastal Engineering must comply with this policy.

In accordance with the College of Engineering IT Security Policy, this policy establishes the Department of Civil and Coastal Engineering Unit IT Security Manager as the central point of contact in the department for the College of Engineering, establishes requirements within the department that also meets the requirements of the College and specifies required documentation that must be provided to the College ISM (IT Security Manager).

2. RESPONSIBLE PERSONNEL

2.1 Level 2 College IT Security Administrator

Level 2 College IT Security Administrator (L2 ISA) is the Dean of the College of Engineering who appoints the Level 2 College IT Security Manager (L2 ISM) for the college. The L2 ISA will oversee the work of the L2 ISM and be responsible for establishing official goals and policy to be implemented by the L2 ISM.

Level 2 College IT Security Administrator (L2 ISA)

Dr. Pramod P. Khargonekar
College of Engineering
Dean
352-392-6000

2.2 Level 2 College IT Security Manager

Level 2 IT Security Manager (L2 ISM) will fulfill, for all units with the college, the functions defined for the position by the University of Florida

Information Technology Security Policy. All units within the college will be represented by the L2 ISM.

Level 2 College IT Security Manager (L2 ISM)

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

2.3 Level 3 Unit IT Security Administrator

Level 3 Unit IT Security Administration (L3 ISA) is the Department Chairman. The L3 ISA appoints the L3 ISM.

Level 3 Unit IT Security Administrator (L3 ISA)

Dr. Kirk Hatfield
Department of Civil and Coastal Engineering
Chairman
352-392-9537 x1401
khh@ce.ufl.edu

2.4 Level 3 Unit IT Security Manager

Level 3 Unit IT Security Manager (L3 ISM) is appointed by the Chairman of the department and is responsible for coordinating with the L2 ISM and supervising implementation of IT security policy and plans. The L3 ISM manages IT security issues for the unit, and will act as the unit's liaison to the L2 ISM and provide a contact point by which the unit will be notified of IT security issues.

L3 Unit IT Security Manager (L3 ISM)

Anthony J. Murphy
Department of Civil and Coastal Engineering
Senior Computer Support Specialist
352-392-9537 x1501
tony@ce.ufl.edu

3. INVENTORY AND NETWORK

3.1 INVENTORY

- a. All departmental owned computers, desktops and laptops, are assigned a five (5) digit inventory number by applying a department inventory label on each machine.
- b. All networked printers are assigned a five (5) digit inventory number by applying a department inventory label on each network printer. A network printer is defined as a printer directly connected to the network via a CAT5 cable and assigned an IP number or use of DHCP IP assignment. This printer is not connected to any computer.
- c. All non-departmental computers or personally owned computers connected to the department network via static or dynamic IP assignment are also inventoried. A 99999 inventory number is assigned in conjunction with the machine host name identifies the individual machine record.
- d. Inventory of these machines is maintained by an inventory program written in Visual Basic 6.0 language. The inventory database includes the inventory number, type of machine, specifics of the machine such as ram, hard drive, purchaser, user, IP number assigned, MAC number, building, room number, etc...
- e. The inventory system can provide reports of the machines in any order such as by IP, room, purchaser, discipline (Structures, Geotech, Construction, Materials, Geosensing, etc...)
- f. The inventory system provides a search engine for locating a specific machine by any of its characteristics such as IP number, host name, room, building, brand, model, etc....

4. CRITICAL IT RESOURCE

Any resource which will significantly impair the operation of a unit if the resource is unavailable for an extended time should be given special consideration in the units IT security policies. The following resources are considered Critical IT Resources:

- 1) Department data file server
- 2) Department E-Mail/Web Servers

5. SUBUNIT SERVERS

A subunit server is defined as a non-departmental server. That being a server for student associations or individual professors administered by students and not by the department IT Staff.

No subunit server may be placed on a unit network without approval of the L3 ISM. (see section 5.1)

The use of subunit servers is prohibited unless the user can show a need that cannot be met by a department server. Procedures for requesting permission to establish a server not managed by the department L3 ISM or other designated staff server administrators (see section 9.5) are described in section 5.1.

Refer to section 9.5 for Department Servers.

5.1 Establishing Subunit Servers

Subunit servers of any sort are discouraged. Subunit servers are defined as servers for student organizations, societies of subunit discipline. A server for an individual will not be allowed under any circumstances.

Subunit servers may only operate when it is not feasible for an existing department server to meet the needs of the organization, society or subunit on the approval of the L3 ISM. Procedures for requesting approval to establish a subunit server are described in section 5.1.1.

5.1.1 Requesting a subunit server

Any subunit wishing to operate a server must first obtain approval from the L3 ISM. The subunit must submit a written management plan that explains:

1. Why the server is necessary.
2. Who will manage the server with contact information
3. Who will be responsible for timely updates
4. Provide proof of OS and application licensure, if server is approved
5. Continuity of management (see section 5.1.2)

Proposals may be hand delivered or e-mailed to:

Unit IT Security Manager
Civil and Coastal Engineering
Box 116580 (if mailed)
454A Weil Hall (if hand delivered)

University of Florida
Gainesville, FL 32611
cce-it@ce.ufl.edu (if e-mailed)

Note-Systems providing Windows networking for peer-to-peer file sharing or printer sharing are not considered servers for the purposes of this section. Subunits may use Windows File and Printer Sharing for local networking.

5.1.2 Subunit Proposals

5.1.2.a Continuity of management

A problem inherent in allowing subunits to operate servers is that they have a very high turnover rate. Normally students are assigned the task to setup the servers and with students eventually leaving either by graduation or transferring, it is common for knowledge to disappear when the student holding it leaves the subunit, even when the knowledge is in written form. It is critical that a workable plan for handling this transition be developed.

5.1.2.b Contact information

It can be very difficult to contact students particularly on weekends and during breaks. Subunit must understand that they are responsible for their servers at all times and that if the system manager cannot be contacted, a compromised server will be disconnected from the network.

5.1.2.c Need

The subunit must demonstrate that its need for services not provided by existing servers compensates for the added risk posed by adding a new server to the network, operated by Sysadmins who have little real-world experience.

6. E-COMMERCE SECURITY

At this time, the Civil and Coastal Engineering Department does not operate an E-Commerce Server.

7. DATA MANAGEMENT AND SECURITY

To be written

8. E-MAIL MANAGEMENT

To be written

9. NETWORK INFRASTRUCTURE AND ACCESS

1. All computers operate in a manner which can be reasonably expected to prevent unauthorized access to network resources.
2. All user passwords must be secure enough that it cannot be easily discovered. Rule of thumb, if it is in the dictionary, it can be discovered in a matter of minutes. Use a letter, number, upper and lower case or special character combination. It should be at least six characters long.
3. All operating systems must be updated at least on a weekly basis. All Anti Virus programs must be up to date and virus definitions updated on a regular basis. It is recommended to run virus definition updates daily.
4. All networked computers are connected via CAT5 cabling. Each floor contains a locked room holding the network switches that are maintained by the College MIS Department. Access to these rooms is restricted to MIS personnel, Office of Information Technology, L2 ISM and the L3 ISM. All networked computers are connected to the network switches on its respective floor.
5. Static IP numbers are assigned by the L3 ISM of the department and by no other office. Dynamic IP's are assigned only after the machine is inventoried and a request to the DHCP Server Administrator is provided by the L3 ISM via e-mail. The dynamic IP is assigned after the machine host name and its MAC number are added to the DHCP database. Anyone found using an unauthorized IP number or an assigned IP number of another machine is forbidden and is considered computer hacking and disciplined by the rules set forth by the University IT Policy.

6. Any computer that is compromised or vulnerable to compromise must be disconnected from the network immediately until the computer is repaired either by system patches or reformatted as UF policy dictates.

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 the network resources.

The department assigns static IP numbers to department computers and network printers. Any other computer connected to the port without an IP number assigned or that is not listed in the DHCP database cannot gain access to the network.

It is forbidden for anyone other than the L3 ISM or department IT staff to assign an IP number. Refer to section 9, paragraph 5.

9.2 Managed vs Unmanaged

To be written.

9.3 User Authentication

9.3.1 Issuing and revoking user accounts

User must read and agree to the UF Acceptable Use Policy (<http://WWW.it.ufl.edu/policies/aupolicy.html>).

At this time, user authentication is performed on the Mail Server and Web Server for those who have a Web Page.

9.3.2 User Authentication

Individual computers do not have a user authentication other than the user account setup on that computer.

Preliminary planning is in the works to setup Gatorlink authentication on each computer for the future.

9.3.3 Logs

The College IT Security Policy requires user authentication be logged and the logs must be retained for at least three years. At this time the only logs kept are those from the DHCP server.

This will be a future project.

9.3.4 Pooled Resources without user accounts

Pooled resources without user accounts by design (e.g. printers) must be tracked in a manner that allows the device using a given network address (IP number) at a given time to be identified.

All network printers assigned an IP address are tracked via the department Inventory System.

9.4 Physical Plant

Each floor is serviced by switches controlled by the College MIS unit and are locked in a room on each floor.

Only authorized personnel have access to these rooms. This includes L2 ISM, L3 ISM, College MIS IT Staff and UF Network Services IT Staff.

Unused ports (wallplates) are not active by disconnection from the servicing switch. Access cannot be obtained until the L3 ISM installs a patch cable for that port or wallplate to the switch.

9.5 Department Servers

All department server administrators are required to maintain all operating system and security updates and patches. Failure to perform these maintenance functions will result in the disconnection of that server from the network.

9.5.1 DHCP Servers

The department DHCP Server is located in a locked and special air conditioned room. (514 Weil Hall)

Server Backup is run Weekly.

System Administrator is Justin Davis 352-392-9537 x1528

His office is 551 Weil Hall.

9.5.2 VPN Servers

The department does not have a VPN Server.

9.5.3 Mail Servers

The department E-Mail Server is located in a locked and special air conditioned room. (514 Weil Hall)

Server Backup is run Weekly.

System Administrator is Justin Davis at 392-9537 x1528

His office is 551 Weil Hall.

9.5.4 Web Servers

The Civil and Coastal Engineering Web Server is located in a locked and special air conditioned room. (514 Weil Hall)
Server backup is run XXXXXXXXXXXXXXXXXXXX
System Administrator is Justin Davis 392-9537 x1528
His office is 551 Weil Hall.

The CTT Center Web Server is also in 514 Weil Hall.
Server Backup is run XXXXXXXXXXXXXXXXXXXX
System Administrator is Jon Keane 392-2371 x243
His office is at 2006 NE Waldo Road.

The BSI Center Web Server is located in 457 Weil Hall.
System Administrator is Jae Chung 392-9237 x1512
Server Backup is run XXXXXXXXXXXXXXXXXXXX
His office is 457 Weil Hall.

9.5.5 DNS Servers

The Civil and Coastal Engineering DNS Server is located in a locked and special air conditioned room. (514 Weil Hall)
Server Backup is run Weekly.
System Administrator is Justin Davis 392-9537 x1528
His office is 551 Weil Hall

9.5.6 Data Servers

The Civil and Coastal Engineering Data File Server located in a locked room. (454A Weil Hall)
This Data Server is also shared by the TRC Center for file sharing.
Server Backup is run Daily.
System Administrator is Tony Murphy 392-9537 x1501
His office is 454A Weil Hall

The T2 Center Data Server is located in a locked and special air conditioned room. (514 Weil Hall)
Server Backup is run XXXXXXXXXXXXXXXXXXXX
System Administrator is Jon Keane 392-2371 x243
His office is at 2110 NE Waldo Road.

The McTrans Center Data Server is located in a locked and special air conditioned room. (514 Weil Hall)
Server Backup is run XXXXXXXXXXXXXXXXXXXX

System administrator is Phil Hill 392-0378 x236

9.6 Inbound Modems

The department does not facilitate any inbound modem access.

9.7 WIRELESS ACCESS POINTS

The department does not operate a wireless access point. There are UFW wireless access points around campus and at various points within Weil Hall supported by the University and administered by CNS and the College of Engineering L2 ISM..

No wireless access is to be installed in the department unless installed and maintained by the University Network Services department or the College of Engineering MIS department. This is University Policy, to prevent channel crossovers and interference since there are only sixteen channels available.

10. STANDARD PROCEDURES

10.1 Incident Response

10.2 User Work Stations

10.3 Business Resumption Plan (Disaster Recovery Plan)

10.4 Logon Banners

10.5 Intrusion Detection and Monitoring

10.6 Transfer of Authority

10.7 Vulnerability Scans

10.8 Software Development Standards

To be written

11. TRAINING

To be written

12. PHYSICAL SECURITY

12.1 General

12.2 Facilities

12.3 Servers

12.4 Routers, Switches and Other Network Infrastructure

12.5 Data Confidentiality

12.6 Surplus Equipment

12.7 Network Ports

To be written

13 EFFECTIVE DATE, REVISION SCHEDULE

To be written

14 DEFINITIONS

To be written

15. PERSONAL LAPTOP AND DESKTOP COMPUTERS

Students are required to have a personally owned laptop or desktop computer and can be connected to the network by DHCP if used on the premises of the CCE department and can not connect to the UFW wireless network.

It is preferred that all personally owned machines with wireless network interface capability connect to the network using the UFW wireless access points provided by the University if available in their building location.

Professors may use a personally owned machine and can be connected to the network. Personally owned machines connected to the network is a privilege extended by the department, not a right.

The user will read and sign an Application for Network Connection. By signing this application, the user agrees to abide by the rules of Acceptable Use Policy as stated by the University and the IT Security and Computer Policy of this department. The use of DHCP is controlled by recording the users MAC address, Host Name and users UF e-mail address in a database on the DHCP server. If this information is not in the database, the computer will not be given access for network connection.

Visiting professors and researchers may also be given network access at the request of the sponsoring department professor. The same rules apply as stated above.

16. COMPUTER SOFTWARE APPLICATIONS

Under no authority will the department or any unit thereof buy and install any software applications to a personally owned computer. This is the responsibility of the owner to purchase all required software applications. No UF purchased software can be installed on a personally owned computer.

Likewise, no personally owned software will be allowed to be installed on a department owned computer without the written approval of the L3 ISM and the software is not installed on any other computer. The license or receipt of purchase and the CD must be maintained by the L3 ISM and will be properly identified with the computer inventory number to which it is installed and the name of the purchaser.

Downloading shareware software from the Internet is strictly forbidden on department owned computers without the written approval of the Professor for whom will purchase the software and the L3 ISM.

Downloading freeware software can be downloaded but only with a printed document stating it is free and with the permission of the L3 ISM. Such software must be downloaded to the computer before it can be installed. For instance: Do not install any software directly from the Internet. Download by saving the installation file in a designated folder first, then execute it from that folder to install the software.

Any software found on a department computer that does not meet the following will be removed from that department computer.

The software must:

1. be purchased by the University or Department
2. be freeware with documentation stating it is free given to the L3 ISM
3. be personally owned software with the license and CD held by the L3 ISM
4. have been written by the user of the computer for project purposes
5. be authorized by the manufacturer free of cost for use in educational purposes with supporting documentation
6. not be shareware unless the supporting professor paid for it with documentation supporting the purchase.
7. be a manufacturer free Demo version that expires
8. have been transferred already installed on a computer with an incoming professor, preferably with supporting documentation or statement stating so.

17. IP SUBNETS

The department maintains access control to the network for the following Subnets:

Weil Hall and Reed Lab buildings:

128.227.72.16 through 128.227.72.254 Public IP subnet
10.227.72.16 through 10.227.72.254 Private IP subnet
10.5.72.16 through 10.5.72.254 Secondary Private IP subnet
128.227.136.16 through 128.227.136.254 Public IP subnet
10.227.136.16 through 10.227.136.254 Private IP subnet
10.245.12.11 through 10.245.12.254 Private IP subnet

Waldo Road facilities:

10.5.121.xxx through 10.5.121.xxx Private IP subnet
128.227.59.96 through 128.227.72.59.114 Public IP subnet
10.253.12.10 through 10.253.12.254 Private IP subnet

IP numbers are not assigned without the approval of the L3 ISM. An IP number can be used only for a valid reason and assigned only by the L3 ISM. Valid reasons are:

- 1) Department Servers
- 2) Network Printers
- 3) Research purposes
- 4) Any application not supporting DHCP for FLEXLM license authentication.
- 5) The computer is department owned.

DHCP usage will expire one year after assignment if designated as STUDENT. The user must renew their Application for Network Connection each year registered for classes within the department. If the designation is VISITOR, the DHCP usage will expire after the established term of their stay. If the designation is FACULTY or STAFF, the DHCP usage will expire upon termination of employment with the department.

18. COMPUTER SUPPORT

All departmental computers and printers are fully supported by the department Computer Support IT Staff.

All personally owned computers or printers used on campus are the personal responsibility of the owner. This means the owner must maintain all operating system updates and patches, install an Anti Virus application and maintain the application updates and virus definition updates. The owner of a personal computer or printer holds the department and University harmless for any liability for loss or destruction to their computer and its contents or printer. The responsibility of the department ends at the wall plate.

The department will not support personally owned computers or printers in any manner such as troubleshooting problems with hardware or software. This is the responsibility of the owner. The owner must seek service from the University's HELP DESK (392-HELP) or outside technical assistance.