

PRINCE SULTAN UNIVERSITY



IT Policies & Guidelines

Prepared by

ITCS Department

Introduction

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

The purpose of the PSU Information Policies and Procedures is:

- To establish organization-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 organization and to allow the organization to satisfy its legal and ethical responsibilities with regard to its information technology resources.
- To enable the PSU to respond to complaints and queries about real or perceived non-compliance with the organization Information Technology Policies and Procedures.

Responsibility

Authorized Users of PSU information technology resources are personally responsible for complying with all organization policies, procedures and standards relating to Information Security, regardless of locations 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 & Computing 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 authorized members will draft the proposed amendment. The proposed amendment will be forwarded to the Information Technology Policies and Procedures Reviewing authority. Upon approval by that authority, 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

Dr. Khalid Al. Mustafa

Supervisor ITCS

Md. Vaseem Jaweed

Director ITCS

UNIVERSITY OF AL-QADISIYAH
جامعة القادسيه

PSU Group IT Policies

Contents

Introduction.....	2
Approvals.....	3
Unauthorized Use Policy	5
Guest User Policy	6
Organization Confidentiality Policy.....	7
Acceptable Use Policy	7
Physical Security Policy.....	12
Workstation Configuration Security Policy	14
Data Center Security Policy	16
Server Configuration Security Policy	20
Router Security Policy.....	23
Change Management Policy.....	24
Password Policy.....	25
Internet Connection Policy.....	27
Approved Application Policy	29
Asset Control Policy.....	31
Remote Access Policy.....	35
IT Equipment Purchase and Failure Prevention Policy.....	37
Mobile Computer Policy.....	38
Computer Training Policy	43
Anti-Virus Policy.....	45
Wireless Use Policy	50
Data Backup Policy.....	52
Firewall Policy.....	54
E-Mail Usage and Management Policy	59
Computer and Hardware Replacement Policy (CRP).....	64

Unauthorized Use Policy

1. Purpose.

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

2. Scope.

This policy covers all Unauthorized Use of the Organization 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 organization, all of whom are referred to in this policy as "Unauthorized Users."

3. Policy.

All Unauthorized Users are prohibited from using PSU Information Technology Network for any purpose whatsoever. Authorized Users are prohibited from using the organization 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 PSU seeks damages and/or other legal and/or equitable remedies. Unauthorized Users who are employees of the PSU may also be subject to disciplinary action, up to and including termination of employment. Unauthorized Users who are employees at the organization may also be subject to disciplinary action, up to and including expulsion from the organization.



Guest User Policy

1. Purpose.

For students, companies, vendors, auditing, and other purposes many external users need organization network access. For supporting them, the PSU IT grants to organization guests and visitors the right to use its information technology resources in compliance with the PSU 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 university employees.

3. Policy.

A Guest User is an Authorized User when utilizing the organization's information technology resources in compliance with the PSU 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 organization and selected Software. The Guests may also be permitted to selected areas of the PSU 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.



Organization Confidentiality Policy

1. Purpose.

Confidential information may be developed or obtained by PSU employees as a result of that person's relationship with the organization.

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:

- Educational and employee information and other private information.
- Operations manuals, Organization practices, academic plans, techniques and materials, development plans, and financial information
- Employee lists grades, personnel and payroll records, records regarding vendors and suppliers, records and files of the business, and other information concerning the business affairs or operating practices of the organization.

3. Policy.

Confidential information must never be released, removed from the Organization premises, copied, transmitted, or in any other way used by the Authorized User for any purpose outside the scope of their organization employment, nor revealed to non-organization employees, without the express written consent of organization management personnel. Information stored on the organization Information Technology Network is confidential and may not be distributed outside the organization except in the course of the organization's business or as otherwise authorized by management personnel. Authorized Users may not remove or borrow from the organization 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

1. Overview.

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

The Organization 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, ERP system, WWW browsing, and FTP, which are the property of the Organization. They are to be used for Organization business purposes and to serve the interests of the Organization, and as well as all Authorized Users. Effective computer Security is a team effort requiring the participation and support of every Organization employee and Authorized User who deals with information and/or information systems. It is the responsibility of every computer user to know the Organization Information Technology Policies and Procedures, and to comply with the Organization Information Technology Policies and Procedures.

2. Purpose.

This policy describes the Authorized Use of the Organization Information Technology Network and protects the Organization and Authorized Users. Unauthorized use exposes the organization 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 Part Organization-owned, third party-owned, or personally-owned computing device that is connected to the Organization Information Technology Network.

4. Policy.

a. General Use and Ownership.

1. Data created by Authorized Users that is on the Organization Information Technology Network is the property of the Organization. There is no guarantee that information stored on the Organization Information Technology Network device will be confidential.

2. Authorized Use includes reasonable personal use of the Organization Information Technology Network by Authorized Users. Organization departments are responsible for creating guidelines concerning personal use of the Organization Information Technology Network. In the absence of such guidelines, users should consult the ITCS Department.

3. Any information that an Authorized User considers to be sensitive or vulnerable should be encrypted. For guidelines on encrypting Email and documents, consult IT Helpdesk.

4. Authorized IT employees may monitor the Organization Information Technology Network traffic at any time, in accordance with the Information Security Procedure.

5. The Organization reserves the right to audit Networks and systems on a periodic basis to ensure compliance with the Organization 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 Organization Information Technology Network as “confidential” or “not confidential,” as defined by Organization Confidentiality Guidelines. Confidential information includes, but is not limited to: Organization private data, specifications, Employee 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 or at least locking out of all systems and accounts when they are not being used; they must not be left 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 Organization Information Technology Network in accordance with the “Laptop Security Guidelines.”

7. Postings by Authorized Users from a Organization Email address must contain a disclaimer stating that the opinions expressed are strictly those of the author and not necessarily those of the Organization, unless posting has been done in the course of Organization business.

8. All computers used by Authorized Users that are connected to the Organization Information Technology Network, whether owned by the individual or the Organization, 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 Organization Information Technology Network.

The following activities are prohibited, although Organization 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 Organization Information Technology Network.

d. 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 organization 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 Organization.
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 Organization 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. Organization management must be consulted prior to export of any material that is in question.
4. Introduction of Malicious Software into the Organization 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 Organization Information Technology Network from home or other non-Organization locations.
6. The use of a component of the Organization 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 Organization policy. Pornographic material is a violation of sexual harassment policies.
7. Making fraudulent offers of products, items, or services originating from any Organization account or otherwise made from a computer connected to the Organization Information Technology Network.

8. Causing Security breaches or disruptions of communication over the Organization 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, Organization employees or Students to non-Organization 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 Organization's name in any unsolicited Email on behalf of, or to advertise, any service or product without the explicit written permission of the Organization.

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.

Physical Security Policy

1. Overview.

Physical Security means providing environmental safeguards for, and controlling physical access to, equipment and data on the Organization 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 Organization Information Technology Network and to protect equipment on the Organization Information Technology Network from environmental factors.

3. Scope.

This policy applies to the entire Organization Information Technology Network, including but not limited to meeting rooms, presentation rooms, Network Closets, and the Information Technology Services Network Operations Center.

4. Policy.

Environmental Safeguards

1. Adequate air conditioning must be operational in Organization Information Technology Network facilities that house information technology resources, to prevent long-term heat damage and equipment failure.
2. All Organization Information Technology Network facilities must have adequate fire extinguishing devices present in the office area. These devices must be inspected by Organization Public Safety personnel.

3. All Organization 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 Organization 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 Organization 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 Organization Information Technology Network facilities must be documented and managed by Information Technology Services.
3. All facilities that house Organization Information Technology Network information technology resources must be physically protected in proportion to the importance of their function.
4. Access to Organization Information Technology Network restricted facilities will be granted only to Organization staff and affiliates whose job responsibilities require access to that facility.
5. The process for granting fingerprint access to Organization Information Technology Network facilities must include approval from the Organization 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 Organization Information Technology Services department, and logged appropriately before they are re-allocated to another Authorized User.
8. Lost or stolen Organization Information Technology Network secured access devices must be reported to Information Security personnel immediately.

9. The Organization Employees responsible for Organization Information Technology Network facilities must remove the secured access device rights of individuals that no longer require access.

10. Organization Visitors and other invitees must be escorted and monitored while in restricted Organization Information Technology Network facilities.

11. Organization Employees responsible for Organization 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 an Organization Employee, in order to reduce the occurrence of unauthorized entry and access.

13. Any piece of Organization 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 Organization 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

1. Purpose.

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

2. Scope.

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

3. Policy.

Ownership and Responsibilities

All Organization Information Technology Network workstations at the Organization must be the responsibility of an operational group that is responsible for computers management. Approved workstation configuration standards must be established and maintained by each that division, 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 Organization IT inventory 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 Organization IT inventory 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 Organization.
2. Audits are managed by the Organization'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.

Data Center Security Policy

Introduction

The security of the equipment and data in PSU Data Centers is of critical importance of the daily functioning of PSU.

This document is to communicate the policies and procedures by which access will be obtained and how individuals will conduct themselves within the Data Center.

1. Background to Policies

a. Personal Naming:

- Data Center Manager: Communication and infrastructure leader (Operation Manager)

- Data Center Stuff: IT team that have the authority to access the Data center for regular maintenance and Back-up. (Application team leader, IT Security Coordinator, IT Technical Manager)
- Authorized Stuff: Servers administrators that require an authorization form to access the housed servers in the Data Center.
- Individuals: An Unauthorized person to access the Data Center ex. Suppliers, cleaning agency ...etc
- Auditors: IT manager, PSU Organization Board member and External auditor.

b. Reactive Work:

Reactive work will be defined as all work that is done as a reaction to a system event or user need. Examples would be handling system problems, hardware failures, requests for changes in authorizations, accounts, and application settings. Work that has a business need to happen in a rapid fashion, either to alleviate a problem with an existing process or system, or a change in configuration.

c. Proactive Work:

Proactive work is all work that can be scheduled for some future time. Work that needs to be done to maintain processes and systems in good functional and secure condition

2. Access Authorization

PSU Organization data centers are consolidated server's rooms intended to provide 24*7 high availability, redundant and secure environment for systems which need a high level of security.

There are two level of authorization based on the level of access required

1. Level 1 Authorization

Authorized stuff, individuals and auditors that will have assisted access to the data center 24 hours a day. They will not be assigned access cards.

In order to access the data center one of the data center stuff should be present. The Process to acquire level 1 authorization is as follow:

- An authorization form must be completed by each employee requesting level 1 access to the data center
- The purpose of each visit must be documented. The employee must sign a log in and out form when entering and exiting the data center

2. Level 2 Authorization

Data center staff and data center manager will have unassisted access to the data center 24 hours a day. They will not need to make arrangements to enter as they will have access cards assigned to them that will allow them to enter when needed

The Process to acquire level 2 authorizations is as follow:

- An employee requiring level 2 access to the data center must complete authorization form
- The purpose of each visit must be documented. The employee must sign a log in and out form when entering and exiting the data center

3. Visitor Procedures

Anyone who is not a Data Center employee, an authorized staff member, or authorized vendor is considered a visitor. All visitors to the Data Center must adhere to the following procedures:

- All visitors must enter through the IT room entrance of the Data Center.
- Visitors must be accompanied by either a Data Center employee or other authorized staff member at all times while in the Data Center. Exceptions to this policy must have the approval of the Data Center manager.
- Visitors must log in/out when entering/exiting the Data Center. The purpose of the visit must be documented.
- Visitors must wear a visitor's badge at all times.
- Visits should be scheduled through the Data Center manager at least 24 business hours in advance. Unscheduled visits to install equipment or perform other tasks may be turned away.

4. Access Control Log

The Data Center Access Control Log must be properly maintained at all times. The Log is maintained by Operations staff. All individuals with Controlling Access to the Data Center are responsible for maintaining this log. The following procedures must be followed:

- Each time an individual with Escorted Access to the Data Center is admitted to the area, he must properly log in on the Access Control Log at the time of entrance. The person admitting the visitor must countersign and fill out the appropriate section of the form.
- Each time an individual with Escorted Access leaves the area, he must properly log out on the Access Control Log at the time he leaves (even if

only for a short time). The person with Controlling Access to the area who allows the visitor to leave must fill out the “Log Out” section of the Access Control Log.

3. Scheduled Maintenance Procedure

The Data Center staff will set scheduled maintenance windows, and adhere to them for system changes which require system downtime. Care will be taken to limit the systems downtimes as much as possible. Care will also be taken to not make changes which require a downtime to systems outside of the scheduled maintenance time period.

4. Hardware Requirement

All new machines going into the Data Center must be rack mountable, unless prior arrangements have been made to allow particular non-rack-mountable hardware into the Data Center. Existing machines which have a business need to be in the Data Center which are not rack mountable will be allowed, but there will be an expectation that these machines will be replaced within a reasonably short time period with more appropriate hardware or the functions that those non-rack-mountable machines to be relocated to other servers which are more appropriate for the Data Center.

All machines and hardware that will move into the Data Center will need to be coordinated and scheduled with the Data Center staff. As we grow the number of machines in the Data Center, we will need to incrementally expand the infrastructure that supports the entire Data Center. Sometimes this may mean a small delay in the deployment of hardware into the Data Center until we have the appropriate infrastructure (including console, network, power, and rack space) for the hardware to be deployed

5. Equipment Installation and removal

The Data Center is intended as a limited physical access location for servers. Systems administrators of machines which are housed in the Data Center should plan their servers as if they will only get physical access to them when it is necessary to perform hardware modifications or replacements. With this in mind, it is highly recommended that all servers be configured with secure access administrative tools to allow for remote maintenance. All machines in the Data Center must be rack mountable, unless prior arrangements have been made to allow particular non-rack-mountable hardware into the Data Center. Certain machines which have a business need to be in the Data Center and currently are not rack mountable should be replaced within a reasonably short time period of time with more appropriate hardware, or the machines’ functions need to be relocated to other servers which are more appropriate for the Data Center.

Any employee intending to install equipment in the Data Center must submit an

installation form.

All new systems and hardware to the Data Center will need to be coordinated and scheduled with Data Center staff. As the number of machines in the Data Center grows, the infrastructure that supports the entire Data Center must incrementally expand. Sometimes this may mean a small delay in the deployment of hardware into the Data Center until we have the appropriate infrastructure (including console, network, power, and rack space) for the hardware to be deployed.

Any employee intending to remove equipment from the Data Center must submit a removal form.

6. Rules while in the Data Center

- No food or drink is allowed within the Data Center
- All packing material must be removed from computer equipment/components in the specified staging areas before being moved into the Data Center. This includes cardboard, paper wrap, peanuts, plastic, wood and other such material
- All packing materials should be removed from the admin area after the installation is completed
- No cleaning supply is allowed within the Data Center without prior approval. This includes water.
- Only filter vacuums may be used inside the Data Center
- No cutting of any material (pipes, floor tiles etc...) shall be performed inside the Data Center unless special arrangements are made
- Boxes, tapes, CD's and other material shall not be stored inside the Data Center
- Only Data Center staff shall access the sub-floor or remove floor tile
- ID must be worn above the waist and visible at all times
- Communicate all problems to the Data Center staff
- In the event of an emergency notify Data Center staff immediately

Server Configuration Security Policy

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 Organization. Effective implementation of this policy will minimize Unauthorized Use of the Organization Information Technology Network or other access to the Organization's Proprietary Information and technology.

2. Scope.

This policy applies to server equipment owned or operated by the Organization, and to servers registered under any Organization-owned internal Network domain. This policy applies specifically to equipment connected to the internal Organization Information Technology Network.

3. Policy.

Ownership and Responsibilities

All internal servers deployed at the Organization 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 Organization 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 Organization 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 Organization.
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.

Router Security Policy

1. Purpose.

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

2. Scope.

All Network infrastructure devices connected to the Organization 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. Organization 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 Organization 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 Organization’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

Organization or termination of employment, 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.

Change Management Policy

1. Purpose.

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

2. Scope.

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

3. Policy.

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

2. 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

When employees are required to change passwords often, meet minimum complexity requirements, and not repeat a password for a minimum amount of time, they may begin to break the rules and start writing passwords down simply because they cannot remember passwords that change so often. The reason for changing passwords is due to the fact that if an attacker gets a hashed or encrypted copy of a password, they can eventually break the password using a brute force attack. This takes a certain amount of computing power and as computers are more powerful, takes less time every year.

However the password policy is setup, it may be worth taking other precautions to protect accounts and passwords. One precaution is not to transmit them on the internet even in encrypted form. Another precaution is to be very careful about network security, to detect any unauthorized sniffing of the internal network, and stringent virus prevention including blocking dangerous email attachments.

Another issue that deals with the use of passwords versus pass phrases. Some contend that passwords are no longer secure and that pass phrases should be used rather than passwords.

Example Password Policy

1.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

2.0 Purpose

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

3.0 Scope

This policy applies to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account.

4.0 Password Protection

1. Never write passwords down.
2. Never send a password through email.
3. Never include a password in a non-encrypted stored document.
4. Never tell anyone your password.
5. Never reveal your password over the telephone.
6. Never hint at the format of your password.
7. Never reveal or hint at your password on a form on the internet.
8. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
9. Never use your university or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
10. Report any suspicion of your password being broken to your IT security division.
11. If anyone asks for your password, refer them to your IT security division.
12. Don't use common acronyms as part of your password.
13. Don't use common words or reverse spelling of words in part of your password.
14. Don't use names of people or places as part of your password.
15. Don't use part of your login name in your password.
16. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
17. Be careful about letting someone see you type your password.

5.0 Password Requirements (subject to change)

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements will be set by the IT security department:

1. Minimum Length - 8 characters recommended
2. Maximum Length - 14 characters
3. Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
 1. Lowercase
 2. Uppercase
 3. Numbers
 4. Special characters such as !@#%&*(){}[]
4. Passwords are case sensitive and the user name or login ID is not case sensitive.

5. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.
6. Maximum password age - 60 days
7. Minimum password age - 2 days
8. Store passwords using reversible encryption - This should not be done without special authorization by the IT department since it would reduce the security of the user's password.
9. Account lockout threshold - 4 failed login attempts
10. Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value is 20 minutes. This means if there are three bad attempts in 20 minutes, the account would be locked.
11. Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal of additional help desk calls. Therefore depending on the situation, the account lockout should be between 30 minutes and 2 hours.
12. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".
13. Rules that apply to passwords apply to passphrases which are used for public/private key authentication

6.0 Choosing Passwords

Use password choosing tips can also be obtained from internet and be sure your passwords meet the minimum guidelines.

7.0 Enforcement

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action recommended by GITD.

8.0 Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

Internet Connection Policy

1.0 Overview

This internet connection policy has components of a user compliance policy and an internal IT policy. The user compliance section specifies how users are allowed to connect to the internet and provides for IT department approval of all connections to the internet or other private network. It requires all connections such as connections by modems or wireless media to a

private network or the internet be approved by the IT department and what is typically required for approval such as the operation of a firewall to protect the connection.

This internet connection policy requires users to use the internet for business only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity. Defines whether a proxy server will be used for user internet access. It defines how the network will be protected to prevent users from going to malicious web sites.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion by malware that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

3.0 Physical Internet Connection

All physical internet connections or connections to other private networks shall be authorized and approved by the IT department. Most users will access the internet through the connection provided for their office by the IT department. Any additional connections must be approved by the IT department. These additional connections include but are not limited to:

1. Modem connection from a computer or communication device which may allow a connection to the network.
2. Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT department.
3. Wireless access points or devices with wireless capability are not allowed unless approved by the IT department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT department when connected to the network.

Any additional internet connections not provided by the IT department must be reviewed and approved by the IT department. Typically any additional connections from the organizational network to the internet or other private network will require.

1. An IT department approved firewall operating at all times and properly configured.
2. Some communications through the connection may require encryption subject to a review of data to be transmitted by the IT department.

4.0 Use of the Internet

1. All employee use of the internet shall be for business purposes only.

2. Employee use of the internet may be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.
3. Employees are urged to use caution when visiting unknown internet sites and through user training set and keep their browser configured to IT approved standards in order to protect against infections of malware. Employees will be trained in the latest IT approved standards to protect against malware when appropriate.

5.0 Internet Control and Logging System

A system will be required to operate on the network with the following capabilities:

1. The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.
2. The ability to log user internet activity including:
 1. Time of the internet activity.
 2. Duration of the activity.
 3. The website visited.
 4. Data and type of data downloaded
 5. Whether the system will cache web pages to increase the internet connection speed. This requires a proxy server.
3. The system (will | will not) require a login ID or it will use the current network login to identify users.

The system used to prevent users from visiting inappropriate, pornographic, or dangerous web sites shall be SRVPROXY01. This same system will not require an additional login ID and will use Active Directory to identify internet users. The system shall be able to log the time of internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.

6.0 Enforcement

Since improper use of mobile computers can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees that do not adhere to this policy may be subject to disciplinary action approved by GITD and HRD.

Approved Application Policy

1.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the approved application policy in order to protect the security of the network, protect data integrity, and protect computer systems.

2.0 Purpose

This policy is designed to protect the organizational resources on the network by requiring all network users to only run or install application programs deemed safe by the IT department.

3.0 Approved Applications

All employees may operate programs on the IT approved application list. If an employee wants to use an application not on the list, they should submit the application program to the IT department for approval prior to using the program on a system connected to the organizational network.

If the employee causes a security problem on the network by installing and running an unapproved program they risk disciplinary action.

4.0 Exceptions

Special exception may be made to this policy for specific employees depending on the required job function and the skills of the employee. Some reasons for exception include:

1. The employee may be the person who needs to test new applications on a test network, then on the main network.
2. The employee may be a developer that must run applications developed by themselves in order to test their own work.
3. Network administrators may be allowed the ability to operate and test new software.

5.0 Enforcement

Since running safe programs is critical to the security of the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

6.0 Approved Applications

IT department approved applications are listed below.

- Windows Operating system
- Microsoft Office Suite
- Microsoft Axapta
- Mozilla Firefox
- Microsoft Internet Explorer
- Adobe Acrobat
- Microsoft Visio
- Symantec/ Trend micro Antivirus
- Roxio Easy CD Creator
- WinZip
- WinRAR
- Nero CD Creator
- Citrix Web client
- Power Archiver
- AutoCAD
- PDF writer

Asset Control Policy

1.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

2.0 Purpose

This policy is designed to protect the organizational resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

3.0 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

3.1 IT Asset Types

This section categorized the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Printers, Copiers, FAX machines, multifunction machines
4. Handheld devices
5. Scanners
6. Servers
7. Firewalls
8. Routers
9. Switches

10. Memory devices

3.2 Assets Tracked

Assets which cost less than SR100 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data.
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

3.3 Small Memory Devices

Small memory storage assets will not be tracked by location but by trustee. These assets include:

1. Floppy disks
2. CD ROM disks
3. Memory sticks

If these types of devices are permitted for some employees, the trustee of the device must sign for receipt of these devices in their possession. All employees must also agree to handle memory sticks, floppy disks, and CD ROM disks in a responsible manner and follow these guidelines:

1. Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
2. Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be on the IT department list of approved programs.

The Memory Device Trustee agreement allows employees to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all employees that will work with any organizational data when the employee begins working for the organization. It will also be submitted when employee receives one or more memory sticks, temporary storage drives, or data backup drives.

4.0 Asset Tracking Requirements

1. All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.

3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

5.0 Transfer Procedure:

1. Asset Transfer Checklist - When an asset type listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be filled out by the trustee of the item and approved by an authorized representative of the organization. The trustee is the person whose care the item is in. If the item is a workstation, then the trustee is the most common user of the workstation. For other equipment, the trustee is the primary person responsible for maintenance or supervision of the equipment.

The trustee must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be filled in:

1. Asset Type
2. ID number
3. Asset Name
4. Current Location
5. Designated Trustee
6. New Location
7. New Trustee
8. Locations of Sensitive Data

Once the trustee fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

2. Data entry - After the Asset Transfer Checklist is completed, it will be given to the asset tracking database manager. The asset tracking database manager will ensure that the information from the forms is entered into the asset tracking database within one week.
3. Checking the database - Managers who manage projects that affected equipment location should check periodically to see if the assets that recently were moved were added to the database. The database should provide a recent move list which can be easily checked. Managers should check the database weekly to be sure assets moved within the last 2 or 3 weeks are included in the database.

6.0 Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.
4. Asset disposal

In all these cases the asset transfer checklist must be completed.

7.0 Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed prior to disposal. Any data storage devices. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:
 1. Floppy disk
 2. Memory stick
 3. DVD or CD ROM disk
 4. Storage tape
 5. Hard drive.
 6. RAM memory
 7. ROM memory or ROM memory devices.

8.0 Media Use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

1. Floppy disk
2. Memory stick
3. DVD or CD ROM disk
4. Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

1. Unclassified - Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
2. Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
3. Confidential - The data may only be removed from secure areas with permission of a Vice -president or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
4. Secret - - The data may only be removed from secure areas with the permission of the President or higher level of management. There must be some security precautions documented for both the transport method and at the destination.

5. Top secret - The data may never be removed from secure areas.

9.0 Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Remote Access Policy

1.0 Overview

This remote access policy defines standards for connecting to the organizational network and security standards for computers that are allowed to connect to the organizational network.

This remote access policy specifies how remote users can connect to the main organizational network and the requirements for each of their systems before they are allowed to connect. This will specify:

1. The anti-virus program remote users must use and how often it must be updated.
2. What personal firewalls they are required to run.
3. Other protection against spyware or other malware.

The remote access policy defines the methods users can use to connect remotely such as dial up or VPN. It will specify how the dial up will work such as whether the system will call the remote user back, and the authentication method. If using VPN, the VPN protocols used will be defined. Methods to deal with attacks should be considered in the design of the VPN system.

2.0 Purpose

This remote access policy is designed to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data.

3.0 Approval

Any remote access using either dial-in, VPN, or any other remote access to the organizational network must be reviewed and approved by the appropriate supervisor. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

4.0 Remote Computer Requirements

1. The anti-virus product called Forefront or Symantec is required to be operating on the computer at all times in real time protection mode.
 1. The anti-virus product shall be operated in real time on the computer. The product shall be configured for real time protection.
 2. The anti-virus library definitions shall be updated at least once per day.
 3. Anti-virus scans shall be done a minimum of once per week.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

2. The computer must be protected by a firewall at all times when it is connected to the internet. Acceptable products include _____. Several popular choices include Zone Alarm, the Windows XP firewall, and Norton Personal firewall.

5.0 Remote Connection Requirements

The remote user shall use either dial-In or virtual private networking (VPN). Dial-In is typically used when the user is in a local calling area. VPN is typically used when the user would need to dial a long distance number to connect with a dial-in connection. VPN uses a local connection to an internet service provider (ISP) and creates a tunnel through the local ISP connection to the organizational network. This section specifies the requirements for Dial-In and VPN connections.

5.1 Dial-In Requirements

1. Number check - The dial in settings shall be set to perform one or the other of:
 1. Verify Caller ID to a specific number - Use this option if caller ID is available
 2. Always Call back to a specific number - If the user must connect from a location other than their designated location such as their home, they should use VPN.
2. Client Check - A requirement that must be set for Dial-In clients is that a firewall must be installed and operational. If the Dial-In client does not meet the criteria, either the connection is not allowed or the client can only access a limited area where they can get the software needed to meet the requirement.
3. Authentication - For authentication of the user, the dial in connection shall use one of:
 1. MS-CHAP version 2
 2. EAP-RADIUS
 3. EAP-TLS
 4. EAP-MD5-Challenge
4. Connection Encryption - This requirement will depend on the data you expect the remote user to be transmitting over the dial-in connection. Typically this should be encrypted especially if the user works for the Finance or Personnel department. The connection shall use one of the following encryption mechanisms:
 1. Microsoft Point to Point Encryption (MPPE)
 2. IPSec

5.2 VPN Requirements

1. Client Check - A requirement that must be set for VPN clients is that a firewall must be installed and operational. Also Anti-virus software must be installed and operational. If the VPN client does not meet the criteria, either the connection is not allowed or the client can only access a limited area where they can get the software needed to meet the requirement.
2. The connection choices are PPTP, L2TP, IPSec, and SSL. The connection shall use IPSec which encrypts the data sent through the connection.

3. Authentication - For authentication of the user, the dial in connection shall use Internet Key Exchange (IKE) with digital certificates. The other choice is Internet Key Exchange (IKE) with a pre-shared key.

IT Equipment Purchase and Failure Prevention Policy

1.0 Overview

This IT Equipment Purchase and Failure Prevention policy provides a guideline for the purchase of IT equipment when the equipment supports organizational identified critical services. This policy will name critical services and provide a guideline for purchasing technologies that are failure tolerant.

2.0 Purpose

The purpose of this policy is to ensure that critical services are not interrupted by a single common failure. It provides standard guidelines to allow IT equipment purchased for essential services to have reliability built into the equipment. This is to prevent service outage for critical services.

3.0 Scope

This policy covers any computers providing critical services to the organization.

4.0 Critical Services

Critical services which are required for normal operation of the organization include:

1. File sharing service on a file sharing server.
2. Web services to the internet
3. Email services
4. Database services for internal users and critical external applications.
5. Critical external application servers.
6. Domain controller servers
7. Firewall to connect these services to the internet.

Any servers or equipment that supports these services should adhere to this policy including connection equipment from the internet to these services.

5.0 Equipment Requirements

All critical services are required to utilize redundant technologies including:

1. Dual power supplies on all servers providing critical services.

2. RAID disk arrays to prevent one disk failure from interrupting services
3. Uninterruptable power supplies that can provide power for a minimum of 1 hour to servers operating critical services in the event of a power outage.

6.0 Additional Requirements

For services that are critical for income or operations that cannot be interrupted the following technologies are also recommended:

1. A backup generator to ensure that long term power outages cannot interrupt service.
2. More than one server for the same service where the servers use clustering or load balancing technology.

Mobile Computer Policy

1.0 Overview

This policy defines the use of mobile computers in the organization. It defines:

1. The process that mobile computers must meet to leave the university network. Both the device and any sensitive data should be password protected.
2. How mobile computers and devices will be protected while outside the organizational network.
3. The process that mobile computers must meet to enter the university network when being brought into a building owned by the organization.

2.0 Purpose

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

3.0 Scope

This policy covers any computing devices brought into the organization or connected to the organizational network using any connection method. This includes but is not limited to desktop computers, laptops, and palm pilots.

Note:

To write this policy, consider data and the sensitivity of the data stored and viewed on the mobile computer including:

1. Email
2. Data the user is working on that is stored locally.
3. Cached data that is stored locally such as cached data from the user's browser. Windows XP allows for cached files to be encrypted using the encrypting file

- system (EFS).
4. Data from the internal network that the user may access while the computer is outside the network.
 5. Locally stored user names and passwords.

Consider loss due to:

6. Theft - should locally stored data be encrypted?
7. Hard drive failure

4.0 Responsibility

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile computer and agrees to adhere to this policy. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator. The user of the computer agrees not to use the mobile computer for personal business and agrees to abide by the organizational computer usage policy.

5.0 Connection Terms

8. Devices connected to the organizational network must be determined to be a benefit to the organization rather than convenience by the designated IT manager.
9. All mobile devices owned by the organization or allowed on the organization network must be identified by their MAC address to the IT department before being connected. (Possibly require static IP address)
10. The device must meet the computer connection standards described in the following section.
11. The device operator must be identified by name and contact information to the IT department.
12. The computer device operator must be familiar with the organization's acceptable use policy.
13. Devices not owned by the organization are subject to a software audit to be sure no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.
14. Access rights to the organizational network cannot be transferred to another person even if that person is using an allowed computing device.

6.0 Mobile Computer Protection

1. Any mobile computer owned by the organization shall at all times operate the following for its own protection:
 1. Antivirus program named Symantec Endpoint Protection with the latest possible virus updates. The program shall be configured for real time protection, to retrieve updates daily, and to perform an anti-virus or malware scan at least once per week.

2. A firewall program named Symantec Endpoint Protection IDF with the latest possible updates. The program shall be operational any time the computer is connected to any untrusted network including the internet to protect the computer from worms and other malware.
 3. Additional malware protection software shall be active on the computer in accordance with the anti-virus and malware policy.
 4. The operating system and application patch levels must be consistent with the current patch levels of our organization for similar devices and operating systems. All mobile computers in the organization shall have wireless access disabled. If wireless access is used, a specific protocol for wireless encryption shall be designated and configured. Also the maximum data sensitivity category shall be noted for the computer depending on the security of the wireless access and other features of the computer.
2. Policy for mobile computers owned by the organization and removed nightly by employees with permission to work from home.
 1. These computers shall always meet requirement 6.0.1 above.
 2. If at any time the computer shall fail to meet the requirement 6.0.1 above, the employee shall report the condition to the IT Security department and a check of the computer equivalent to any check of an unsecure computer entering the building shall be performed.
 3. It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password. Operating systems that do not safely support this process shall not be used in mobile computers. The IT Security department will determine and specify the proper tools to be used for authentication and access controls.
 4. Data to be stored on the computer will be evaluated and rated to consider the sensitivity of the data according to the Data Assessment Process document. Any data stored on the computer that is considered to be sensitive will be stored only in an encrypted format, possibly using an Encrypting File System (EFS). The policy must define the encryption tool to use and how it will be maintained.
 5. The computer shall be checked weekly by IT Security department personnel at designated times when the computer will be entering a secure building area. The check will include a scan for malware and a test to determine whether the computer has a worm. The state of stored sensitive data shall also be checked to determine whether it is encrypted and whether data of too high a level of security is being stored on the computer. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.
 3. Policy for computers being used for travel - Protection of these computers shall be the encryption of all sensitive data and a requirement for a valid user ID to operate the computer.
 4. These computers shall always meet requirement 6.0.1 above. If any additional software installation is required, it must be done and configured before the computer leaves the building.
 5. It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password. Operating systems that do not safely support

this process shall not be used in mobile computers. The IT Security department will determine and specify the proper tools to be used for authentication and access controls.

6. Data to be stored on the computer during the time the computer is not in a security facility will be evaluated and rated to consider the sensitivity of the data according to the Data Assessment Process document. Any data stored on the computer that is considered to be sensitive will be stored only in an encrypted format, possibly using an Encrypting File System (EFS). The policy must define the encryption tool to use and how it will be maintained. Any data not considered to be safe to be stored on the computer will be removed using a designated program to be sure it has been removed so it cannot be read using special technology later. There will be a list of documented sensitive data including storage locations for all sensitive data stored on the computer. This list will be created before the computer leaves the facility.
 7. If there is a chance that the user will view any sensitive data using their web browser or other program, cached data will need to be encrypted. Cached data that is stored locally such as cached data from the user's browser will be set to be encrypted using the encrypting file system (EFS). This may require Windows XP or some third party software. In Windows XP, this may be enabled using the following procedure:
 1. Open "My computer"
 2. Click on "Tools" and select "folder Options".
 3. Select the "Offline files" tab.
 4. Check the box next to "Encrypt offline files to secure data".
 5. Click "OK" to exit.
 8. If the computer will acquire irreplaceable and valuable data while on the road, the computer user must notify the IT department so arrangements can be made for a method to back the data up.
- Policy for computers being used by contractors
 1. The computer will first be checked for compliance with section 6.01 above.
 2. The computer will be scanned for malware and tested to determine whether the computer has a worm. Any malware on the computer shall be removed if any was detected. Log information about any malware found.
 3. If the computer is in compliance with section 6.01 and contains no malware, the contractor shall report any sensitive data related to the organization that is expected to be stored on the computer.
 4. Data to be stored on the computer will be evaluated and rated to consider the sensitivity of the data according to the Data Assessment Process document. Any data stored on the computer that is considered to be sensitive will be stored only in an encrypted format, possibly using an Encrypting File System (EFS). The policy must define the encryption tool to use and how it will be maintained.
 5. The ID of the computer shall be recorded and it shall be certified for use on the organizational network.
 6. The computer shall be checked weekly by IT Security department personnel at designated times when the computer will be entering a secure building area. The check will include a scan for malware and a test to determine whether the computer has a worm. The state of stored sensitive data shall also be checked to determine whether it is encrypted and

whether data of too high a level of security is being stored on the computer. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly. If the computer is storing data improperly, the certification of the computer shall be reviewed.

7.0 Protecting the Network

Mobile computers entering the network shall meet the following requirements.

1. If the computer is owned by the organization and used regularly by employees according to 4.0.2 above, then the computer shall be checked according to that part of the policy.
2. If the computer is owned by the organization and is returning from a period when an employee used it for travel, the following check shall be performed.
 1. Determine whether the anti-virus program is up to date, has the latest virus definitions, is configured properly, and is running properly. If it fails one of these conditions or has not been scanned for a virus within the last week, a full virus scan must be done before the computer can be used in the building.
 2. Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
 3. Test the state of stored sensitive data to be sure it is encrypted.
 4. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.
3. If the computer is owned by an outside organization the following must be done.
 1. The outside organization must agree in writing to allow a malware scan of their computer and agree pay any costs if malware is found on their computer.
 2. A full virus scan must be done.
 3. Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
 4. Remove any malware on the computer if any was detected. Log information about any malware found. The outside organization may be billed for services depending on organizational policy.

8.0 Enforcement

Since improper use of mobile computers can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.



Computer Training Policy

A computer training policy and training of computer users will benefit the organization in both increased productivity but also fewer security incidents. This example computer training policy is a very rough draft and lists some areas that user training would be very beneficial to the organization.

However, given the current state of computer security and the fact that many attacks are directly against the user's web browser or through e-mail, user training is becoming an ever more important part of computer security. User's must be wise to the methods of attack in order to protect themselves in many instances. User training does not need to be extremely technical but should ensure that the user retains basic computer knowledge along with some knowledge about specific computer attacks that they may experience.

1.0 Overview

This policy defines the minimum training for users on the network to make them aware of basic computer threats to protect both themselves and the network. This policy especially applies to employees with access to sensitive or regulated data.

2.0 Purpose

This policy is designed to protect the organizational resources on the network and increase employee efficiency by establishing a policy for user training. When users are trained about computer use and security threats, they work more efficiently and are better able to protect organizational resources from unauthorized intrusion or data compromise. This policy will help prevent the loss of data and organizational assets.

3.0 Training Categories

Training categories will include but not be limited to the following areas:

- Basics:
 1. What files are
 2. How to set view for details and show extensions for known file types
 3. Why not seeing file extensions is a security hazard to you
 4. File storage size - how to determine
 5. Mail attachments
 6. Where to store files
 - How to use your network drive
 - What your network drive is and what it means to you
 7. How to copy files
 8. Ways to increase efficiency on the computer such as keyboard shortcuts
- Ways to get malware:
 1. Through email
 2. Through browser

3. By connecting
 4. By installing unapproved programs
- Email viruses:
 1. How they spread
 2. Spoofing sender
 3. Dangerous attachments
 - Email SPAM
 1. Protect your email address
 2. Filtering spam
 - Hoaxes:
 1. Phishing
 2. Fraud methods
 - Email use
 1. How to set up email for remote users or with your ISP with POP3
 2. How to set up out of office reply
 3. How to set mail filtering rules
 4. How to use, import, and export personal folders
 5. What an undeliverable response to an email message means
 - Use of web browser
 1. Safe browser?
 2. Avoid adware and spyware - ignore ads that may compromise your computer or get you to install an illicit program
 3. How to change browser settings for better security
 4. Products to prevent malware.
 - Passwords
 1. Why protect my password?
 2. Why do I need to change my password every 30 days
 3. How to change your password
 4. How to choose strong passwords that you can remember
 5. If I log in on a website can someone see my password?
 - Other
 1. Reasons for firewall -- worms and others
 2. Why worry about malware?
 3. What is vulnerability?
 4. Why not run all services?
 5. Social engineering

4.0 Training Opportunities

Basic training as listed in section 3.0 shall be provided internally by the organization and shall include the following opportunities:

Scheduled training seminars for 1 to 4 hours per day.

5.0 Requirements

All organizational staff shall make measurable and continuous progress in the training areas

listed in section 3. Each employee manager shall be responsible for ensuring that employees under their supervision make progress in the required training areas. Each employee must retain knowledge about training in areas listed in section 3 within the first year of employment.

6.0 Enforcement

Since training is very important to the security of the organization, auditing shall be used as a mechanism to be sure the training policy is being followed. Auditors may test employees at random about their knowledge in the areas listed in section 3. If an employee gets malware on their computer, they may be audited.

Anti-Virus Policy

1.0 Overview

This policy is an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

3.0 Anti-Virus Policy

The organization will use a single anti-virus product for anti-virus protection and that product is Symantec Endpoint Protection. The following minimum requirements shall remain in force.

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

4.0 Email Server Policy

The email server will have additional protection against malware since email with malware must

be prevented from entering the network.

4.1 Email Malware Scanning

In addition to having the standard anti-virus program, the email server or proxy server will additionally include ScanMail from Symantec Endpoint Protection which will be used to scan all email for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

4.2 Blocked Attachment Types

The email server or proxy server will block all emails with attachment types listed below. This is because these attachment types are dangerous containing active content which may be used to infect a computer with hostile software or because these attachment types are commonly successfully used by virus programs or malware to spread.

1. ade - Microsoft Access project extension can contain executable code.
2. adp - Microsoft Access project can contain executable code.
3. app - Microsoft FoxPro application is executable code.
4. asp - Active server pages
5. asx -
6. bas - Basic program source code is executable code.
7. bat - Batch file which can call executable code.
8. chm - Compiled HTML help file can contain executable code.
9. cmd - Windows NT command script file is executable code.
10. com - Command file program is executable code.
11. cpl - Control panel extension
12. crt
13. csh
14. dll - Dynamic link library is executable code. Could be placed on your system then run by the system later.
15. exe - Binary executable program is executable code.
16. fpx - Microsoft FoxPro is executable code.
17. hlp - Help file
18. hta - HTML program
19. inf - Setup information
20. ins - Internet naming service
21. isp - Internet communication settings
22. js - JavaScript file

23. jse - JavaScript encoded file
24. ksh - Unix shell file
25. lnk - Link file
26. mda - Microsoft Access add-in program
27. mdb - Microsoft Access program
28. mde - Microsoft Access MDE database
29. mdt - Microsoft Access file
30. mdw - Microsoft Access file
31. mdz - Microsoft Access wizard program
32. msc - Microsoft Common Console document
33. msi - Microsoft windows installer package
34. msp - Windows Installer patch
35. mst - Visual Test source files
36. ops - FoxPro file
37. pcd - "Photo CD image or Microsoft Visual Test compiled script"
38. pif - "Shortcut to MS-DOS program"
39. prf - "Microsoft Outlook Profile Settings"
40. prg - "FoxPro program source file"
41. reg - Registry files
42. scf - "Windows Explorer Command file"
43. scr - Screen saver
44. sct - Windows® script component
45. shb - Document shortcut
46. shs - Shell scrap object
47. url - Internet address
48. vb - Visual Basic file
49. vbe - Visual Basic encoded script file
50. vbs - Visual Basic file
51. vsd
52. vss
53. vst
54. vsw
55. wsc - Windows script component
56. wsf - Windows script file
57. wsh - Windows script host settings file
58. xsl - XML file may contain executable code
59. zip - Many viruses are commonly zipping files to keep them from being scanned and providing instructions to users about how to run the attachment. Many users still do this so to secure the network, it has become necessary to block this attachment type.

Do not depend on your anti-virus software on each computer to prevent these viruses. Viruses have a period of time when they spread unrecognized by anti-virus software. Blocking these file attachments will prevent many trouble calls. Give the users a work around for your network to get some of their files sent to other organizations. Your solution will depend on your network and the software that is being used to block the file attachments. In one case we renamed the file

to another type and instructed the recipient to rename it back to the original name before using it. This will not work in all cases since some file blocking software senses the actual file type regardless of its named file extension.

When an email breaks the rules and contains an illegal file attachment your policy should define one of the following to be done:

1. Delete the email and notify neither the sender nor the recipient. The problem with doing this is in the fact that people may be trying to send legitimate files to each other and have no way of knowing their communication attempts are failing. Training by letting users know what files are blocked can help remedy this problem
2. Delete the email and notify the sender - This will notify senders when their emails do not go through, but it will also notify senders who really did not send an email (when a virus spoofed them as the sender) that they sent an email with an illegal attachment. This can cause more additional help desk requests and questions for the administrator on the spoofed sender's side.
3. Delete the email and notify the sender and recipient. - This would have all the drawbacks of the above policy but would also increase help desk calls in your organization.
4. Remove the attachment and let the email go through. - This would let the receiver know that someone tried to send them an illegal attachment. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent. This policy would very likely cause your organization's help desk calls to increase with users calling to ask questions about why someone is trying to send them these files.

There is no ideal policy here and your system administrators must choose the best method depending on the situation being experienced by your organization. usually use the first option and provide training to users so they know these files are blocked and what the work around is for this situation.

4.3 Proxy or anti-spam Server

To increase mail security, many organizations are adding an anti-spam server or proxy mail server to their network. This reduces their mail server to the threat of being intruded upon and an anti-spam server can significantly reduce the load on the mail server, not to mention the reduction of spam. Your organization should decide whether to use one of these types of servers or whether to use a service to prevent spam. The service or devices used for this purpose should be defined in this policy. Periodic updates should also be defined and the person who manages the additional servers or is the point of contact for the services should be defined.

5.0 File Exchange Policy

This part of the policy specifies methods that are allowed to be used when files are sent into the network by members of the public or employees of the organization. It specifies:

1. All legitimate methods used including:
 1. FTP transfer to a FTP server.
 2. File transfer to a Web server with a legitimate file upload program.
 3. Any other method.

2. The method and type of software to be used to scan the files for hostile content before they are completely transferred into the network. It will also specify the update frequency for the scanning software.
3. The point in time when the files will be scanned.

6.0 Network Exploit Protection

This part of the policy should specify how hostile software that uses network exploits should be prevented. This policy will not cover system updates but may refer to the system update policy. This policy combined with other quoted policies should prevent worms from entering the network. This policy may also refer to the remote user policy and mobile computer policy.

This policy will specify that all systems be protected by a firewall any time they are connected to the internet. It would specify that systems on the organizational network be connected to a part of the network that is protected from the internet or untrusted network by an approved firewall system. It will also specify or refer to policy that requires computers operating outside the organizational network to have a local firewall software program operational at all times when these computers are connected to the internet. It should specify one or more acceptable software firewall products. This policy may refer to the mobile computer policy which may require users of mobile computers to have their computers checked for malware before connecting to the main network.

7.0 Other Malware Policy

This policy should cover any other possible malware including adware and spyware. It may specify methods to prevent and remove this type of malware. It may specify acceptable prevention and removal software. If the anti-virus product is a product that also handles other types of malware such as adware or spyware, it should be stated here.

Applicable Training

1. Blocked email attachments
2. How viruses work and avoidance
3. Adware and spyware avoidance



Wireless Use Policy

A wireless use policy is necessary for computer security since there is demand for wireless equipment in every organization today. It is best to set conditions and specify equipment that is approved for wireless use in order to minimize security risk associated with wireless.

1.0 Overview

This wireless use policy defines the use of wireless devices in the organization and specifies how wireless devices shall be configured when used.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion by those who would use wireless media to penetrate the network.

3.0 Scope

This policy applies to all wireless devices in use by the organization or those who connect through a wireless device to our organizational network.

4.0 Risk Assessment

The use of wireless technology has historically been a serious security risk to organizations. This is because it can be an easy access point to gain access to an organizational network. In addition data sent across it may be readable sometimes even when it is encrypted due to some of the vulnerabilities of the encryption schemes used. Therefore this policy requires a risk assessment any time a new type of wireless device is added to the network. Several items must be assessed including:

1. Is this a new technology?
2. Does this device use encryption and if so how well tested is the encryption protocol?
3. What is the cost of implementing a secure encryption protocol?
4. Has this type of device been used on our network before?
5. Can this device be configured to only allow authorized users to access it or the network through it?
6. How easy will it be for an attacker to fool this device into allowing unauthorized access? What methods may be used?
7. What secure authentication schemes are available and what cost or overhead is associated with their implementation and maintenance?
8. How practical is wireless use considering the cost, potential loss, and added convenience?

4.1 Authentication

The authentication mechanisms of all approved wireless devices to be used must be examined closely. The authentication mechanism should be used to prevent unauthorized entry into the network. One authentication method shall be chosen. The following must be considered.

1. How secure is the authentication mechanism to be used?

2. How expensive is the authentication mechanism to be used?

4.2 Encryption

The encryption mechanisms of all approved wireless devices to be used must be examined closely. The encryption mechanism will be used to protect data from being disclosed as it travels through the air. The following must be considered.

1. How secure is the encryption mechanism?
2. How sensitive is the data traveling through the wireless device?
3. How expensive is the encryption mechanism?

4.3 Configuration

The SSID of the wireless device shall be configured in such a manner so it does not contain or indicate any information about the organization, its departments, or its personnel including organization name, department name, employee name, employee phone number, email addresses, or product identifiers.

4.4 Access Points

All wireless access points and wireless devices connected to the organizational network must be registered and approved by the designated IT department representative. All wireless devices are subject to IT department audits and penetration tests without notice.

5.0 Authority

The acting CIO or highest level member of IT management shall have final authority over the management and security of wireless devices and wireless networking. This person may delegate these authorities as they see fit. This person should be responsible for the operation of the network.

6.0 Network Separation

This policy requires that parts of the network containing and supporting wireless devices directly (the wireless network) be separated from the part of the network that does not support wireless connections. The part of the network supporting wireless devices or connections shall be considered less trusted than the part of the network that does not. All file servers and internal domain controlling servers shall be separated from the wireless network using a firewall. One or more intrusion detection devices shall monitor the wireless network for signs of intrusion and log events. The type of logged events will be determined by the network administrator.

7.0 Allowable Wireless Use

1. Only wireless devices approved by make and model shall be used.
2. All wireless devices must be checked for proper configuration by the IT department prior to being placed into service.
3. All wireless devices in use must be checked monthly for configuration or setup problems.

8.0 Enforcement

Since improper use of wireless technology and wireless communications can open the network to additional sniffing and intrusion attacks, authorized and proper use of wireless technology is critical to the security of the organization and all individuals. Employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

Data Backup Policy

1. Purpose and Scope

The purpose of this policy is as follows:

- To safeguard the information assets of PSU
 - To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
 - To permit timely restoration of information and business processes, should such events occur.
 - To manage and secure backup and restoration processes and the media employed in the process.
2. This policy applies to all servers in the Information Technology (IT) Data and data Centers, including the Network Attached Storage (NAS)
3. The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.
- Backup retention periods are in contrast to retention periods defined by legal or business requirements.
 - System backups are not meant for the following purposes:
 - Archiving data for future reference.
 - Maintaining a versioned history of data.

4. Policy

A. Systems will be backed up according to the schedule below:

- Data stored on the NAS appliance will be regularly backed up as follows:
 - Incremental backup daily (Sat.-Thurs.) and data located on-site.
 - Full backup weekly (Fri.) and data located off-site.
- Exchange Mailbox stores will be regularly backed up as follows:
 - Full backup daily (Mon.-Fri.) and data located on-site.
 - Full backup weekly (Sat.) and data located off-site.
- Windows Servers (not in DMZ) will be regularly backed up as follows:
 - Incremental backup daily (Mon.-Fri.) and data stored on-site.

- Full backup weekly (Sat.) and data located off-site.
- The Virtual Machine Server will have its VM data drive regularly backed up as follows:
 - Image backups of virtual machines will be taken on Tuesday and Thursday. These backup files will be stored on-site.
 - Weekly file and folder full backup will be taken on Sunday. These backup files will be stored off-site.
- The Catalog tape will be regularly backed up as followed:
 - Full Hot Catalog backup daily (Mon.-Fri.) stored to Hard Disk on NAS.
 - Full backup weekly (Sat.) copied to tape stored off-site.

B. Backup tapes will be transported and stored as described below:

- Currently all backups will be written to reusable DDS4 media with capacity of 20 GB uncompressed (40 GB compressed) and a transfer rate of 60 MB/Sec (native).
- Media will be clearly labeled and stored in a secure area that is accessible only to IT staff or employees of the contracted secure off-site media vaulting vendor used by IT.
- During transport or changes of media, media will not be left unattended.
- Daily backups will be stored on-site in a physically secured fire-proof safe located in a building separate from the Data Center.
 - Daily backups will be maintained for one week.
- Weekly backups will be stored in a physically secured, off-site media vaulting location maintained by a third party.
 - Weekly backups will be maintained for a period of three weeks.
 - After the period of three weeks has elapsed, the tapes will be returned to IT and will be either re-used or destroyed.

C. Media will be retired and disposed of as described below:

- Prior to retirement and disposal, IT will ensure that:
 - The media no longer contains active backup images
 - The media's current or former contents cannot be read or recovered by an unauthorized party.
- With all backup media, IT will ensure the physical destruction of media prior to disposal.

D. Backups will be verified periodically.

- On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
 - To check for and correct errors.
 - To monitor the duration of the backup job.
 - To optimize backup performance where possible.
- IT will identify problems and take corrective action to reduce any risks associated with failed backups.

- Random test restores will be done once a week in order to verify that backups have been successful
- IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

E. Data Recovery

- In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.
- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

F. Restoration Requests

- In the event of accidental deletion or corruption of information, requests for restoration of information will be made to Organization IT department.

Firewall Policy

PSU's department of information Technology and Network Services operates a firewall to enhance security between the Internet and the organization network to establish a reliable network for the organization computers and network resources. The Firewall is a key component of the Organization's network security architecture.

This Firewall Policy governs how the firewall will filter Internet traffic to mitigate the risks and losses associated with security threats to the PSU network and information systems. This policy will attempt to balance risks incurred against the need for access.

1. Purpose

A firewall is one element of security for the campus network. It reduces the threat of outsiders either damaging PSU systems or using the systems as a jumping off point for illegal entry into other systems. A firewall does not prevent malicious or illegal activities from inside the firewall. This policy is designed to protect the PSU computers (users, servers) from hacking and virus attacks by restricting access to computers on the organization network from users who are outside the network.

2. Scope

The policy applies to all PSU information technology network users: employees, contractors, vendors, partners, systems, applications and networks.

3. Definitions

Firewall

A Firewall is a hardware and software device that controls access between two networks. There are several different mechanisms for performing this access control but the essential point is that a firewall implements a network security policy.

Firewall System

A firewall system includes both the Firewall Product and additional controls, that may or may not be available as part of the base firewall product. Typically these can comprise solutions to block or filter content; e.g. anti-virus email gateways, intrusion detection systems, audit and logging tools, mobile code (ActiveX, Java) monitors, integrity checkers, email content scanners and URL blockers.

4. Responsibilities

PSU IT Operations department is responsible for implementing and maintaining the organization network perimeter firewall. Therefore, IT department is also responsible for activities relating to this policy. Responsibility for information systems security on a day-to-day basis is every employee's responsibility. Specific guidance and direction for information systems security is the responsibility of IT Operations.

PSU Network to the Internet: Services which are NOT allowed	Internet to PSU Network: Services which ARE allowed
<ul style="list-style-type: none">• All Microsoft Networking Protocols• Network Monitoring Protocols• Virus Related Protocols• Spyware Related Protocols	<ul style="list-style-type: none">• E-mail Server• Web Server• Moodle• SSS (FTP Only)• Software (FTP Only)• Library Catalog and Databases• Remote Desktop to Any OSX and Windows XP System• Web Helpdesk• Terminal Services• Library Catalog Search• Remote Desktop (as needed)• Other Departmental Servers

5. Operational Procedures

Only firewall system administrators are permitted to logon to the firewall.

- Access to firewall hosts must be tightly controlled. Only firewall system administrators are allowed to have user accounts on firewall hosts.
- Firewall system administrators must have personal accounts; i.e. no group logins are allowed.
- Direct remote root access is not allowed. All root access must be via a personalized logon.
- Only personnel with the appropriate authorization can make changes to the firewall access rules, software, hardware or configuration.
- All changes should be as a result of a request recorded using the Firewall Change Request Procedure although emergency modifications can be requested by phone, with a follow up email and change request.
- Only authorized personnel must be able to implement the changes and an audit log must be retained.

ONLY AUTHORIZED departmental technical contacts may request any changes to the PSU firewall. These requests must be submitted in writing or electronic including a rationale for the request by submitting the Firewall Change Request Procedure. It is recommended that submit the request by visiting the helpdesk site.

The Operations Manager of PSU will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the original requestor and alternative solutions will be explored.

If during the implementation it is determined that the original request does not provide the functionality to meet the unit's business need, then the Operations Manager of PSU has the authority to deny the request.

IT Operations division will, on a short-term basis; provide open access through the firewall.

Subsequently, long-term, the IT Operations division will work with the requestor to determine exactly what ports are needed to meet the unit's business needs. Certain mission-critical functions require outside vendors and other entities to have secured and limited access to departmental network resources from the Internet to PSU network. This access needs to be approved by the department technical contact and then coordinated through IT Operations division by submission of the Firewall Change Request Procedure.

If the original requestor considers the solution to be unsatisfactory, the request may be appealed to the Director of Information Technology and Network Services.

Turnaround time for a request for a normal change request will be handled in approximately 5 business days from the receipt of the Firewall Change Request Procedure. Common Services include:

- FTP
- Telnet/SSH
- Mail
- Remote Access
- SMTP
- HTTP/HTTPS

Turnaround time of a request for any emergency request will be handled as quickly as possible. To be an emergency the change must correct a major security risk. This additional time is needed to investigate that risk associated to the organization.

6. Configuration

The firewall will be configured to deny any service unless it is expressly permitted.

- If there are no rules defined for a organization network address, then traffic to or from that address must be denied.
- Access to the organization network must be blocked during the start-up procedure of the firewall.

The firewall Operating System will be configured for maximum security.

- The underlying operating systems of firewall hosts must be configured for maximum security, including the disabling of any unused services.

The firewall product suite must reside on dedicated hardware.

- Applications that could interfere with, and thus compromise, the security and effectiveness of the firewall products, must not be allowed to run on the host machine.

The initial build and configuration of the firewall must be fully documented.

- This provides a baseline description of the firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

Security must not be compromised by the failure of any firewall component.

- If any component of the firewall fails, the default response will be to immediately prevent any further access, both "outbound" as well as "inbound".
- A firewall component is any piece of hardware or software that is an integral part of the firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g. bad maintenance of the rules database on the firewall or software which is incorrectly installed or upgraded.
- IP forwarding at the operating system level must be disabled until the firewall software is operational and IP filtering policies active.

7. Audit and Compliance

Regular testing of the firewall will be carried out

a. The firewall must be regularly tested for:

- Configuration errors that may represent a weakness that can be exploited by those with hostile intent.
- Consistency of the firewall rule set; i.e. to confirm the current status matches that expected (and documented).
- secure base system implementation; i.e. the integrity of the firewall hosts and applications must be verified using an integrity-checking tool

The firewall system must have an alarm capability and supporting procedures

b. When an agreed specified event occurs, an alarm must be sent to the security personnel.

Documented procedures must exist to permit an efficient response to such firewall security alarms and incidents.

- c. There may be specific circumstances when it would be advantageous for the firewall system to react in an automated manner to defined security events.
- d. In the event that the firewall itself is the subject of malicious attempts to penetrate it, and the firewall has the capability, delivery of services should be terminated rather than permit uncontrolled access to the organization network.

There must be an active auditing/logging regime to permit analysis of firewall activity either during or after a security event

- An audit trail is vital in determining if there are attempts to circumvent the firewall security.
- Audit trails must be protected against loss or unauthorized modification.
- The firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

8. Periodic Review of Firewall Security Policies

Firewall security policies will be reviewed at least yearly. When there are major changes to the network requirements this may warrant changes to the firewall security policy.

9. Policy and Procedures

The Firewall permits the following for outbound and inbound Internet traffic:

- **Outbound**- Allow ALL Internet traffic to hosts and services outside of PSU network with the exception of known security vulnerabilities. This allows anyone connected to the PSU Network to utilize all services on the Internet with the exception of known vulnerabilities.
- **Inbound**- Only specific services which support PSU business mission will be allowed to be accessed from the Internet. The chart identifies the most common services used for Internet communications within the PSU network environment.

The following is a limited explanation for each column:

Server Functions and Services - This a listing of the most common Internet services used on the organization file servers to support the mission and business of the organization.

Organization Network to Internet - All traffic originating from organization computers to an external host has no firewall policies applied except for known security vulnerabilities which are described in the chart.

Internet to Organization Network - All traffic originating from a computer on the Internet (somewhere outside network) to a computer on the organization network is only allowed into the following systems.



E-Mail Usage and Management Policy

Introduction and Statement of Purpose

Electronic mail (e-mail) refers to the electronic transfer of information typically in the form of electronic messages, memoranda, and attached documents from a sending party to one or more receiving parties via an intermediate telecommunications system. E-mail is a core tool utilized by companies to improve the way they conduct business by providing a quick and cost-effective means to create, transmit, and respond to messages and documents electronically. Well-designed and properly managed e-mail systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. These opportunities are, however, at risk if e-mail systems are not used and managed effectively.

The purpose of this policy is to promote the use of e-mail as an efficient communication and data gathering tool, to ensure that companies have the information necessary to use e-mail to their best advantage in supporting University business, to avoid non-work-related distractions of employees, to avoid subjecting the State's e-mail system to computer viruses, and to otherwise avoid interfering with or damaging the effective functioning of the organization's e-mail system. By establishing and maintaining compliance with a policy for appropriate use and management of e-mail, risks and costs to agencies can be mitigated while maximizing the potential of this communication tool.

1. Scope

This policy applies to all organization employees, as well as contract staff, who use the organization's electronic mail.

General Policy

It is the policy of organization that e-mail is used for internal and external communications that serve legitimate Organization functions and purposes. Any personal use must be of an incidental nature and not interfere with business activities. Personal use must not involve solicitation, must not be associated with any outside business activity or personal gain, must not be libelous or defamatory, must not violate the organization Policy on Employee Harassment, must not potentially embarrass the organization, its employees, its employers or be used for any unlawful purpose. Copyright restrictions and regulations shall be observed. The information communicated over University e-mail systems is subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats and is not to be utilized for political purposes.

Organization is responsible for enforcing this policy and establishing management practices consistent with this policy that, among other goals:

- support organization business;
- reduce legal and other potential risks;
- define managerial authority over e-mail communications;
- describe the appropriate use of e-mail communications;
- train employees in e-mail use and policies; and
- Provide for necessary records retention, accessibility, and protection.

Agencies with special requirements for information confidentiality (for example, confidential client records) may be required to establish additional safeguards to protect this data.

Access to E-mail Services

E-Mail services are provided to all appropriate staff and contractors within departments. To request access, contact the IT Operations or IT User service division.

Privacy and Access

- Mail messages are not personal and private. Managers, supervisors, and technical staff may access an employee's e-mail in accordance with the department security policy for reasonable business purposes, including but not limited to:
 - for a legitimate business purpose (e.g., the need to access information when an employee is absent);
 - to diagnose and resolve technical problems involving system hardware, software, or communications; and/or
 - To investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.
- An employee, with the exceptions noted above, is prohibited from accessing another user's e-mail without his or her permission.
- All e-mail messages including personal communications may be subject to discovery proceedings in legal actions.
- All e-mail messages sent or received and which are not otherwise protected by law, are public documents and may be released to the public under the Freedom of Access.

Security

E-mail security is a joint responsibility of technical staff and e-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their e-mail account by unauthorized individuals.

Management and Retention of E-mail Communications

A. Applicable to all e-mail messages and attachments

Since e-mail is a communications system, messages should not be retained for extended periods of time.

Users should:

- Remove or archive all e-mail communications in a timely fashion.
- Delete records of transitory or little value that are not normally retained in record keeping systems as evidence of a business activity.

B. Applicable to records communicated via e-mail

E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records and are subject to the records management requirements documented by the organization Archives. Records communicated using e-mail need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements.

For organization specific questions surrounding record retention requirements contact IT Operations division Archives for assistance.

Examples of messages sent by e-mail that typically are records include:

- policies and directives
- correspondence or memoranda related to official business
- work schedules and assignments
- agendas and minutes of meetings
- drafts of documents that are circulated for comment or approval
- any document that initiates, authorizes, or completes a business transaction
- final reports or recommendations

Some examples of messages that typically do not constitute records are:

- personal messages and announcements
- copies or extracts of documents distributed for convenience or reference
- phone message notes

Roles and Responsibilities

- Executive management will ensure that the policy is implemented by program unit management and unit supervisors.
- Unit managers and supervisors will develop and/or publicize record keeping practices in their area of responsibility including the routing, formatting, and filing of records communicated via e-mail. They will train staff in appropriate use, including appropriate

personal use of e-mail that does not result in performance issues, and be responsible for ensuring the security of physical devices and passwords.

- Network administrators and internal control (and/or internal audit) staff is responsible for e-mail security, backup, and disaster recovery.
- Users are responsible for adherence to this policy.

Proper Usage

All e-mail users will understand and comply with this policy, including but not limited to:

- understand that personal use must be of an incidental nature only
- comply with University and unit policies, procedures, and standards
- protect confidentiality
- be aware that sending e-mail of a political nature (supporting candidates, soliciting contributions, etc.) is against the law and subject to criminal penalties
- immediately delete any chain letters received through the organization's e-mail system
- consider organizational access before sending, filing, or destroying e-mail messages.
- protect their passwords
- receive approval of supervisor and permission from the CEO, Presidents, Directors of the Department of Administrative and Financial Services, or her designee, before sending organization wide communications
- respond to e-mail in a timely fashion
- do not in any way use e-mail access or transmit prohibited content of a sexual nature
- delete any messages that may contain offensive material and report to management
- Remove personal messages, transient records, and reference copies in a timely manner.
- not use e-mail for outside business activity or personal gain
- observe all copyright restrictions and regulations
- not use e-mail for any unlawful or illegal purpose
- not use e-mail to promote discrimination on the basis of race, religion, national origin, disability, sexual orientation, age, marital status, gender, or political affiliation
- not create e-mails that may be defamatory or libelous
- consider organizational access and retention requirements before sending, filing, or destroying e-mail messages
- be courteous and follow accepted standards of etiquette
- must not use the e-mail system to solicit for causes unrelated to organization business
- must not knowingly send or receive e-mails that contain a virus

Violations of this policy

Any violation of this policy could result in disciplinary action up to and including termination.

Policy Review and Update

The Office of Chief Information Officer will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be directed to the Chief Information Officer.



Computer Replacement Program (CRP) Policy

In an effort to provide the PSU faculty and staff with the appropriate technology resources, ITCS staff and the Technology Committee have devised a Computer Replacement Program (CRP). The CRP is a system for centralized management of institutional computer resources for inventory control maintaining schedules and standardization of the desktop computing environment for compatibility and service offering.

Objectives/Goals:

The goal of the program is to ensure that computing resources in the PSU are current and adequate for performing work related tasks.

The objectives of the CRP are to:

- Ensure that all faculty and staff members who use computing resources in their positions have access to a computer of sufficient capability to support basic computing needs* in fulfillment of their work responsibilities;
- Ensure that appropriate computing resources are available in departmental computing facilities and university offices in support of PSU mission;
- Streamline the specification, acquisition, and deployment of new equipment and re-deployment or disposal of old equipment;
- Deploy a campus-wide backup program to protect university data on desktop computers.
- No faculty left behind program (faculty development)

The goals of the technology committee in regards to the CRP are:

- Establish a centralized budget which provides basic computing resources for PSU employees, thereby providing relief to area budgets and reducing reliance on year-end surplus and current fund contingency for the CRP;
- Implement minimum standards for computing resources in PSU increasing the supportability of the institution's installed base of equipment;
- ERTC staff and the technology committee will review the technology plan and evaluate the CRP annually, monitor information collected through audits, feedback from program participants, external vendor and industry sources, and institutional priorities to make recommendations.

* “Basic Computing Needs” include word processing, electronic messaging, Library access, Internet (web) access, spreadsheet, simple database, and basic institutional data access. Other specialized needs, such as secondary computers, advanced hardware, and other specialized needs must be funded from other funds.



Program Guidelines

CRP Process

The program seeks to provide adequate technology for employees. We expect to replace and / or upgrade equipment once every two to four years. This lifecycle enables users to have the latest computer technology and the most recent operating systems and application versions. However, the volatility of the computer industry and system prices may require minor adjustments to this lifecycle.

CRP Replacement Criteria

1. Advances in technology are used to determine replacement along with age of existing system and the ability to run current software.
2. The cut-off point for which computers should be replaced is determined by the hardware audit and the level of performance that it can run current applications efficiently. The audit is an automatic service that runs when logging onto the network that records all hardware and software installed on the computer.

Note: *Hardware may be upgraded for a lower cost than replacing the complete system and may be a determining factor in some situations.*

What you should do to prepare for the replacement?

1. **Backup up your files.** It is crucial that you save any important or critical data files to a network drive or to other reliable media such as a CD or DVD before the ERTC arrives to replace your computer. If you must save files to your computer, please save them in your My Documents folder.
2. **Know where your files are saved.** Locate any specialized files or custom configuration files and save them to your backup location. For example, your Internet Explorer bookmark file (*bookmark.htm*), an image used for your Windows wallpaper, etc.
3. **Gather up any non-standard software you use.** You will need to supply the ERTC with the original media, along with a proof of purchase. If you have software that is Shareware, you must supply documentation proving this. There have been instances in the past in which Universities have been audited for legal software, with the unfortunate result being very stiff fines for the inability to prove software legality.

