



Information Technology Policies And Procedures

April 13, 2005



Introduction

University information technology resources constitute a valuable University asset that must be managed accordingly to ensure their integrity, security, and availability for teaching, research and business activities. Carrying out this mission requires the University to establish basic Information Security policies and standards and to provide both access and reasonable Security at an acceptable cost. The University Information Technology Policies and Procedures are intended to facilitate and support authorized access to University information.

The purpose of the University Information Policies and Procedures is:

- To establish University-wide Protocol for Information Security.
- To help identify and prevent the compromise of Information Security and the misuse of University information technology resources.
- To protect the reputation of the University and to allow the University to satisfy its legal and ethical responsibilities with regard to its information technology resources.
- To enable the University to respond to complaints and queries about real or perceived non-compliance with the University Information Technology Policies and Procedures.

Defined Terms

The definitions of capitalized words and phrases in these Policies and Procedures have special meanings. Their definitions appear in Appendix A and readers should review those terms prior to reading these Policies and Procedures and thereafter refer to them as needed.

Responsibility

Authorized Users of University information technology resources are personally responsible for complying with all University policies, procedures and standards relating to Information Security, regardless of campus center or location and will be held personally accountable for any misuse of these resources.



Amendments

Proposals for amendments to this document may be submitted to the Information Technology Services Department for review. If the review results in the need to amend the Information Technology Policies and Procedures Manual, Information Security personnel and the Vice President and General Counsel will draft the proposed amendment. The proposed amendment will be forwarded to the Information Technology Policies and Procedures Review Committee. Upon approval by that committee, the proposed amendment will be forwarded to the Executive Staff for review and if approved, for inclusion in the Information Technology Policies and Procedures Manual.

Approvals

This document in its initial form has received the following review and approvals from University administration:

	President	4-13-05
Beverley Byers-Pevitts, PhD	Title	Date

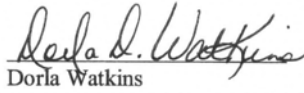
	Vice President of Finance and Administration	4-13-05
Dorla Watkins	Title	Date



Table of Contents

Unauthorized Use Policy	5
Guest User Policy	6
University Confidentiality Policy	7
Acceptable Use Policy	8
Electronic Communications Policy.....	14
Password Policy	16
Acceptable Encryption Policy.....	21
Remote Access Policy.....	22
Virtual Private Network Policy.....	25
Physical Security Policy	27
Workstation Configuration Security Policy	30
Computer Lab Security Policy	33
Server Configuration Security Policy	36
“De-Militarized Zone” Network Equipment Policy	39
Router Security Policy	43
Wireless Communication Policy.....	45
Change Management Policy	47
Information Security Audit Policy	49
Appendix A: Defined Terms.....	51



Unauthorized Use Policy

Revised: 01/20/2005

1. Purpose.

This policy sets forth the University's policy regarding Unauthorized Use of the University Information Technology Network.

2. Scope.

This policy covers all Unauthorized Use of the University Information Technology Network, whether such Unauthorized Use is done by a person who is not an Authorized User, or by an Authorized User who exceeds the limits of that person's authorization whose use exceeds Authorized Use permitted by the University, all of whom are referred to in this policy as "Unauthorized Users."

3. Policy.

All Unauthorized Users are prohibited from using University Information Technology Network for any purpose whatsoever. Authorized Users are prohibited from using the University Information Technology Network in any way that exceeds the limits of their individual authorization.

4. Enforcement.

Unauthorized Users may be subject to criminal prosecution and/or civil suits in which the University seeks damages and/or other legal and/or equitable remedies. Unauthorized Users who are employees of the University may also be subject to disciplinary action, up to and including termination of employment. Unauthorized Users who are Students at the University may also be subject to disciplinary action, up to and including expulsion from the University.



Guest User Policy

Revised: 01/20/2005

1. Purpose.

The University promotes sharing and learning within the academic community. In doing so, the University often grants to University guests and visitors the right to use its information technology resources in compliance with the University Information Technology Policies and Procedures. Such authorized persons are Guest Users and are also Authorized Users to the extent of their authorization.

2. Scope.

This policy applies only to any Guest Users and does not include faculty, staff, or Students.

3. Policy.

A Guest User is an Authorized User when utilizing the University's information technology resources in compliance with the University Information Technology Policies and Procedures and as long as the use remains within the limits of the Guest User's individual authorization. The Guest User may be authorized to use computers in the University's computer labs and selected Software. The Guests may also be permitted to selected areas of the University's Information Technology Network.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



University Confidentiality Policy

Revised: 01/20/2005

1. Purpose.

Confidential information may be developed or obtained by University employees/interns/work study Students as a result of that person's relationship with the University.

2. Scope.

All Authorized Users who have contact with and access to confidential information must keep such information confidential. Confidential information includes, but is not limited to, the following types of information:

- Student and employee information, such as address, telephone number, social security number, birth date and other private information.
- Operations manuals, University practices, marketing plans, techniques and materials, development plans, and financial information
- Student or applicant lists, grades, personnel and payroll records, records regarding vendors and suppliers, records and files of the University, and other information concerning the business affairs or operating practices of the University.

3. Policy.

Confidential information must never be released, removed from the University premises, copied, transmitted, or in any other way used by the Authorized User for any purpose outside the scope of their University employment, nor revealed to non-University employees, without the express written consent of University management personnel.

Information stored on the University Information Technology Network is confidential and may not be distributed outside the University except in the course of the University's business or as otherwise authorized by management personnel. Authorized Users may not remove or borrow from the University premises any computer equipment, disks, or related technology, product or information unless authorized to do so.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Acceptable Use Policy

Revised: 01/20/2005

1. Overview.

This policy is intended to protect the University's faculty, employees, Students and employees as well as the University from the consequences of illegal or damaging actions by individuals using the University Information Technology Network.

The University Information Technology Network includes: Internet/Intranet/Extranet-related systems, including but not limited to computer/Networking equipment, Software, Operating Systems, storage media, Network accounts providing electronic mail, Instant Messaging, student information system, WWW browsing, and FTP, which are the property of the University. They are to be used for University business purposes and to serve the interests of the University, and as well as all Authorized Users. Effective computer Security is a team effort requiring the participation and support of every University faculty member, employee, student and Authorized User who deals with information and/or information systems. It is the responsibility of every computer user to know the University Information Technology Policies and Procedures, and to comply with the University Information Technology Policies and Procedures.

2. Purpose.

This policy describes the Authorized Use of the University Information Technology Network and protects the University and Authorized Users. Unauthorized uses expose the University to many risks including legal liability, Virus attacks, and the compromise of Network systems, Services, and information.

3. Scope.

This policy applies to all persons with a Park University-owned, third party-owned, or personally-owned computing device that is connected to the University Information Technology Network.



4. Policy.

a. General Use and Ownership.

1. Data created by Authorized Users that is on the University Information Technology Network is the property of the University. There is no guarantee that information stored on the University Information Technology Network device will be confidential.
2. Authorized Use includes reasonable personal use of the University Information Technology Network by Authorized Users. University departments are responsible for creating guidelines concerning personal use of the University Information Technology Network. In the absence of such guidelines, employees should consult their supervisor, manager, or the Information Security Guidelines; Students should consult the Student Assistance Center.
3. Any information that an Authorized User considers to be sensitive or vulnerable should be encrypted. For guidelines on information classification, see Information Security's Information Sensitivity Policy. For guidelines on encrypting Email and documents, consult Information Security's Awareness Initiative.
4. Authorized University employees may monitor the University Information Technology Network traffic at any time, in accordance with the Information Security Audit Policy.
5. The University reserves the right to audit Networks and systems on a periodic basis to ensure compliance with the University Information Technology Policies and Procedures.

b. Security and Proprietary Information.

1. Authorized Users are required to classify the user interface for information contained on the University Information Technology Network as “confidential” or “not confidential,” as defined by University Confidentiality Guidelines. Confidential information includes, but is not limited to: University private data, specifications, student information, and research data. Employees are required to take all necessary steps to prevent unauthorized access to this Sensitive Information.



2. Authorized Users are responsible for the Security of their passwords and accounts and must keep passwords confidential and are not permitted to share accounts.
 3. Authorized Users are responsible for logging out of all systems and accounts when they are not being used; they must not be left unattended.
 4. All laptops and workstations that are part of or connected to the University Information Technology Network are required to be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the device will be unattended.
 5. Encryption of information must be used in compliance with Information Security's Acceptable Encryption Use Policy.
 6. Authorized Users are required to exercise special care to protect laptop computers that are part of or connected to the University Information Technology Network in accordance with the "Laptop Security Guidelines."
 7. Postings by Authorized Users from a University Email address must contain a disclaimer stating that the opinions expressed are strictly those of the author and not necessarily those of the University, unless posting has been done in the course of University business.
 8. All computers used by Authorized Users that are connected to the University Information Technology Network, whether owned by the individual or the University, must be continually executing approved Virus-scanning Software with a current Virus Database.
 9. Authorized Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain Viruses, e-mail bombs, or Trojan Horse codes.
- c. Unacceptable Use of the University Information Technology Network.

The following activities are prohibited, although University employees who are Authorized Users may be exempted from these restrictions during the performance of their legitimate job responsibilities. Under no circumstances is an Authorized User permitted to engage in any activity



that is illegal under local, state, federal or international law while utilizing the University Information Technology Network.

Unacceptable use includes, but is not limited to the following activities:

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other Intellectual Property, or similar laws or regulations, including, but not limited to, the installation or distribution of copyrighted or other Software products that are not licensed for use by the University.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted Software for which the University or the Authorized User does not have an active license is strictly prohibited.
3. Exporting Software, technical information, Encryption Software or technology, in violation of international or regional export control laws, is illegal. University management must be consulted prior to export of any material that is in question.
4. Introduction of Malicious Software into the University Information Technology Network (e.g., Viruses, Worms, Trojan Horses, e-mail bombs, etc.).
5. An Authorized User's revelation of that person's account password to others or allowing use of an Authorized User's account by others, including family and other household members when an Authorized User's computer is connected to the University Information Technology Network from home or other non-University locations.
6. The use of a component of the University Information Technology Network or other computing asset to actively engage in procuring or transmitting material that violates sexual harassment or hostile



workplace laws or that violates any University policy. Pornographic material is a violation of sexual harassment policies.

7. Making fraudulent offers of products, items, or services originating from any University account or otherwise made from a computer connected to the University Information Technology Network.
8. Causing Security breaches or disruptions of communication over the University Information Technology Network. Security breaches include, but are not limited to, accessing data or other communications of which the Authorized User is not an intended recipient or logging into an account that the Authorized User is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, Network Sniffing, traffic floods, Packet Spoofing, Denial of Service, etc.
9. Port Scanning or Security Scanning is expressly prohibited unless prior notification to Information Security is made.
10. Executing any form of Network monitoring which will intercept data not intended for the Authorized User is expressly prohibited, unless this activity is a part of the Authorized User's normal job/duty.
11. Circumventing User Authentication or Security of any device, Network, or account.
12. Interfering with or denying Service to any user other than the individual's Host (for example, a Denial of Service attack).
13. Using any Program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means locally or remotely.
14. Providing information about, or lists of, University employees or Students to non-University parties.

Email and Communications Activities

1. Sending unsolicited Email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (Email SPAM).



2. Any form of harassment via Email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of Email header information.
4. Solicitation of Email for any other Email address, other than that of the Authorized User's own account, with the intent to harass or to collect replies.
5. Creating or forwarding Chain email, Phishing, or other scams of any type.
6. Use of the University's name in any unsolicited Email on behalf of, or to advertise, any service or product without the explicit written permission of the University.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).

5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Electronic Communications Policy

Revised: 01/20/2005

1. Purpose.

Electronic communications systems that utilize the University Information Technology Network are not an open forum, but rather are owned and operated by the University to promote teaching and learning, and to conduct official University business. Authorized Users may use these systems only within the scope of University Information Technology Policies and Procedures. Electronic communication systems include, but are not limited to: all electronic mail and Instant Messaging systems, electronic bulletin boards, web content, and Internet access.

2. Scope.

This policy covers appropriate use of any electronic message sent from a University account, and applies to all Authorized Users of the University Information Technology Network.

3. Policy.

Prohibited Use

The University Email system must not to be used for the creation or distribution of any disruptive or offensive messages, including but not limited to: offensive comments about race, gender, disability, age, sexual orientation, religious belief and practice, political belief, or national origin. Individuals who receive any electronic communications with objectionable content should report the matter to their supervisor or to Information Security personnel immediately.

Personal Use

Authorized Users may use a reasonable amount of University resources for personal Emails. However, non-work related Email shall be saved in a separate folder from work related Email. Sending Chain Email or joke Emails from a University Email account is prohibited. These restrictions also apply to the forwarding of Email received by an Authorized User.

Mass Emailings

Mass Emailings over the University Information Technology Network from the University must be approved by the Office of the President or a University Vice President before sending. The approval must be noted at the bottom of the Email



and must include the name of the approving individual and the date of approval. Emergency Mass Emailings may be sent with director approval. Examples of Mass Emailings include, but are not limited to, sending to the “All Campus Email Users” group or any group of Students. Emails sent by faculty members who are Authorized Users to their current Students are permitted.

Signatures

Signatures in Emails and other electronic messages may contain some or all of the following only: name, title, department name, name of University, and workplace contact information (phone number, fax number, mailing address, Email address). Quotations, such as proverbs, witticisms, etc., are not allowed in signatures.

Monitoring

Authorized Users of University accounts shall have no expectation of privacy in anything they store, send or receive in a University’s Information Technology Network. The University may monitor communication on the University Information Technology Network without prior notice, but is not obliged to do so.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Password Policy

Revised: 01/20/2005

1. Overview.

Passwords are essential to computer Security. They are the front line of protection for Authorized User accounts. A poorly chosen password can result in the compromise of the entire University Information Technology Network. All Authorized Users are responsible for taking the actions outlined below, to select and secure their passwords.

2. Purpose.

The purpose of this policy is to establish a standard for creation and protection of strong passwords for Authorized Users of information technology resources on the University Information Technology Network. This policy will also establish the frequency of change for those passwords.

3. Scope.

The scope of this policy includes all Authorized Users who are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University facility, accesses the University Information Technology Network, or stores any non-public University information.

4. Policy.

General

- All system-level passwords (e.g. the "root" account on UNIX-based Operating Systems, the "enable" functionality of Routers, the Windows "administrator" account, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All system-level passwords on all equipment must be part of the University Password Management System.
- All user-level passwords (e.g. Email, web, desktop computer, etc.) must be changed at least every sixty days.
- Authorized User accounts that have system-level privileges granted through group memberships or Programs such as "sudo" or "SU" must have a unique password that is different from all other accounts held by that Authorized User.
- Passwords must not be included in Email messages, phone conversations, or other forms of electronic communication.



- Where Simple Network Messaging Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults ("public," "private," or "system") and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g. SNMP version 2).
- All user-level and system-level passwords must conform to the guidelines described below.

Standards

a. General Password Construction Guidelines

Passwords are used for various purposes at the University. Some of the more common uses include: user-level accounts, web accounts, Email accounts, screen saver protection, voice mail passwords, and local Router logins. Very few systems have support for one-time Tokens (i.e. dynamic passwords which are only used once), thus everyone must be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word, such as:
 - Names of family members, pets, friends, co-workers, fictional characters, etc.
 - Computer terms and names, commands, sites, companies, Hardware and Software terms
 - The words "Park University", "sanjose", "sanfran" or any derivation
 - Birthdays and other personal information, such as addresses and phone numbers
 - Word or number patterns like aaabbb, qwerty, xyzy, 123321, etc.
 - Any of the above spelled backwards
 - Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

Strong passwords have the following characteristics:

- The password contains both upper and lower case characters (e.g. a-z, A-Z)
- The password has digits and punctuation characters as well as letters, if possible
(e.g. 0-9, !@#\$%^&*()_+|~-=\`{}[]:"';<>?,./)
- The password is at least eight alpha-numeric characters long
- The password is not a word in any language, slang, dialect, jargon, etc.
- The password is not based on personal information, names of family, etc.



Passwords must never be written down or stored on-line. Passwords should be created so that they can be easily remembered while still having strong password characteristics. One way to do this is to create a password derived from a song title, affirmation, or other phrase. For example, the phrase might be "This May Be One Way To Remember" and the corresponding password might be "TmB1w2R!", or "Tmb1W>r~", or some other variation.

NOTE: These particular examples are now public, and must not be used as real passwords!

b. Password Protection Standards

Authorized Users must not use the same password for University accounts as for other non-University access (e.g. personal ISP account, option trading, benefits, etc.). Wherever possible, the same password must not be used for various University access needs. For example, the password for the CARS systems must be separate from the password for other Information Technology systems. Also, a separate password must be selected for a Windows account and a UNIX account.

University passwords must not be shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as confidential University information. Groups accounts (an account shared among two or more users) are prohibited.

Users must not do the following:

- Passwords must not be revealed or hinted at over the phone to anyone without proper verification, in an Email message which includes the user name, to any supervisors or co-workers, on questionnaires or Security forms, or to family members.
- The "Remember Password" feature of applications (e.g. Eudora, Outlook, or Netscape Messenger) must not be used.

If someone demands a password, they should be referred to this document or they should call Information Security personnel.

Again, passwords must not be written down and stored anywhere by the Authorized User. Passwords must not be stored in a file on ANY computer system (including Palm Pilots or similar devices) without Encryption.

If an account or password is suspected to be compromised, the incident must be reported to Information Security personnel and the password must be changed immediately.



Password Cracking or guessing may be performed on a periodic or random basis by Information Security personnel. If a password is guessed or cracked during one of these scans, the user will be required to change it.

c. Application Development Standards

Application developers must ensure their Programs contain the following Security precautions:

- Applications must support User Authentication of individual Authorized Users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must provide for some sort of role management, so that one Authorized User can take over the functions of another without having to know the other's password.
- Applications should support advanced User Authentication systems (e.g. RADIUS), wherever possible.

d. Use of Passwords and Pass-phrases for Remote Access Users

Remote Access to the University Information Technology Network must be controlled using either one-time password authentication or a public / private key system with a strong Pass-phrase.

e. Pass-phrases

Pass-phrases are generally used for public / private key authentication. A public / private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the Authorized User. Without the Pass-phrase to "unlock" the private key, the Authorized User cannot gain access.

Pass-phrases are not the same as passwords. A Pass-phrase is a longer version of a password and is, therefore, considered more secure. A Pass-phrase is typically composed of multiple words. Because of this, a Pass-phrase is more secure against "dictionary attacks."

A good Pass-phrase is relatively long and contains a combination of upper- and lower-case letters, numerals, and punctuation characters. The following is an example of a good Pass-phrase:

"R34d car3fu!!y. B3 h0n3\$t."



All of the rules above that apply to passwords, also apply to Pass-phrases.

5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Acceptable Encryption Policy

Revised: 01/20/2005

1. Purpose.

The purpose of this policy is to limit the use of Encryption by Authorized Users to methods that receive substantial public review and work effectively. Additionally, this policy provides direction to ensure compliance with Federal regulations, and to ensure legal authority is granted for the dissemination and use of Encryption technologies outside of the United States.

2. Scope.

This policy applies to all Authorized Users including Park University employees and affiliates.

3. Policy.

Proven, standard Encryption methods (e.g. DES, Blowfish, RSA, RC5, IDEA, etc.) must be used as the basis for Encryption technologies. These methods represent the actual Cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) technology uses the IDEA method in combination with RSA or Diffie-Hellman methods, while Secure Socket Layer (SSL) technology uses RSA Encryption. Symmetric Cryptosystem key lengths must be at least 128 bits. Asymmetric Cryptosystem keys must be of a length that yields equivalent strength. Park University's key length requirements are reviewed annually and upgraded as technology allows.

Authorized Users may not use Proprietary Encryption Algorithms for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Information Security personnel. Be aware that the export of Encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States need to be aware of the Encryption technology laws of the country in which they reside.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Remote Access Policy

Revised: 01/20/2005

1. Purpose.

This policy defines standards for connecting to the University Information Technology Network from any Host. These standards are designed to minimize potential exposure of the University to damages that result from Unauthorized Use of the University Information Technology Network. Damages include, but are not limited to: the loss of sensitive or confidential data, loss of Intellectual Property, damage to the University's public image, damage to the University's internal systems, and financial damages of all kinds.

2. Scope.

This policy applies to all Authorized Users including University faculty, staff, Students, employees and affiliates, who utilize University-owned or personally-owned information technology resources to connect such devices to the University Information Technology Network. This policy applies to Remote Access connections used to do work on behalf of the University, including but not limited to Email correspondence and accessing Intranet web resources.

Remote Access implementations that are covered by this policy include, but are not limited to: dial-up Modems, Frame Relays, Integrated Services Digital Network (ISDN) connections, Digital Subscriber Line (DSL) connections, Cable Modems, etc.

3. Policy.

General

1. Authorized Users with Remote Access privileges to the University Information Technology Network must ensure that their Remote Access connection complies with the University Information Technology Policies and Procedures, and treat it with the same consideration as their on-site connection to the University.
2. General access to the Internet through the University Information Technology Network, for reasonable recreational use by immediate household members of University on personal computers, is permitted. Each Authorized User is responsible for ensuring that the family members comply with the University Information Technology Policies and Procedures, does not perform illegal activities, and does not use the access for outside business purposes. Each Authorized User bears responsibility for any consequences of misuse.
3. Authorized Users must review the following policies to determine how to protect information when accessing the University Information Technology



- Network via Remote Access methods, and for acceptable use of the University Information Technology Network:
- a. The University Acceptable Encryption Policy
 - b. The University Virtual Private Network Policy
 - c. The University Wireless Communications Policy
 - d. The University Acceptable Use Policy
4. For additional information regarding the University's Remote Access connections, Authorized Users should contact the Information Technology Services department.

Requirements

1. Secure Remote Access must be strictly controlled. Control will be enforced via one-time password authentication or public / private keys with strong Pass-phrases. For information about how to create a strong Pass-phrase, Authorized Users should refer to the Password Policy.
2. Authorized Users must not provide their login identification to the University Information Technology Network or its resources to anyone, not even family members.
3. Authorized Users who, as a University employee or affiliates with Remote Access privileges, must ensure that University-owned or personal information technology resources are not connected to any other Network at the same time they are connected to the University Information Technology Network (with the exception of personal Networks that are under the complete control of the Authorized User).
4. Authorized Users who, as a University employee or affiliates with remote Authorized User access privileges to the University Information Technology Network must not use non-University Email accounts (e.g. Hotmail, Yahoo, and AOL) or other external resources to conduct University business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the University Information Technology Network must meet the minimum authentication requirements of the Challenge Handshake Authentication Protocol (CHAP).
6. Reconfiguration of an Authorized User's home equipment for the purpose of Split-Tunneling or Dual Homing is not permitted.
7. Frame Relay must meet the minimum authentication requirements of Data-Link Connection Identifier (DLCI) standards.
8. Non-standard Hardware configurations must be approved by Information Technology Services personnel, and Information Security personnel must approve Security configurations for access to Hardware.
9. All Hosts that are connected to the University Information Technology Network via Remote Access technologies, including personal computers, must use the most recent corporate-standard Anti-Virus Software. Third-party connections to the University Information Technology Network must comply with requirements as stated in the Third Party Agreement documentation.



10. Personal equipment that is used to connect to the University Information Technology Network must meet the same requirements applied to University-owned equipment for Remote Access.
 11. Organizations or Authorized Users who wish to implement non-standard Remote Access solutions to the University Information Technology Network must obtain prior written approval from the Information Technology Services department.
4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Virtual Private Network Policy

Revised: 01/20/2005

1. Purpose.

This Policy provides standards for Remote Access by Authorized Users to the University Information Technology Network via Virtual Private Network (VPN) connections, using the IP Security (IPSec) or Layer 2 Tunneling Protocols.

2. Scope.

This policy applies to all Authorized Users utilizing VPNs to access the University Information Technology Network. This policy also applies to implementations of VPN that are directed through an IPSec concentrator.

3. Policy.

Authorized Users who are reviewed by the Information Technology Services department may utilize Virtual Private Networks. A VPN is a “user-managed” Service, in which the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation of the Service as well as any required Software, and paying all fees. Further details may be found in the Remote Access Policy documentation.

1. It is the responsibility of the Authorized VPN User to ensure that Unauthorized Users are not allowed access to the University Information Technology Network.
2. Authorized Users must be in compliance with the Password Policy.
3. When actively connected to the University Information Technology Network, the VPN Software forces all traffic to and from the user’s information technology resource over the VPN tunnel. All other traffic is dropped.
4. Dual (or split) tunneling is not permitted. Only one Network connection is allowed.
5. VPN gateways must be set up and managed by Information Technology Services personnel.
6. All information technology resources connected to the University Information Technology Network by Authorized Users via VPN or any other technology must use the most recent corporate-standard Anti-Virus Software.
7. Authorized VPN Users are automatically disconnected from the University Information Technology Network after thirty minutes of inactivity. The Authorized VPN User must then log on again to reconnect to the University Information Technology Network. Pings or other artificial Network processes must not be used to keep the connection open. Special consideration for campus centers will be granted.



8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Authorized Users of information technology resources that are not owned by the University must configure their resources to comply with the University's VPN and Network Policy documentation.
10. Only VPN clients utilized by Authorized Users and approved by appropriate Information Security personnel can be used.
11. By using VPN technology with personal equipment, Authorized Users must understand that their machines are a de-facto extension of the University Information Technology Network, and as such are subject to the same rules and regulations that apply to equipment owned by the University (i.e. their machines must be configured to comply with University Information Technology Policies and Procedures documentation).

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Physical Security Policy

Revised: 01/20/2005

1. Overview.

Physical Security means providing environmental safeguards for, and controlling physical access to, equipment and data on the University Information Technology Network in order to protect information technology resources from Unauthorized Use, in terms of both physical Hardware and data perspectives.

2. Purpose.

The purpose of this policy is to establish standards for granting, monitoring, and terminating physical access to the University Information Technology Network and to protect equipment on the University Information Technology Network from environmental factors.

3. Scope.

This policy applies to the entire University Information Technology Network, including but not limited to computer labs, Network Closets, and the Information Technology Services Network Operations Center.

4. Policy.

Environmental Safeguards

1. Adequate air conditioning must be operational in University Information Technology Network facilities that house information technology resources, to prevent long-term heat damage and equipment failure.
2. All University Information Technology Network facilities must have adequate fire extinguishing devices present in the office area. These devices must be inspected by University Public Safety personnel.
3. All University Information Technology Network information technology resources must be fitted with effective Surge Protectors to prevent power spikes and subsequent damage to data and Hardware.
4. Critical University Information Technology Network information technology resources must each be connected to an Uninterrupted Power Supply (UPS) in order to prevent power spikes, brownouts, and subsequent damage to data and Hardware.
5. Electrical outlets must not be overloaded by connecting too many devices. Proper and practical usage of extension cords are to be reviewed annually.
6. Water sensors must be placed under any raised floor.



Physical Access

1. All University Information Technology Network physical Security systems must comply with all regulations, including, but not limited to, building codes and fire prevention codes.
2. Physical access privileges to all University Information Technology Network facilities must be documented and managed by Information Technology Services.
3. All facilities that house University Information Technology Network information technology resources must be physically protected in proportion to the importance of their function.
4. Access to University Information Technology Network restricted facilities will be granted only to University staff and affiliates whose job responsibilities require access to that facility.
5. The process for granting card or key access to University Information Technology Network facilities must include approval from the University Director of Information Technology Services.
6. Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or loaned to others by Authorized Users.
7. Secured access devices that are no longer needed must be returned to the University Information Technology Services department, and logged appropriately before they are re-allocated to another Authorized User.
8. Lost or stolen University Information Technology Network secured access devices must be reported to Information Security personnel immediately.
9. The University Employees responsible for University Information Technology Network facilities must remove the secured access device rights of individuals that no longer require access.
10. University Visitors and other invitees must be escorted and monitored while in restricted University Information Technology Network facilities.
11. University Employees responsible for University Information Technology Network facilities must review access records and visitor Logs for the facility on a periodic basis, and investigate any unusual access.
12. All spaces housing information technology resources must be kept locked when not occupied by a University Employee, in order to reduce the occurrence of unauthorized entry and access.
13. Any piece of University Information Technology Network equipment which resides in a public access area must be secured to a piece of furniture, counter-top, or other suitably deterrent object with a theft-inhibiting device. Portable computers that are part of the University Information Technology Network must also be secured with theft-inhibiting devices.



5. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Workstation Configuration Security Policy

Revised: 01/20/2005

1. Purpose.

The purpose of this policy is to establish standards for the base configuration of workstations that are owned or operated by the University. Effective implementation of this policy will minimize unauthorized access to the University Information Technology Network and other Proprietary Information and technology.

2. Scope.

This policy applies to all University Information Technology Network workstation equipment owned or operated by the University, and to workstations registered under any University-owned internal Network domain.

3. Policy.

Ownership and Responsibilities

All University Information Technology Network workstations at the University must be the responsibility of an operational group that is responsible for system administration. Approved workstation configuration standards must be established and maintained by each operational group, based on business needs. Operational groups must monitor configuration compliance and request special approval for any noted exceptions. Each operational group must establish a process for changing the configuration standards, which includes review and approval by appropriate Information Security personnel.

1. Workstations must be registered within the University Security Management System. At a minimum, the following information is required to positively identify the point of contact:
 - a. Workstation contact(s) and location, and a backup contact
 - b. Hardware and Operating System (OS) version numbers
 - c. Main functions and applications, if applicable
2. Information in the University Security Management System must be kept current.
3. Configuration changes for workstations must comply with the Change Management Policy documentation.



General Configuration Standards

1. OS configuration must comply with approved Information Security Standards.
2. Services and applications that are unused must be disabled where practical. Exceptions must be noted and approved by authorized Information Security personnel.
3. Access to Services must be protected through authorized access-control methods (e.g. TCP wrappers), if possible.
4. The most recent Security Patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
5. Trust Relationships between systems constitute a Security risk, and their use should be avoided and should not be used when another method of communication will suffice.
6. The standard Security principle of Least Required Access must be utilized when performing a function.
7. If a methodology for Secure Channel connection is available (i.e. technically feasible), privileged access must be performed over Secure Channels (e.g. encrypted Network connections using IPSec or Secure Shell).

Monitoring

Security-related events must be reported to appropriate Information Security personnel, who review Logs and report incidents to management-level personnel in the Information Technology Services department. Corrective measures are prescribed as needed. Security-related events include (but are not limited to):

1. Port scan attacks
2. Evidence of unauthorized access to privileged accounts or data
3. Anomalous occurrences that are not related to specific applications on the Host

Compliance

1. Audits are performed on a regular basis by authorized parties within the University.
2. Audits are managed by the University's internal audit group or appropriate Information Security personnel, in accordance with the Audit Policy documentation. Findings not related to a specific operational group are filtered by Information Security personnel, and then presented to the appropriate support staff for remediation or justification.
3. Reasonable efforts are made to prevent audits from causing operational failures or disruptions.



4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Computer Lab Security Policy

Revised: 01/20/2005

1. Purpose.

This policy establishes University Information Technology Network Information Security requirements for the University Computer Labs, to ensure that confidential information and technologies are not compromised, and to ensure that production Services and other University interests are protected from University computer lab activities.

2. Scope.

This policy applies to all University Computer Labs, as well as all Authorized Users who use the University Computer Labs. All existing and future equipment, which falls under the scope of this policy, must be configured in accordance with the following requirements.

3. Policy.

Ownership Responsibilities

1. University Computer Lab operational groups are composed of faculty and staff members designated as managers of one or more computer labs. An operational group may consist of members from several departments.
2. University Computer Lab operational groups are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. University Computer Lab owners must maintain current POC information with the Information Technology Services department.
3. University Computer Lab managers are responsible for the Security of their labs and the labs' impact on the University Information Technology Network and non-University Networks.
4. University Computer Lab managers are responsible for assuring the labs' and Authorized Users' compliance with all University Security policies. The following policies are particularly important: Acceptable Use Policy, Password Policy, Wireless Security Policy, Anti-Virus Policy, and Physical Security Policy. Where policies and procedures lack specificity, lab managers must do their best to safeguard the University from security Vulnerabilities.
5. University Computer Lab managers are responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or authorized designee.
6. The Information Technology Services Department must maintain a Firewall device between the University Information Technology Network and all lab equipment.



7. The Information Technology Services Department and Information Security personnel have the right to interrupt lab connections that negatively impact the University Information Technology Network.
8. All lab Internet Protocol (IP) addresses are recorded by the Information Technology Services department. These IP addresses, which are routed within the University Information Technology Network, are stored in a University Address Management System along with current contact information for that lab.
9. Any University Computer Lab operational group that desires additional external connections to other Network segments must provide a diagram and documentation to appropriate Information Security personnel with a business justification, the equipment, and the IP address space information. Information Security personnel will review the provided documentation for Security concerns, and must approve the implementation of such connections.
10. All Authorized User passwords must comply with the University's Password Policy documentation.
11. No University lab shall provide production Services. These must be managed by the Information Technology Services department.

General Configuration Requirements

1. All traffic between the University Information Technology Network and the University Computer Lab Networks must go through a Firewall maintained by the Information Technology Services department. University Computer Lab Networks, wireless or physical, must not circumvent the Firewall.
2. Original Firewall configurations and any changes to them must be reviewed and approved by appropriate Information Security personnel. Security improvements are requested by Information Security personnel as needed.
3. Authorized Users utilizing University Computer Labs are prohibited from engaging in port Scanning, Network Auto-Discovery, Traffic Flooding, and other similar activities that negatively impact the University Information Technology Network or non-University Networks.
4. Traffic between the University Information Technology Network and the University Computer Lab Networks is permitted based on business needs, as long as the traffic does not negatively impact other Networks. Authorized Users utilizing University Computer Labs must not advertise Network Services that may compromise the University Information Technology Network or put confidential information at risk.
5. Information Security personnel have the right to audit University Computer Lab-related data and administration processes at any time, including, but not limited to: in-bound and out-bound packets, Firewalls, Network peripherals, etc.



6. Network devices within University Computer Labs must comply with all University product Security advisories and must be authenticated against University-provided authentication servers.
 7. The “enable” password for all University Computer Lab Network devices must be different from all other equipment passwords in such lab. The password must comply with the University's Password Policy, and must only be provided to those Authorized Users who are authorized to administer the University Computer Lab Network.
 8. In University Computer Labs where non- University personnel have physical access (e.g., training labs), direct connectivity to the University Information Technology Network is not allowed. Additionally, no Authorized User may enter confidential information into nor permit such confidential information to reside on any information technology resources in University Computer Labs. Connectivity for authorized personnel from University Computer Labs can be allowed to the University Information Technology Network only if authenticated against University-provided authentication servers, temporary access lists (lock and key), Secure Shell (SSH), Virtual Private Networks (VPNs), or similar technology approved by appropriate Information Security personnel.
 9. Infrastructure devices (e.g. IP Phones) needing University Information Technology Network connectivity must adhere to the Open Areas Policy.
 10. All University Computer Lab Networks with external connections must not be connected to the University Information Technology Network or any other internal Network directly, via a wireless connection, or via any other form of computing equipment.
4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Server Configuration Security Policy

Revised: 01/20/2005

1. Purpose.

The purpose of this policy is to establish standards for the base configuration of server equipment that is owned or operated by the University. Effective implementation of this policy will minimize Unauthorized Use of the University Information Technology Network or other access to the University's Proprietary Information and technology.

2. Scope.

This policy applies to server equipment owned or operated by the University, and to servers registered under any University-owned internal Network domain.

This policy applies specifically to equipment connected to the internal University Information Technology Network. For secure configuration of equipment external to the University on the "De-Militarized Zone" (DMZ), refer to the University "De-Militarized Zone" Equipment Policy documentation.

3. Policy.

Ownership and Responsibilities

All internal servers deployed at the University must be the responsibility of an Operational Group that is responsible for system administration. Approved server configuration standards must be established and maintained by each Operational Group, based on business needs. Operational Groups must monitor configuration compliance and request special approval for any noted exceptions. Each Operational Group must establish a process for changing the configuration standards, which includes review and approval by Information Security personnel.

1. Servers must be registered within the University Security Management System. At a minimum, the following information is required to positively identify the point of contact:
 - a. Server contact(s) and location, as well as a backup contact
 - b. Hardware and Operating System (OS) version numbers
 - c. Main functions and applications, if applicable
2. Information in the University Security Management System must be kept current.
3. Configuration changes made by Authorized Users for production servers must comply with the Change Management Policy documentation.



General Configuration Standards

1. OS configuration must be in accordance with approved Information Security Standards.
2. Services and applications that are unused must be disabled where practical. Exceptions must be noted and approved by Information Security personnel.
3. Access to Services must be logged or protected through appropriate Access Control methods (e.g. TCP wrappers), if possible.
4. The most recent Security Patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
5. Trust Relationships between systems are a Security risk, and their use should be avoided. Do not use a Trust Relationship when some other method of communication will do.
6. Authorized Users must always use the standard Security principle of Least Required Access to perform a function.
7. If a methodology for Secure Channel connection is available (i.e. technically feasible), privileged access must be performed over Secure Channels (e.g. encrypted Network connections using IPSec or Secure Shell).
8. All servers must be physically located in an access-controlled environment.
9. Authorized Users are specifically prohibited from operating servers in uncontrolled office areas.

Monitoring

1. All Security-related events on critical or sensitive systems must be logged by Information Security personnel and audit trails saved as follows:
 - a. All Security-related Logs must be kept online as required in the specific server standards document.
 - b. Daily incremental tape Backups must be retained as required in the specific server standards document.
 - c. Weekly full tape Backups of Logs must be retained as required in the specific server standards document.
 - d. Monthly full Backups must be retained as required in the specific server standards document.
2. Security-related events must be reported by Authorized Users to Information Security personnel, who review Logs and report incidents to management-level personnel in the Information Technology Services department. Corrective measures are prescribed as needed.



Security-related events include, but are not limited to:

- a. Port scan attacks
- b. Evidence of unauthorized access to privileged accounts or data
- c. Anomalous occurrences that are not related to specific applications on the Host

Compliance

1. Audits must be performed on a regular basis by authorized parties within the University.
2. Audits must be managed by the internal audit group or Information Security personnel, in accordance with the Audit Policy documentation. Findings not related to a specific Operational Group are filtered by Information Security personnel, and then presented to the appropriate Information Technology Services staff for remediation or justification.
3. Every effort will be made to prevent audits from causing operational failures or disruptions.
4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



“De-Militarized Zone” Network Equipment Policy

Revised: 01/20/2005

1. Purpose.

University information technology resources that connect directly to the Internet are considered part of a "De-Militarized zone" (DMZ) on the University Information Technology Network. These resources are particularly vulnerable to attack since they are directly accessible from the Internet.

The purpose of this policy is to articulate standards that govern the use of all University Information Technology Network information technology resources, which are located within a University DMZ Network. These standards are designed to minimize the exposure of the University from the loss of sensitive or confidential data, Intellectual Property, damage to the University's public image, etc., which may result from Unauthorized Use of University Information Technology Network information technology resources.

The policy defines the following standards:

- Operational Group responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirements

2. Scope.

All University Information Technology Network information technology resources deployed in a DMZ owned or operated by the University, including but not limited to servers, Routers, or switches, must be operated in accord with this policy. Additionally, all information technology resources registered in any Domain Name System (DNS) domain owned by the University are subject to this policy. Any devices outsourced or hosted at third-party service providers, if said information technology resources reside in the "park.edu" domain or appear to be owned by the University, are also subject to this policy.

All new University Information Technology Network equipment that is subject to this policy must be configured according to the applicable configuration documents, unless a waiver is obtained from University Information Security personnel. All existing and future University Information Technology Network equipment deployed on a University DMZ Network must comply with this policy.



3. Policy.

Ownership and Responsibilities

University Information Technology Network equipment and applications within the scope of this policy must be administered by the Information Technology Services department, and be approved by authorized Information Security personnel for DMZ-level management of the relevant system, application, or Network access.

The Information Technology Services department is responsible for the following:

1. Documenting equipment in the University Security Management System, recording at least the following information:
 - a. Host contacts and location
 - b. Hardware and Operating System version numbers
 - c. Main functions and applications
 - d. Password groups for privileged passwords
2. Assuring that University Information Technology Network interfaces have appropriate DNS records (minimum of A and PTR records).
3. Assuring that password groups are maintained in accordance with the University Password Management System and the Password Policy.
4. Assuring that immediate access to University Information Technology Network equipment and system Logs is granted to Information Security personnel upon demand, in accordance with the Audit Policy.
5. Assuring that changes to University Information Technology Network existing equipment and deployment of new equipment comply with the University Change Management System and comply with the Change Management Policy.

To verify compliance with this policy, University Information Security personnel periodically perform an audit on DMZ equipment as set forth in the Audit Policy.

General Configuration Policy

All University Information Technology Network equipment must comply with the following configuration policy:

1. Hardware, Operating Systems, Services and applications must be approved by University Information Security personnel, as part of the pre-deployment review phase.



2. Operating System configuration must be done in accord with the secure server and Router installation and configuration standards, as defined in the Server Configuration and Workstation Configuration policy.
3. All Patches and updates recommended by the equipment vendor and Information Security personnel must be installed. This applies to all Services installed, even though those Services may be temporarily or permanently disabled. Operational Groups must have processes in place to stay current on appropriate Patches and updates.
4. Services and applications not serving business requirements must be disabled.
5. Trust Relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by University Information Security personnel.
6. Services and applications not for general access must be restricted by Access Control Lists.
7. Insecure Services or Protocols (as determined by University Information Security personnel) must be replaced with more secure equivalents whenever such exist.
8. Remote administration must be performed over Secure Channels (e.g. encrypted Network connections using Secure Shell) or Console Access independent from a DMZ Network.
9. All server content updates must occur over Secure Channels.
10. Security-related events must be logged and audit trails saved to Logs approved by University Information Security personnel. Security-related events include, but are not limited to, the following:
 - a. User login failures
 - b. Failure to obtain privileged access
 - c. Access policy violations

New University Information Technology Network Installations and Change Management Procedures

All new installations and changes to the configuration of existing University Information Technology Network equipment and applications must comply with the following standards:

1. New installations must be done in compliance with the DMZ Equipment Deployment Process.
2. Configuration changes must comply with the University Change Management Policy.
3. Information Security personnel must be notified to perform system or application audits prior to the deployment of new Services.
4. Information Security personnel must be engaged, directly or in accordance with the University Change Management System, to approve all new deployments and configuration changes.



University Information Technology Network Equipment Outsourced to External Service Providers

The responsibility for the Security of University Information Technology Network information technology resources deployed by external service providers must be articulated in the contract with the service provider and must include Security contacts. Escalation procedures must also be documented. Contracting University departments are responsible for the third-party organization's compliance with this policy.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Router Security Policy

Revised: 01/20/2005

1. Purpose.

This document describes a required minimal Security configuration for all Routers and switches connected to the University Information Technology Network or used in a production capacity on behalf of the University.

2. Scope.

All Network infrastructure devices connected to the University Information Technology Network are subject to this policy.

3. Policy.

Every Router must meet the following configuration standards:

1. The Router must have no local user accounts configured. Routers must use the Terminal Access Controller Access Control System (TACACS+) Protocol for User Authentication.
2. The “enable” and “secret” passwords on the Router must be kept in a secure encrypted form. The Router must have the “enable” and “secret” passwords set to the current production Router passwords provided by the Information Technology Services department.
3. The following are prohibited:
 - a. IP directed broadcasts
 - b. Incoming packets at the Router sourced with invalid addresses (e.g. RFC1918 addresses)
 - c. TCP small Services
 - d. UDP small Services
 - e. All source Routing
 - f. All web Services running on Router
4. University standardized Simple Network Messaging Protocol (SNMP) community strings must be used.
5. Information Technology Services has the authority to, and will add, rules to the Access Control List as business needs arise.
6. The Router must be included in the University Security Management System with a designated point of contact.
7. Each Router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. Users must have explicit permission from Park University's Information Security to access or configure this device. All activities



performed on this device may be logged, and violations of this policy may result in disciplinary action, including expulsion from the University (if a student) or termination of employment (if an employee), and may be reported to law enforcement. Authorized Users who utilize this device have no right to privacy.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Wireless Communication Policy

Revised: 01/20/2005

1. Purpose.

This policy defines the standards that govern the use of wireless communication equipment to access the University Information Technology Network.

2. Scope.

This policy covers all wireless data communication devices, including, but not limited to, personal computers, cellular phones, and wireless access points (WAPs) connected to the University Information Technology Network. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices or Networks that do not connect to the University Information Technology Network are not subject to this policy. University Computer Lab Wireless Networks fall under the University Computer Lab Wireless Policy.

3. Policy.

Use of Wireless Equipment

Authorized Users may only access the University Information Technology Network via wireless systems that meet the criteria set forth in this policy, unless they have been granted a written waiver by Information Security personnel.

Register Access Points and Cards

All WAPs and base stations connected to the University Information Technology Network must be registered with and approved by Information Security personnel. Use of these devices by Authorized Users subjects the devices to periodic penetration tests and audits by Information Security. All Wireless Network interface cards used in resources owned by the University must be registered with the Information Technology Services department.

Approved Technology

All wireless Local Area Network (LAN) access must use vendor products and Security configurations approved by Information Security personnel before being connected to the University Information Technology Network.



VPN Encryption and Authentication

All computers with wireless LAN devices intended for connection to the University Information Technology Network for the purpose of conducting University business must utilize a Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic, and must be approved by Information Security personnel before being connected to the University Information Technology Network. To comply with this policy, Authorized Users must use wireless implementations that maintain point-to-point Hardware Encryption of at least 128 bits. All implementations must support a Hardware address that can be registered and tracked (e.g. a Media Access Control address). All implementations must support and employ strong User Authentication.

Setting the SSID

The Authorized User must configure the Service Set Identifier (SSID) so that it does not contain any identifying information about the University, such as the University name, division title, employee name, or product identifier.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Change Management Policy

Revised: 01/20/2005

1. Purpose.

This policy describes a systematic process to document and manage changes to the University Information Technology Network in order to permit effective planning by the University Information Technology Services to serve the University user-base.

2. Scope.

This policy applies to all Authorized Users that install, maintain, or operate University information technology resources, including, but not limited to: computer Hardware, Software, and Networking devices.

3. Policy.

Any change to a University Information Technology Network information technology resource is subject to this policy, and must be performed in compliance with the University's Change Management Procedure.

All changes affecting University Information Technology Network computer-based environmental facilities, including but not limited to air-conditioning, water, heat, plumbing, electricity, and alarms, must be reported to or coordinated with the Information Technology Services department.

A formal written change request must be submitted to the Information Technology Services department for all changes, both scheduled and unscheduled.

All scheduled change requests and supportive documentation must be submitted in compliance with the Change Management Procedure. The request will then be reviewed by the Change Management Committee, and a decision will be made whether to allow or delay the request.

The Change Management Committee may deny a scheduled or unscheduled change for reasons that include, but are not limited to, the following: inadequate planning, inadequate reversion plans, negative impact of change timing on a key business process, or inadequate resource availability.

Customer notification must be completed for each scheduled or unscheduled change, in compliance with the Change Management Procedure documentation.



A Change Review must be completed for each change to the University Information Technology Network, whether scheduled or unscheduled, successful or not.

A Change Management Log must be maintained for all changes. The Log must contain (but is not limited to):

- Date of submission
- Requestor of change
- Date of change
- Implementer of change
- Nature of the change
- Results of the change

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Information Security Audit Policy

Revised: 01/20/2005

1. Purpose.

Information Security personnel utilize various methods to perform electronic scans of the University's Networks and Firewalls, or on any system connected to the University Information Technology Network.

Information Security personnel are authorized to conduct audits to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible Security incidents
- Ensure compliance to University Information Technology Policies and Procedures documentation
- Monitor Authorized User or system activity where appropriate

2. Scope.

This policy covers all computer and communication devices owned or operated by the University. This policy also covers any computer and communications device that are connected to the University Information Technology Network, but which may not be owned or operated by the University. Information Security personnel will not perform Denial of Service or other disruptive activities.

3. Policy.

Authorization to Audit

Only Information Security personnel or other specifically authorized parties may audit devices that are owned by the University or are connected to the University Information Technology Network. Third-party organizations may only perform audits with the explicit written permission of the Information Technology Services department.

Access

Information Security personnel shall be granted access to the following in order to effectively perform audits:

- User level or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the University Information Technology Network



- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and Log traffic on the University Information Technology Network

Remediation

Information Security personnel will report all results to the appropriate supervisory personnel and will follow up with the processes necessary to resolve any exceptions.

4. Enforcement.

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.



Appendix A: Defined Terms

Revised: 01/20/2005

1. **Access Control**: The prevention of Unauthorized Use of a resource, including the prevention of use of a resource in an unauthorized manner.
2. **Access Control List**: A means of determining the appropriate access rights to a given object given certain aspects of the user process that is requesting them, principally the process's user identity.
3. **Algorithm**: A finite set of well-defined instructions for accomplishing some task.
4. **Anti-Virus Software**: Computer Programs that attempt to identify, thwart and eliminate computer Viruses and other Malicious Software.
5. **Asymmetric Cryptosystem**: A method of Encryption in which two different Pass-phrases are used: one for encrypting and one for decrypting the data.
6. **Authorized Use**: The use of the University Information Technology Network by any person who is authorized to do so by the University within the limits of that person's authorization, and as described in and permitted by the University Information Technology Policies and Procedures.
7. **Authorized User(s)**: Person(s) authorized by the University to use the University Information Technology Network including but not limited to faculty, staff, Students, and guests, within the limits of such person's authorization.
8. **Backup**: The process of periodically copying all of the files on a computer's disks onto a magnetic tape or other removable medium.
9. **Blowfish**: A method for encrypting information included in a large number of Encryption products, developed as a general-purpose Algorithm unencumbered by patents, non-proprietary, and open to the public.
10. **Cable Modem**: A type of Modem that allows people to access the Internet via their cable television service.
11. **Certificate**: A set of Security-relevant data issued by a trusted third-party organization, together with Security information which is used to provide the integrity and data origin authentication Services for the data (Security Certificate).



12. **Chain Email**: A term used to describe Emails that encourage you to forward them on to someone else.
13. **Challenge Handshake Authentication Protocol (CHAP)**: An authentication Protocol used to log on a user to an Internet access provider.
14. **Change Management**: The process of developing a planned approach to change in an organization.
15. **Cipher**: A private alphabet, system of characters, or other mode of writing, contrived for the safe transmission of secrets.
16. **Console Access**: Communicating with an information technology resource through a locally-connected device, such as a keyboard / pointer device / monitor combination.
17. **Cracking**: The act of breaking into an information technology resource; what a cracker does.
18. **Database**: Any set of information may be called a Database. In this context, the term refers to computerized data, represented as an information set with a regular structure.
19. **Data-Link Connection Identifier (DLCI)**: A unique number assigned to an end point in a Frame Relay Network.
20. **Decryption**: The reverse of Encryption by which the encrypted text is transformed to the readable text.
21. **De-militarized Zone (DMZ)**: Any un-trusted Network connected to, but separated from, the University's Information Technology Network by a Firewall, used for external (Internet/partner, etc.) access from within the University, or to provide information to external parties.
22. **Denial of Service (DoS)**: An attack on a computer system or Network that causes a loss of Service to users, typically the loss of Network connectivity and Services by overloading the computational resources of the victim system.
23. **Data Encryption Standard (DES)**: A method for encrypting information selected as an official Federal Information Processing Standard for the United States, and which has enjoyed widespread use internationally, but is now considered to be insecure for many applications.



24. **Digital Subscriber Line (DSL)**: A family of digital telecommunications Protocols designed to allow high speed data communication over the existing copper telephone lines between end-users and telephone companies.
25. **Domain Name System (DNS)**: A system that stores information about computer and Network names in a kind of distributed Database on Networks, such as the Internet.
26. **Dual Homing**: Having concurrent connectivity to more than one Network from a computer or Network device.
27. **Email**: The electronic transmission of information through a mail Protocol such as SMTP.
28. **Email Bomb**: Causing a user's Email account to reach maximum storage capacity by through the excessive sending of Email messages for the sole purpose of being malicious.
29. **Encryption**: The process of making data unreadable to unauthorized entities by applying a cryptographic Algorithm (an Encryption Algorithm).
30. **Extranet**: An interconnection between two or more organizations in order to create a private Network to share information.
31. **File Transfer Protocol (FTP)**: A Software standard for transferring computer files between machines with widely different Operating Systems
32. **Firewall**: A piece of Hardware or Software which functions in a Networked environment to prevent some communications forbidden by the Network policy. It has the basic task of preventing intrusion from a connected Network device into other Networked devices.
33. **Forwarded Email**: Email explicitly redirected from one account to another.
34. **Frame Relay**: An efficient data transmission technique used to send digital information quickly and cheaply to one or many destinations from one point.
35. **Guest User**: Any visitors to the University, not including faculty, staff, or Students who are properly authorized to use the University Information Technology Network.
36. **Hardware**: The physical, touchable, material parts of a computer or other system. The term is used to distinguish these fixed parts of a system from the



more changeable Software or data components which it executes, stores, or carries.

37. **HyperText Transfer Protocol (HTTP)**: The primary method used to communicate information on the World Wide Web.
38. **Host**: Any computing device attached to a computer Network.
39. **Information Security**: Information Security is the part of Information Technology Services that is responsible for coordinating and overseeing campus wide compliance with university policies and procedures regarding the confidentiality, integrity, and Security of its information assets.
40. **Information Security Awareness Initiative**: An educational initiative developed by Information Security that will train Authorized Users about the University Information Technology Policies and Procedures and how to stay in compliance with them. This will include, but is not limited to, teaching classes, sending alerts and reminders, and writing guidelines.
41. **Information Security Guidelines**: (in development) Attached to these policies are guidelines that help the user comply with the policies.
42. **Instant Messaging**: An on-line communication Service in which conversations happen in real-time, and the "on-line status" between users is conveyed such as if a contact is actively using the computer.
43. **Integrated Services Digital Network (ISDN)**: A set of communications standards allowing a single wire or optical fibre to carry voice, digital Network Services and video.
44. **Intellectual Property**: A form of legal entitlement which allows its holder to control the use of certain intangible ideas and expressions.
45. **International Data Encryption Algorithm (IDEA)**: A method for encrypting information which is patented but is free for non-commercial use, and is considered to be the best and most secure method available.
46. **Internet**: The publicly available worldwide system of interconnected computer Networks.
47. **Internet Message Access Protocol (IMAP)**: A Protocol used for accessing Email on a remote server from a local client.



48. **Internet Protocol (IP) Address**: A unique number used by machines (usually computers) to refer to each other when sending information through the Internet.
49. **IP Security (IPSec)**: A standard for securing Internet communications by encrypting and authenticating all data.
50. **IP Security (IPSec) Concentrator**: A device where IPSec connections merge into a Network and are no longer encrypted.
51. **Intranet**: An Intranet is a Network used internally in an organization.
52. **Layer 2 Tunneling Protocol (L2TP)**: A Protocol used to support virtual private Networks.
53. **Log**: A chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event (also known as an audit trail).
54. **MAC Address**: A code on most forms of Networking equipment that allows for that device to be uniquely identified.
55. **Malicious Software (malware)**: Any Software developed for the purpose of doing harm to a computer system.
56. **Mass Emailing**: An Email that is sent to a group of individuals.
57. **Modem**: An electronic device for converting between data from a computer and an audio signal suitable for transmission over a telephone line connected to another Modem.
58. **Network**: A system for communication among two or more computers.
59. **Network Auto-Discovery**: A process for automatically learning what information technology resources are available on a Network.
60. **Network Closet**: A physically-secured room where production network devices reside.
61. **Network Drive**: A computer storage medium accessible from a Network connection.
62. **Network Sniffing**: The act of watching Internet Protocol packets as they traverse a local Network.



63. **Operating System (OS)**: The system Software responsible for the direct control and management of Hardware and basic system operations, as well as running application Software.
64. **Packet Spoofing**: To capture, alter, and retransmit a communication stream in a way that misleads the recipient.
65. **Pass-phrase**: A collection of 'words' used for access control, typically used to gain access to a computer system.
66. **Patch**: An update to an existing piece of Software that corrects errors or adds new features (also known as a hot-fix).
67. **Phishing**: The act of sending Email for the purpose of surrendering private information that will be used for identity theft.
68. **Ping**: Slang term for a small Network message sent by a computer to check for the presence and alertness of another computer.
69. **Post Office Protocol version 3 (POP3)**: A Protocol used to retrieve Email from a remote server to a local client.
70. **Pretty Good Privacy (PGP)**: A computer Program which provides cryptographic privacy and authentication.
71. **Principle of Least Access**: A user must have access to the resources necessary to accomplish a given task, but not to resources unnecessary for completing the task, thus minimizing potential Security risks.
72. **Program**: See Software.
73. **Proprietary Encryption**: An Encryption Algorithm that has not been made public and/or has not withstood public scrutiny.
74. **Proprietary Information**: Information on the University Network that is owned by the University, a form of Intellectual Property.
75. **Protocol**: A convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints.
76. **Public Switched Telephone Network (PSTN)**: The concatenation of the world's public telephone Networks.



77. **Public-key Cryptography**: A form of modern cryptography which allows users to communicate securely without previously agreeing on a shared secret key.
78. **Remote Access**: Communicating with an information technology resource from different location.
79. **Restoration**: Action taken to repair and return to Service one or more information technology resources that have a degraded quality of Service or have a Service outage.
80. **Risk Analysis**: A process to ensure that the Security controls for a system are fully commensurate with its risks.
81. **Risk Assessment**: The process of assessing Security-related risks from internal and external Threats to an entity, its assets, or personnel.
82. **Rivest Cipher 5 (RC5)**: A method of Encryption notable for its simplicity.
83. **Router**: A device that forwards data across Networks toward their destination Network.
84. **Routing**: Routing provides the means of discovering paths along which information can be sent.
85. **RSA**: A public-key method for both Encryption and authentication, the entire Security of which depends on the difficulty of factoring.
86. **Scanning**: Checking for Services presented on Networks, usually as part of a Cracking attempt or computer Security scan.
87. **Secure Channel**: A communication that uses strong Encryption.
88. **Secure Shell (SSH)**: Both a computer Program and an associated Network Protocol designed for logging into and executing commands on a remote computer. It provides secure encrypted communications between two un-trusted Hosts over an insecure Network
89. **Secure Sockets Layer (SSL)**: A cryptographic Protocol to provide secure communications on the Internet.
90. **Security**: The term “Security” is used in the sense of minimizing the Vulnerabilities of assets and resources.



91. **Security Audit**: This function provides monitoring and collection of information about Security-related actions, and subsequent analysis of the information to review Security Policies, controls and procedures.
92. **Security Guideline**: A guideline is a collection of system specific or procedural specific “suggestions” for best practice. They are not requirements to be met, but are strongly recommended.
93. **Security Policy**: A policy is a document that outlines specific requirements or rules that must be met.
94. **Security Standard**: A standard is a collection of system-specific or procedural-specific requirements that must be met by everyone.
95. **Sensitive Information**: Information is considered sensitive if it can be damaging to University or its reputation.
96. **Service**: Work performed (or offered) by a server.
97. **Service Set Identifier (SSID)**: A code attached to all data on a Wireless Network to identify the data as part of that Network.
98. **Simple Mail Transfer Protocol (SMTP)**: The de facto standard for Email transmission across the Internet.
99. **Simple Network Management Protocol (SNMP)**: Supports monitoring of Network-attached devices for any conditions that warrant administrative attention
100. **Software**: A loadable set of instructions which determines how the computer will operate autonomously or in reaction to user input, when running.
101. **SPAM**: Unauthorized or unsolicited electronic mailings.
102. **Split-tunneling**: See Dual Homing.
103. **Student(s)**: Person(s) enrolled in at least one credit class of the University.
104. **Surge Protector**: An appliance designed to protect electrical devices from power surges.
105. **Symmetric Cryptosystem**: A method of Encryption in which the same key is used for both Encryption and Decryption of the data.



106. **Telecommunication Circuit**: The complete path between two resources over which one-way or two-way communications may be provided.
107. **Terminal Access Controller Access Control System (TACACS+)**: A remote authentication Protocol that is used to communicate with an authentication server.
108. **Threat**: A potential violation of Security.
109. **Token**: An abstract concept passed between cooperating agents to ensure synchronized access to a shared resource.
110. **Traffic Flooding**: To send an excessive amount of traffic to an information technology resource, causing a Denial of Service attack.
111. **Trojan Horse**: Malicious Software that is disguised as legitimate Software.
112. **Trust Relationship**: A relationship between two Networks that enables a user in one Network to access resources in the other.
113. **Unauthorized Disclosure**: The intentional or unintentional revealing of restricted information to people, both inside and outside the University, who are not authorized to know that information.
114. **Unauthorized Use**: Use of the University Network by Unauthorized Users in violation of the law or in violation of the University Information Security Policies and Procedures.
115. **Unauthorized Users**: Use of the University Network who are not Authorized Users, or use of the University Information Technology Network in violation of the law or in violation of the University Information Technology Policies and Procedures.
116. **Uninterrupted Power Supplies (UPS)**: A device or system that maintains a continuous supply of electric power.
117. **University**: The Board of Trustees of Park University, a Missouri nonprofit corporation that does business as “Park University.”
118. **University Address Management System**: System that stores IP addresses routed within the University Technology Network.



119. **University Change Management System:** System that manages the approval process for any modifications to the University Information Technology Network, and that stores documentation for each modification.
120. **University Password Management System:** System that stores and manages passwords on the University Information Technology Network for all system-level and user-level accounts.
121. **University Security Management System:** System that stores information about the University Information Technology Network, including but not limited to contact information, Hardware, and Software (for every part of it).
122. **University Information Technology Policies and Procedures:** Policies and Procedures of the University that govern the use of the University Information Technology Network, as from time to time amended, all as approved by the board of trustees of the University or the boards delegates.
123. **University Information Technology Network:** Internet/Intranet/Extranet-related systems, including but not limited to computer/Networking equipment, Software, Operating Systems, storage media, Network accounts providing electronic mail, Instant Messaging, student information system, WWW browsing, and FTP, are the property of the University.
124. **University Computer Labs:** A collection of publicly accessible University computers that are connected to the University Information Technology Network, from which Authorized Users can access the University Information Technology Network.
125. **University Data:** Data that belongs to the University that is entered into the University Information Technology Network by University and other Authorized Users.
126. **University Employees:** Persons employed by the University including faculty members, staff, and student workers.
127. **University Operational Group:** Group responsible for system administration on all internal servers deployed at the University.
128. **Un-Trusted Network:** Any Network separated by a Firewall from the corporate Network to avoid impairment of production resources from irregular Network traffic, unauthorized access, or anything else identified as a potential Threat to those resources.



129. **User Authentication**: A method by which the user of a system can be verified as a legitimate user independent of the system being used.
130. **Virtual Private Network (VPN)**: A method for accessing a remote Network via an encrypted "tunnel" through the Internet.
131. **Virus**: A self-replicating Program that spreads by inserting copies of itself into other Programs or documents.
132. **Vulnerability**: Any weakness that could be exploited to violate a system or the information it contains.
133. **Wireless Networks**: Telephone or computer Networks that use radio as their carrier or physical layer.
134. **World Wide Web (WWW)**: A distributed system that operates over the Internet, primarily used for displaying documents which contain automated cross-references to other documents.
135. **Worm**: A self-replicating Program that is self-contained and does not need to be part of another Program to propagate itself.