

Carnegie Institution Headquarters Information Systems Policies and Procedures

The following information systems policies and procedures of the Carnegie Institution's Headquarters office are intended to support the protection, control and management of the organization's information systems assets. All employees, contractors, consultants, visitors, and other workers of the Carnegie Institution, and those employees of external organizations who utilize Carnegie Institution systems resources or access information and records of the Carnegie Institution's Headquarters are covered by certain applicable portions of these policies and procedures.

Table of Contents

Selected IS Policies for Users.....	4
Acceptable Use.....	4
Appropriate Use of Information Systems Resources.....	4
Excessive Use of Information Systems Resources.....	4
Misuse and Abuse of Information Systems Resources.....	4
User Accounts.....	4
Eligibility.....	4
Privileges.....	5
Responsibilities.....	5
Account Creation, Management and Termination.....	5
Passwords.....	6
Networking.....	7
Connecting to the Network.....	7
Remote Access.....	8
Wireless Access.....	8
Third-Party Access.....	8
Email.....	9
Email Accounts.....	9
Email Aliases.....	10
Email Lists.....	10
Systems Support.....	10
Help Desk.....	10
Data Backup, Storage and Retrieval.....	11
Purchasing, Recycling, Retiring and Disposal.....	12
Acquisition of Information Systems Resources.....	12
Inventory Control.....	12
Recycling, Retiring and Disposal of Information Systems Assets.....	13
Computer Data and Media Disposal Policy.....	13
Computer Equipment Replacement Policy.....	13
Security.....	14
Protection against Viruses, Malicious Software, Hoaxes, and Spam.....	14
Systems Vulnerability Scanning.....	15
Reporting Information Security Incidents.....	15
Privacy and Legal Policies.....	15
Privacy and Confidentiality of Electronic Information and Information Systems Resources.....	15
Software Copyrights Policy.....	16
General IS Policies.....	17
Information Systems Governance.....	17
Corporate Governance.....	17
Headquarters Information Systems Planning Council.....	17
Strategic Planning.....	17

IS Organizational Structure and Responsibilities.....	17
Policies, Procedures, Standards and Guidelines.....	17
Lifecycle Management.....	18
Budgeting.....	18
Capacity Planning.....	18
Service Support.....	18
Incident Management.....	18
Problem Management.....	18
Change and Release Management.....	18
Patch Management Policy	19
Service Delivery.....	19
Domain Names.....	19
WWW Policy.....	20
Information Security.....	21
Information Classification and Handling.....	21
Information Security Awareness and Training Policy.....	22
Information Security Roles and Responsibilities.....	22
Risk Assessment and Treatment.....	24
Credit Card Processing and Security.....	24
Segregation of Information Systems Duties.....	25
Physical and Environmental Security of Facilities.....	26
Continuity Management and Disaster Recovery.....	26
Systems Audit.....	27
Procedures.....	28
Account Creation Procedure.....	28
Account Changes Procedure.....	28
Account Termination Procedure.....	28
Data Backup and Storage, Financial System.....	28
User Account Management, Financial System.....	29
Systems Development Life Cycle Methodology, Administrative Systems.....	29
In-house Development of Software.....	30
Guides and Best Practices.....	31
Guide for Appropriate Use of Information Systems Resources.....	31
Guide for Appropriate Use of Email.....	32
Guide for Secure Removal of Data.....	32
Guide for Laptop and Portable Device Use.....	33
Email list manager and owner responsibilities.....	33

Selected IS Policies for Users

Acceptable Use

Appropriate Use of Information Systems Resources

The Carnegie Institution Headquarters' information systems are for authorized use only. Access for any reason must be specifically authorized by the Carnegie Institution. Carnegie Institution computers, computing systems and their associated communication systems are provided to support the official business of the Institution. Official business includes authorized work connected with the operation of the Institution, including but not limited to associated and authorized development, education, administrative and support activities. See Human Resources policy and Guide for Appropriate Use of Information Systems Resources for additional information.

Excessive Use of Information Systems Resources

Excessive use exists when a user or process has exceeded established limits placed on the service, consumes a resource to a level that degrades service to other users, or where the actions of a user could cause degradation if the user is permitted to continue the practice or activity. The systems administrator will notify the user that he or she is consuming an excessive share of the resource. If the user's need cannot be accommodated, then the user may find it necessary to cease the activity, reduce the activity to an appropriate level, or find other options on a temporary or permanent basis. IS staff may temporarily suspend or block access to an IS resource, or stop active processes in an account, when it reasonably appears necessary to protect the integrity, security, or functionality of the resource, or to protect other computing resources, or to protect the Institution from potential liability.

Misuse and Abuse of Information Systems Resources

Misuse or abuse are uses that violate existing laws or institutional policies and procedures, or that otherwise violate generally accepted ethical norms and principles. Misuse or abuse often involves the use of IS resources to engage in behavior that is prohibited or otherwise addressed in general policies and procedures issued by the Carnegie Institution. Whenever appropriate, such general policies and procedures will be used to address misuse or abuse of IS resources. IS staff members are available to provide consultation or advice related to systems use or misuse to any employee. Reports of apparent misuse or abuse of Carnegie Institution IS resources should be made to IS staff. Reports of misuse or abuse are normally resolved through established Carnegie disciplinary policies and procedures.

User Accounts

Eligibility

Current Headquarters staff, departmental staff, interns, volunteers, contractors, consultants, and certain persons affiliated with external agencies collaborating with Carnegie are eligible to access and use Carnegie Headquarters IS resources.

Appointed staff, interns, volunteers and hourly employees are eligible to use resources until the termination of their employment or appointment.

Contract employees, consultants and persons associated with external entities that have a contract or other collaboration with Carnegie Headquarters are eligible to use systems resources, if such access is necessary to fulfill the purposes of the contract or collaboration. A full-time Carnegie Headquarters faculty or staff member in the unit that is most closely associated with the activity must submit the request to add an account via the Help Desk system.

Other external persons are eligible to use Carnegie systems resources with certification by an appropriate administrator of the person's involvement in activities that support the mission of Carnegie.

Return to Index

The Institution may also provide limited access accounts for specialized purposes, such as for potential employees, employees who are not yet enrolled, departed employees, conference attendees, or visitors requiring only access to the Internet from their personal computers. A service fee may be assessed for this access.

The privilege of initial and continued eligibility to use IS resources by all persons requires initial and periodic verification by the appropriate staff member and the systems administrator that the access is for purposes that support the operations or mission of the institution. Units are responsible for keeping official personnel records updated to reflect new and departed personnel. The system administrator shall conduct monthly eligibility reviews based on information supplied by the Human Resources office and other documents, record the reviews in the Help Desk system, and correct all problems if necessary.

Privileges

Access – The Carnegie Institution will provide access to appropriate Headquarters information systems resources and the attached networks to all eligible members of the Carnegie community whose work requires it. In general, access to public and internally available information is not restricted by access controls that discriminate by specific user. Access to confidential or restricted information is granted only when a legitimate business need has been demonstrated and access has been approved in advance by the information owner. Access to special hardware and software must be restricted based on business need.

Availability - The Carnegie Institution seeks to make its central computing and systems resources and networks available to users with few interruptions and a high level of service.

Security - Headquarters IS staff will help users of its central and shared systems resources protect the information they store on those resources from accidental loss, tampering, unauthorized search, or other access.

Privacy and Confidentiality – Carnegie will provide a confidential environment under the conditions set by its “Privacy and Confidentiality of Electronic Information and Information Systems Resources” policy.

Responsibilities

All headquarters systems resources and network capacity are for purposes related to Carnegie's mission of research, education, and public outreach.

Users are responsible for correct and sufficient use of the tools that each system provides for maintaining the security and confidentiality of information stored on it.

Systems resources and network capacity have to be used for appropriate purposes as described in the Acceptable Use policies.

Users can facilitate systems usage in the Headquarters environment in many ways. Collegiality demands the practice of facilitative computing, including regular deletion of unneeded files from one's accounts, refraining from overuse of storage space, printing facilities, or other processing capacity and refraining from overuse of Internet services and network capacity.

Users must be familiar with and comply with Carnegie Institution Headquarters Information Systems Policies and Procedures.

Account Creation, Management and Termination

Generally, the employee's manager should initiate approval for access via an email to the Help Desk. All non-employees, contractors, consultants, temporary employees, outsourcing organizations and other eligible entities must also go through a similar access control request and authorization process initiated by the relevant project manager. Units are responsible for keeping official personnel records related to projects to reflect the access rights of new, active and departed personnel.

Any privileges remain in effect until the person's job changes or the person leaves the Carnegie Institution. Managers should notify IS staff immediately of employment status changes. Accounts of terminated employees and other departed personnel should be disabled as soon as the person leaves the Institution unless requested otherwise by the person's

Return to Index

supervisor. Eligibility and privileges are subject to periodic reviews.

Each user must be assigned his or her own unique user ID. Every Carnegie Institution user ID and related password are intended for the exclusive use of a specific individual. The user is responsible for all activity that takes place under his or her user ID and password or other authentication mechanism.

System tools may be deployed to check for any computer accounts that have not been used for a certain period of time. Dormant user IDs of eligible personnel that have no activity will have their privileges reviewed after 30 to 90 days.

Managers and systems administrators may temporarily suspend or block access to an account when it reasonably appears necessary to do so in order to protect the integrity, security, and functionality of the Institution or other computing resources, or to protect the Institution from liability.

Access to Carnegie systems resources may be removed immediately by means of a request to the Help Desk from the appropriate authorities, the supervisor or administrator of an employee, or the sponsor of the account. Reasons for removal may include, but are not limited to, the following: the individual is terminated for cause and there is concern for safety of systems or data; there is reasonable belief that the individual to whom the account is assigned has perpetrated or is involved in illegal activities or activities that violate Carnegie policy.

The systems administrator responsible for a particular service may disable access unilaterally if processes in an assigned account are causing or reasonably appear likely to cause damage to systems or data, or serious service degradation for other users. Except when prohibited by law, or notice is inappropriate or impractical, the systems administrator will notify the involved individual prior to disabling the computer account. Where prior notification is not permitted, appropriate, nor practical, the systems administrator will make all efforts to notify the involved individual in a timely manner. Unless other policies are invoked, access will be restored as soon as possible after the removal of the threat.

Passwords

All Headquarters employees, third parties, contractors and others with access to Carnegie Institution systems are responsible for taking the appropriate steps to select and secure their passwords.

Passwords must be complex, and changed regularly. Employees should not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences, personal details. Users must not construct fixed passwords that combine a set of characters that do not change, with a set of characters that predictably change. Strong password protection should be enforced by the system when possible.

Passwords issued by systems administrators must be forced to expire, requiring the user to choose another password before the next login process is completed.

In general, a user should be authenticated in person to obtain a new or changed password. In some instances, such as when an employee is on travel or works at an off-site location, other authentication methods can be used.

Fixed password changes and resets may be performed only by the involved user. Under no circumstances may a user delegate or otherwise request that another person handle this task on the user's behalf. Employees must not share Carnegie Institution passwords with anyone, including IS staff members, supervisors, or assistants.

Fixed passwords must not be stored in voice messages, sent unencrypted in electronic messages or emails, or in readable form in files, automatic login scripts, or in any other locations where unauthorized persons might discover or use them. Passwords sent in encrypted electronic messages or stored in encrypted files must be separate from user IDs, having no indications about the nature of the content.

Users must never write down or otherwise record a readable password and store it near the access device to which it pertains.

Users must change their password immediately if they suspect that it has been discovered or used by another person. Users must notify an IS staff member if an access control mechanism is broken or if they suspect that these mechanisms have been compromised.

Scanning for weak password should be the part of a periodic vulnerability assessment review. Security incidents related to weak passwords or inappropriate sharing should be also reviewed periodically by systems administrator. The systems administrator shall record the results of these reviews in the Help Desk system and correct all problems if necessary.

Networking

Connecting to the Network

Users must register their computers and other network devices with the systems administrator before connecting them to the network. IS maintains a database of unique machine identification, network address and owner for the purposes of contacting the owner of a computer when it is necessary.

Users may connect devices to the Headquarters network only at appropriate connectivity points such as data jacks, approved wireless network access point, or a VPN or SSH tunnel.

Only IS staff is allowed to extend or modify the Carnegie network, including adding switches, hubs, wireless access points, or network extension cables.

Every computer or other device connected to the network, including a desktop computer, must have an associated owner or custodian. Owners and custodians are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it.

Owners and custodians must ensure that all computers and other devices capable of running anti-virus/anti-malware software have Carnegie-licensed anti-virus software (or other approved virus protection products) installed and running.

Computer owners or custodians must install the most recent security patches on the system as soon as practical. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.

Computer owners of computers that contain sensitive Carnegie data should apply extra protections with the help of IS staff.

Headquarters units are responsible for providing reliable services for certain functional areas of the entire Institution. As such, individuals may not operate any service which might disrupt or interfere with centrally-provided services. These services include, but are not limited to firewalls, file servers, wireless services, POP, IMAP, SMTP, DNS, DHCP, WWW, FTP and streaming services.

Carnegie staff members regularly monitor the network for external intruders, scan hosts on the network for suspicious anomalies and block harmful traffic. All network traffic passing in or out of Carnegie's network is monitored by an intrusion detection system for signs of compromises. By connecting a computer or device to the network, users of the Carnegie network acknowledge that the network traffic to and from their computers may be scanned.

Carnegie staff members routinely scan devices attached the network, looking for vulnerabilities. At times, more extensive testing may be necessary to detect and confirm the existence of vulnerabilities. By connecting to the network, users agree that their computer or device can be scanned.

The Carnegie Institution reserves the right to take necessary steps to contain security exposures and/or improper network traffic. Carnegie will take action to contain devices that deviate from normal usage patterns, therefore allowing normal traffic and central services to resume. Carnegie will block devices that impose an exceptional load on a service, exhibit a pattern of network traffic that disrupts centrally provided services, exhibit a pattern of malicious network traffic associated with scanning or attacking others, and/or exhibit unacceptable behavior, see "Excessive Use" and "Misuse and Abuse of Information Systems Resources" policies.

The Carnegie Institution reserves the right to restrict certain types of traffic coming into and across its network. We restrict traffic that is known to cause damage to the network or hosts on it, and may control other types of traffic that consume too much network capacity, such as file-sharing traffic.

By connecting to the network, users acknowledge that a computer or device that exhibits any of the behaviors listed above is in violation of this policy and will be removed from the network.

Remote Access

Remote access to Carnegie Institution computers and network is granted only to those users who have a demonstrable business need for such access.

The Carnegie Institution's security requirements apply at remote locations, although the specific implementation may differ.

All portable and remote computers that are under the control of Carnegie Institution Headquarters employees and that are used to process Carnegie Institution information must be used exclusively by the employee and should be protected with an approved access control method to authenticate and authorize users and computers, where appropriate, prior to granting access to a Carnegie Institution information system asset. Access control implementations must prevent unauthorized use of the machines and unauthorized access to Carnegie Institution information. Computers must be further protected from virus infections and other types of damage from malicious software.

All remote users must connect to Carnegie Institution Headquarters computers and internal networks through authorized communications systems such as firewalls, and VPN gateways. Inbound and outbound connections to and from Carnegie Institution computers or networks through an office desktop modem are prohibited unless specific approval has been obtained from information systems staff.

Care of any Carnegie Institution owned equipment and supplies at a remote location is the responsibility of the employee. Equipment owned or provided by the employee is used at no cost or risk to the Institution and is maintained by the employee. In general, employees are responsible for operating costs, home or building maintenance, or any other incidental cost (e.g. utilities) associated with a remote location. Exceptions require upfront approval by the appropriate manager.

Permissions to access Carnegie Institution Headquarters computers remotely and related security incidents should be reviewed periodically by supervisors and IS staff members. The systems administrator shall record the reviews in the Help Desk system and correct all problems if necessary.

Wireless Access

The design of wireless networks, specifically the placement of wireless access points to maximize coverage area and to minimize interference with other access points or devices and to ensure network security, requires coordination. Information systems staff are responsible for the operation and management of the wireless network infrastructure.

Access to the Carnegie Institution networks via unsecured wireless communication mechanisms is generally prohibited. All wireless Access Points / Base Stations connected to the institutional network must be registered, approved, and managed by members of the information systems staff.

Wireless network access requires the registration and the validation of the client system before granting unrestricted access to the Institution's internal network.

Search for rogue wireless stations should be conducted on a regular basis and related security incidents should be reviewed periodically by IS staff members. The systems administrator shall record the reviews in the Help Desk system and correct all problems if necessary.

Third-Party Access

All third parties requesting access to the Institution's network are required to obtain specific approval from an information systems staff member. All remote third party connections to any system located on any Carnegie Institution network will use Carnegie approved methods and applications for network connectivity.

Third-parties should be given only in-bound connection privileges, when possible, and when they have a legitimate business need. These privileges must be enabled only for the time period required to accomplish previously-defined and approved tasks.

As a condition of gaining access to the Carnegie Institution computer network, each third party must secure its own connected systems in a manner consistent with Carnegie Institution requirements.

Security incidents related to third-party access should be reviewed periodically by IS staff members. The systems administrator shall record the reviews in the Help Desk system and correct all problems if necessary.

Email

Email Accounts

Electronic Mail is a primary means of communication in support of the Institution's mission of research, education and public service. Carnegie should facilitate the widespread use of email by providing email services to eligible personnel. The principal email domain name for Headquarters employees is "ciw.edu." All Headquarters employees must have an official Carnegie email address that ends in @ciw.edu. The Institution sends much of its correspondence solely through email. This includes policy announcements, emergency notices, meeting and event notifications, and official correspondence between staff. Such correspondence will be mailed only to the official Carnegie email address. Staff must use their @ciw.edu emails in official communications and publications. They can forward email from their official email address to another email address if they so choose. However, they are responsible for managing both the Carnegie account and the account to which the email is forwarded to so as to ensure that all official Carnegie correspondence continues to be delivered. Email lost, or secure, confidential or private information compromised because of forwarding does not modify the responsibilities associated with communications sent to the official email address. The Carnegie Institution is not responsible for email handled by non-Carnegie servers.

Email is a mission-critical service and is expected to be available 24/7 with the exception of scheduled maintenance.

Only Carnegie employees and other eligible persons who receive permission under the appropriate Carnegie authority are authorized users of the Institution's electronic mail systems and resources.

Electronic mail accounts, like user IDs, must be uniquely associated with specific individuals and must not be shared. No generic email accounts will be issued. For cases when the underlying person can change in a role while the role remains the same, users can request the creation of email aliases. Delivery of emails to multiple recipients will be handled via email lists.

If users are unable to check their mail for extended periods, mail can be forwarded to another Carnegie Institution employee for business purposes.

In general, upon departure from Carnegie, a user's institutional electronic mail account should be terminated. Routine exceptions to this approach include staff who will continue to do consulting work at the institution as well as a transition period. These and other exceptions will be documented by the IS staff.

All information acquired from the emails and the Internet can be considered suspect until confirmed by separate information from another source. Users should not rely on the alleged identity of a correspondent unless the identity of this person is confirmed through methods such as digital certificates or digital signatures.

Carnegie records retention policies do not distinguish among media with regard to the definition of Carnegie records. As such, electronic mail records are subject to these policies. There is no single retention period for e-mail messages. The value of e-mail messages is based upon their informational content and function.

The Institution currently does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail will normally be backed up to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally.

Email users should be aware that generally it is not possible to assure the preservation of all electronic mail records for record-keeping purposes. Email users and those in possession of Carnegie Institution records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring electronic mail to a more lasting medium/format. E-mail records must be maintained in a usable format throughout the approved retention period. If the record is to be maintained in an electronic format, it must be migrated to new software and storage media as upgrades occur. If the e-mail record is printed out and retained in paper form, all envelope information must be printed and retained with the

Return to Index

record.

Email addresses that are issued by the Carnegie Institution to employees or others affiliated with Carnegie are generally considered to be public information and as such, may be made available in electronic or paper directories, and may be released upon request in accordance with applicable policies and laws.

All employees should follow a few simple rules regarding Carnegie's e-mail systems described in the "Guide for Appropriate Use of Email" document.

The privilege of initial and continued eligibility to use email addresses by all persons requires initial and periodic verification by the systems administrator that the access is for purposes that support the operations or mission of the institution. The system administrator shall conduct periodic eligibility reviews, record the results in the Help Desk system and correct all problems if necessary.

Email Aliases

Carnegie will issue email aliases based upon availability of the alias requested. An email alias should not conflict with a current or potential normal email address. It should be as descriptive as possible of the role, person, unit or organization making the request. Using email lists is the recommended method to define mailing lists which include multiple recipients, however, aliases can be also used for this purpose.

The system administrator shall conduct regular reviews of email aliases, remove aliases that are no longer in use and those pointing to expired email addresses. The systems administrator shall record the results of these reviews in the Help Desk system and will establish proper controls to prevent future problems if necessary.

Email Lists

Mailing lists may be used for legitimate purposes related to research, administration, and Institution approved social activities.

The Carnegie Institution generally supports opt-in email lists. Occasionally, opt-in lists are not appropriate, such as the construction of lists to distribute business and emergency information. The Institution should avoid renting email lists, and avoid participation in cooperative email databases unless users have specifically authorized them to share data in this manner.

The first email message from a list should be an acknowledgment restating the user's subscription to the list.

Messages distributed via email lists must always include clear instructions on how to unsubscribe. A human should monitor and respond promptly to email inquiries and requests. At a minimum, account "abuse" should be monitored.

The system administrator shall conduct regular reviews of business related lists and synchronize list memberships with roles and responsibilities related to official Carnegie personnel data. The systems administrator shall record the results of these reviews in the Help Desk system and will establish proper controls to prevent future problems if necessary.

Additional responsibilities for mailing lists are shared by three parties, the mailing list manager, the sponsor, and information systems staff and are described in the "Email list manager and owner responsibilities" guide.

Systems Support

Help Desk

Information systems staff provide day-to-day operational support, advice and guidance to users through the Help Desk function. It is also being used to communicate and promote IS services, manage and control service communications to users, coordinate incident management activities, manage people, processes and technologies that form the support infrastructure, and provide management information about general support quality and operations.

Return to Index

Information systems problems and requests and their resolutions will be logged into Help Desk software for tracking and reporting purposes.

IS staff will maintain the Help Desk, monitor and report trends, and be responsible for establishing service levels, escalation criteria and procedures.

All logged problems and requests will be addressed in order of priority.

All requests will be allocated to an IS staff member for action.

All requests will be attended to and resolved as soon as possible.

To ensure long term success of Help Desk functions, IS staff will conduct satisfaction surveys, and will seek to respond within established service level targets.

The systems administrator will periodically review incidents that are not resolved within an acceptable period. The systems administrator shall record the results of these reviews in the Help Desk system and will adjust procedures to improve the Help Desk function, if necessary.

Data Backup, Storage and Retrieval

Carnegie Headquarters backs up all networked resources daily but it is the user's responsibility to periodically review whether his or her data are being backed up. The frequency and extent of backups should be in accordance with the importance of the information and the acceptable risk, as determined by the user and the information systems staff, and consistent with best practices and any legal requirements.

Data retention periods should be in accordance with the importance of the information and the acceptable risk as determined by the data owner, information systems staff, information systems best practices and legal requirements.

If a staff member needs to recover a deleted or changed file(s), he or she should contact the Help Desk. Unless otherwise directed, systems staff will seek to restore the file(s) from the most recent set of applicable backups that include them to a restore location.

All Carnegie Institution employees, including contractors and vendors with access to Carnegie Institution backup data, are responsible for taking the appropriate steps to maintain the integrity of the Carnegie Institution's backup data.

Adequate physical access controls should be implemented at all off-site backup storage locations.

Tapes and other backup media will be stored in approved, industry-standard fire-and waterproof media safes. Backups must be periodically tested to ensure that they are recoverable.

To ensure long-term continual access to digital materials when required hardware, software, and other technologies evolve over time, a systematic data migration plan should be designed.

Following this plan, the Carnegie Institution will move data from any storage media, data format and associated hardware and/or software that are becoming obsolete to new media, format, hardware, and/or software that are or are becoming standard or currently considered best practice.

The Carnegie Institution will keep its data server infrastructure (hardware, software, etc.) up to date and perform periodic updates and upgrades.

The backup and recovery process for each system should be sufficiently documented and periodically reviewed by the systems administrator. The systems administrator shall record the results of these reviews in the Help Desk system and will adjust backup procedures to improve the backup and restore function if necessary.

Purchasing, Recycling, Retiring and Disposal

Acquisition of Information Systems Resources

The acquisition of information systems equipment and services is governed by the overall procurement policy (see G. Procurement), as well as any special requirements related to grants and contracts. All systems requisition requests should be submitted to the systems administrator. All major systems purchases should be planned and budgeted for, see “Budgeting” and “Capacity Planning” policies for more information.

Software and Architecture

Software used throughout Headquarters, such as operating systems or office application software packages, should be purchased and managed as part of a centralized software asset management program. In general, the diversity of operating systems and software in use will be determined by the needs of the individual units. All units should attempt to minimize the diversity of operating systems and software packages the IS staff will have to support. Software in use should be supported with vendor- or developer-supplied security patches and updates which meet security policy requirements. Carnegie employees interested in software and operating system purchases or upgrades should seek advice on selection and configuration from IS staff prior to submitting a requisition request.

Site Licenses

As required, existing and future site licenses that can reasonably be identified shall be included in annual systems budget submissions to permit appropriate bulk discounts. Carnegie will generally favor the selection of stable, multi-platform software of wide utility that is in use at multiple groups, runs on shared resources, including equipment managed by information systems staff, or on individual machines if the software is necessary for special purposes. Software purchased will be subject to periodic review by IS staff to determine its usage and value.

Hardware

Carnegie’s priority in making decisions about hardware is to select equipment that will maximize productivity and meet the needs of its employees. Staff should strive to minimize, where feasible, the diversity of computers, printers, and other devices that the IS staff will have to support. Selections should take into account the total cost for the entire lifecycle of the item, the reputation of vendor, the terms of the warranty, and architectures already in service. Limiting the diversity of devices to one or two different types in each hardware category greatly reduces the complexity of support needs. New equipment should be purchased with adequate warranty service. Non-standard, customized features of any hardware should be well documented in order to reduce operational risks.

Infrastructure

The infrastructure put in place at Headquarters should meet the needs of Carnegie employees, enable information sharing inside and across the department and outside the Institution, guarantee and enhance the Institution's ability to deliver secure, effective, efficient and timely services to employees, promote interoperability, improve the conditions for administrative work, and where appropriate promote migration to solutions with reduced complexity and support costs. Relying on widely accepted standards and limiting the complexity of the infrastructure greatly reduces support needs. Non-standard, customized features of the IS infrastructure should be well documented in order to reduce operational risks.

Inventory Control

The Systems Administrator must maintain an inventory of information systems assets detailing all existing hardware, software, and communications links. This list will help Headquarters properly plan for emergencies and disasters, will be useful to negotiate volume purchase agreements with vendors, and will be helpful for controlling information security activities. The existence of an asset inventory will also help in efforts to identify and control stolen and lost equipment, and will help with contingency planning efforts, equipment upgrade efforts, and missing equipment insurance reimbursement efforts.

Recycling, Retiring and Disposal of Information Systems Assets

The process for retiring and disposal of information systems equipment is governed by the overall equipment policy (see A. Accounting and Financial Management), as well as any special requirements related to grants and contracts.

Computer Data and Media Disposal Policy

In order to eliminate accidental or innocent destruction of data, computer data and media disposal processes have to comply with Carnegie's "Record Retention Policy." Users shall not knowingly destroy data with the intent to obstruct or influence an investigation or proper administration of any matter or in relation to or contemplation of such matter or case.

Carnegie-owned computer and digital storage media must have all institutional data and licensed software reliably erased from the device prior to its transfer out of Carnegie control, and/or the media must be destroyed, using current best practices for the type of media.

All computer and digital storage media leaving Carnegie's possession and/or control while still intact must be transferred in accordance with the Carnegie Institution overall equipment policy.

Data on computers and digital storage media, which are included as part of a trade-in purchase, must be erased and identified on the purchase order for new equipment.

The "Guide for Secure Removal of Data" contains useful information about removing confidential information from media.

Computer Equipment Replacement Policy

Replacement Cycle

The CIO will determine an appropriate average replacement cycle for Headquarters owned computers in primary placement locations. Primary placement locations include Carnegie managed servers and systems specifically designated to individual staff.

Computer equipment located in secondary placement locations, such as the library, public areas, assigned to visitors, etc., will be replaced with suitable recycled systems as they become available.

Computer equipment originally acquired through grant funding will be replaced with suitable recycled systems and treated as secondary placement equipment if additional grant money or funding is not available to replace it with new equipment.

New Computer Hardware Expansion Guidelines

Requests to add new computing equipment to our existing inventory that are not being funded through grants or external funds must be submitted to the systems administrator by the supervisor. The requests will be reviewed as part of the regular budgeting cycle. Funding will be sought for requests that pass this review. Requests to add new computing equipment to our existing inventory that are being funded through grants or external funds must be also submitted to the systems administrator for review. This review will ensure that the proposed equipment will be compatible with the existing Headquarters infrastructure and architecture, and that the proposed solution will not increase systems complexity and support costs in an uncontrolled fashion.

Replacement Equipment Guidelines

In an effort to improve support and keep costs down, Carnegie selects computer configurations and models that will meet the computing needs of the average user for the term of the replacement cycle. Carnegie will upgrade components of the system as appropriate to keep it at a reasonable level of functionality for the term of the replacement cycle.

The selected system should allow the user to fulfill his job related responsibilities, create word processing documents, spreadsheets, simple multimedia presentations, and web pages, as well as check e-mail and access information on the Internet in a reasonably efficient fashion.

Security

Protection against Viruses, Malicious Software, Hoaxes, and Spam

In general, this policy applies to all computers connected to Headquarters networks. These include, but are not limited to, desktop computers, portable devices, laptop computers, and servers. Alternative protection approaches may be developed for other equipment where necessary so that there is no negative impact on performance.

The most current versions of virus, worm, spyware and other malicious software checking software approved by information systems staff must be running on all computers with operating systems susceptible to viruses, including personal computers, servers, and firewalls with external network connections. Anti-virus software and other signature files must be kept up-to-date, and distributed centrally. Real-time protection must be enabled, and users must not turn off or disable virus-checking systems.

All files coming from external sources must be checked before execution or usage. If encryption or data compression has been used, these processes must be reversed before the virus-checking process takes place. Employees should never open or forward any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Employees should delete such files together with spam, chain, and other junk email without forwarding.

All files containing software or executable statements must be certified as virus free prior to being sent to any third party.

All incoming and outgoing electronic mail must be checked for viruses, spyware, and other malicious software on Carnegie Institution mail servers.

Systems without the required software patches or systems that are virus-infested must be disconnected from the network until they are verified as virus and malicious code free and their patches are up-to-date. If a virus or malicious software is detected, or if users obtain virus or similar alerts, they must immediately follow the procedures described in the "Reporting Information Security Incidents Policy" document.

Any activities with the intention to create and/or distribute malicious programs into Carnegie Institution's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, spyware, etc.) are prohibited.

Users must not install new or upgrade operating systems or application software on personal computers or other machines used to process Carnegie Institution business information. This approach permits Carnegie Institution to perform automatic software distribution, automatic software license management, automated remote backup and related functions on a centralized and coordinated basis.

Software resident on the Internet should not be downloaded to any Carnegie Institution computer processing, storing and/or accessing administrative and financial data unless it is received directly from a known and trusted source or software verification tools, like digital signatures, are employed.

Before any files are restored to a Carnegie Institution computer system from backup storage media, these files must have been scanned with the latest version of virus screening software.

Hoaxes are commonly e-mails purporting to warn users about a potential flaw or virus just discovered. They also include chain letters promising financial rewards, and pyramid schemes. We ask that users deal with hoax e-mails individually. If you have received a security or virus warning, and are unable to determine its authenticity, you should ask the Help Desk to review it.

Carnegie will continuously explore systems that can block spam without disrupting legitimate use of Carnegie systems. Despite our best efforts, spam emails may reach accounts. Employees should either simply delete the message or report it to the correct authorities. When reporting spam, the employee must include the full headers of the spam received. If employees receive spam that appears to come from a valid Carnegie account, it should be reported to the Help Desk. If employees receive email that makes them feel personally threatened, the local police department should be contacted.

Information systems staff members are available to provide consultation and advice related to viruses, spyware, email use or misuse, spam and hoaxes.

Systems Vulnerability Scanning

Any equipment attached to the Carnegie Headquarters network is subject to security vulnerability scans. Systems that are not properly managed can become a potential threat to the health and well-being of Carnegie systems and networks, and will be disconnected. Systems on the Headquarters network will be subject to frequent, in-depth security scans since they carry a particular risk and are essential to the smooth functioning of the Institution.

The system administrator shall conduct regular reviews of security vulnerability scan outputs. The systems administrator shall record the results of these reviews in the Help Desk system. He will make the necessary steps to correct the problems and establish proper controls to prevent future problems if necessary.

Reporting Information Security Incidents

If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its owner and the Information Systems staff must be notified immediately.

Specific information about information system vulnerabilities, such as the details of a recent system break-in, must not be distributed to persons who do not have a demonstrable need to know.

All significant errors, incomplete processing and improper processing of business applications must be promptly reported to the Help Desk. Depending on the incident and system, additional reporting may be required.

All unusual and suspicious information-security-related events, all information security alerts, warnings, suspected vulnerabilities, and the like, and all security-related incidents should be reported immediately to the information systems staff. The information systems staff is responsible for following up on all reports of security-related incidents. The response will depend on the nature of the incident.

If an information systems security breach, a verifiable information systems security problem, or a suspected but likely information security problem at the Carnegie Institution causes private, proprietary or private third party information to be exposed, then these same third parties must be notified immediately so that they can take appropriate action. In order to prevent such problems, private, confidential, proprietary or private third party information should not be sent in unencrypted email messages, put on public websites or file servers, or stored without appropriate access controls.

A written log should be kept for all security incidents that are under investigation. The document should contain the dates and times of incident-related communications, when incident-related events were discovered or occurred, the amount of time spent working on incident-related tasks, people you have contacted or who have contacted you, and the data, names of systems, programs or networks that have been affected.

The follow-up investigation must provide sufficient information so that management can take steps to ensure that such incidents will not be likely to take place again, and effective security measures have been reestablished.

Privacy and Legal Policies

Privacy and Confidentiality of Electronic Information and Information Systems Resources

In general, electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of the Carnegie Institution are the property of the Institution. Electronic files created, sent, received, or stored on Headquarters Information Systems resources owned, leased, administered, or otherwise under the custody and control of the Carnegie Institution are not private and may be accessed if necessary by Carnegie Institution employees at any time without the express consent or knowledge of the information resource User or Owner.

In general, personal information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals. Carnegie will assume that computer users wish the information they store on central and shared computing resources to remain confidential. Carnegie will try to maintain the confidentiality of all information stored its computing resources.

Return to Index

Similarly, privileged information on account usage (i.e., that available only to users with system privileges) will be held in confidence.

However, users should also be aware that their uses of Carnegie computing resources are not private. While Carnegie does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the computing resources require the backup of data and communication records, the logging of activity, the monitoring of general usage patterns, and other such activities. Carnegie may also inspect files or monitor usage when there is reason to believe a user has violated its policies. In addition, a supervisor may find it necessary to retrieve a file of assigned work by inspection without notice when an employee is unavailable for timely consultation.

Requests for disclosure of confidential information will be reviewed by the administrator of the computer system involved. Such requests will be honored only when approved by Carnegie officials, or when required by state or federal law. Except when inappropriate, computer users will receive prior notice of such disclosures.

Employees must safeguard the privacy and security of third party information that was entrusted to the Carnegie Institution. Access to personally identifiable data should be limited based on business need for such access. Personal information must not be distributed to third parties without advance authorization.

Carnegie systems administrators may remove from central resources any information that is inappropriate, as defined above. Users whose information is removed will be notified of the removal as soon as is feasible.

Privacy policies governing the treatment of visitors to Carnegie's websites are available at <http://www.ciw.edu/>.

The systems administrator shall record all requests for private, confidential data in the Help Desk system except when inappropriate.

Software Copyrights Policy

Only legally licensed software is permitted to be installed on Carnegie Institution computers, and only installed on the number of computers permitted under the license.

Reproducing computer software without authorization violates the U.S. Copyright Law. Therefore, users must not make copies of or use software unless they know that the copies are in keeping with the vendor's license to the Carnegie Institution.

The Carnegie Institution purchases or licenses the use of copies of computer software from a variety of outside companies. The Carnegie Institution does not own the copyright to this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer.

With regard to use on local area networks or on multiple machines, employees may use the software only in accordance with the license agreement.

Any misuse of software or related documentation within Headquarters should be reported.

Information Systems staff should regularly review and maintain documentation reflecting all software licenses. Questions about licensing should be directed to Information Systems staff.

Information Systems staff should ensure that users are properly following the license terms.

Making regular backups of software for contingency planning purposes is permissible.

Licensing information and media that contain the software should be maintained by Information Systems staff. Copies of licensing terms and all related software documentation should be provided to users if requested.

The system administrator shall conduct regular reviews of licensed software usage for licensing violations and make recommendations for adjustments and efficient use of resources. The systems administrator shall record the results of these reviews in the Help Desk system and will establish proper controls to prevent future problems when necessary.

General IS Policies

Information Systems Governance

Corporate Governance

Carnegie manages its information systems within the overall governance structure of the Institution, including its Board of Trustees, President, and Chief Information Officer. This document includes specific roles and responsibilities for these and other officials as related to information systems activities.

Headquarters Information Systems Planning Council

The Headquarters Information Systems Planning Council ensures that IS governance is adequately addressed at Carnegie's Headquarters; advises on strategic direction; and reviews major investments. Members participate in strategic planning and assist with resolving information systems budgeting conflicts. Members of the IS strategy committee are the the Director of Administration and Finance, the Chief Advancement Officer, the Chief Information Officer, and a co-director of CASE. The CIO will serve as the secretary to the council. The council chair is selected from the remaining members and rotated on an annual basis.

The Information Systems Planning Council shall make recommendations to the President on the prioritization of information systems investment programs in line with Carnegie's Headquarters strategy, policies and priorities. The council tracks the status of major projects; measures progress; resolves resource conflicts; and monitors service levels and service improvements. Members recommend information systems policies, procedures and standards; and participate in information systems budgeting, operational and tactical planning.

Strategic Planning

IS strategic planning is required to manage and direct all IS resources in line with Carnegie's strategy and priorities. Both systems and administrative unit stakeholders are responsible for ensuring that optimal value is realized from project and service portfolios. The strategic plan will describe and assess IS opportunities and limitations, assess current performance, identify capacity and human resource requirements, and clarify the level of investment required. The plan is subject to review and approval by the President.

IS Organizational Structure and Responsibilities

The Headquarters Information Systems group, headed by the CIO, is responsible for the development, maintenance, and support of Headquarters' key administrative applications, and the management, operation and security of the Carnegie's enterprise servers and network infrastructure. The group provides services in systems planning, budgeting and purchasing, security, programming, database and WWW administration and development, business and process analysis, user training and education. The unit is also responsible for providing technical support, and help desk services for all Headquarters operating units.

Policies, Procedures, Standards and Guidelines

All Headquarters information systems policy and procedure documents shall be reviewed by members of the Headquarters Information Systems Planning Council and submitted for final approval to the President. Approved documents will be published and communicated to employees, and relevant external parties as appropriate. Information systems policies and procedures should be reviewed at planned intervals, not less than two years.

Lifecycle Management

Budgeting

All Headquarters units should submit an annual equipment and service request to the systems administrator as part of the annual budgeting cycle (see general Budget policy). IS staff must prepare an annual budget that reflects the needs and priorities established by Headquarters' units, and includes the ongoing costs of operating and maintaining the current infrastructure. The overall Headquarters' IS budget includes items for all individual administrative units programs, with specific emphasis on the IS components. The President approves the systems budget, with any necessary changes.

Capacity Planning

Users are responsible for providing information about their anticipated needs to the systems administrator as part of the annual budgeting cycle, and giving regular feedback to information systems staff about the quality of service they receive.

IS staff should ensure that personnel and infrastructure capacity levels support established and expected service level targets; ensure that sufficient capacity levels are provided for at the individual IS asset level; and finally ensure that appropriate levels of capacity are built into new IS solutions and proposals.

Headquarters should perform ongoing monitoring and analysis of current performance levels to guarantee that appropriate levels of capacity are provided and that resources are optimally utilized. Information system planning should also take into account compliance with fiscal, security and privacy requirements and other regulations; staffing, space and utilities requirements; and continuity and contingency plans.

Service Support

Incident Management

Carnegie Information Systems staff should restore normal operations as quickly as possible with the least possible impact on either the institution or the user, at a cost-effective price.

All incidents should be reported to and managed via the Help Desk system. A resolution or work-around should be established as quickly as possible in order to restore the service for all incidents that cannot be resolved quickly.

Information systems staff should conduct satisfaction surveys on a periodic basis, and should resolve incidents within service targets.

Problem Management

Carnegie Information Systems staff should try to find and resolve the root cause of incidents and thus minimize the adverse impact of incidents and problems that are caused by errors within the IS infrastructure, and to prevent recurrence of incidents related to these errors.

Incidents that do not cause immediate hazardous effects but repeat over a long period of time should be monitored and resolved using established change management processes.

Change and Release Management

In general, information systems staff should establish internal processes designed to provide an orderly method in which changes to their essential information systems components are requested, approved, and installed. These include changes to the hardware, software, service level, or applications. This process may also include modifications, additions or changes to the infrastructure, LAN/WAN, network or server hardware and software.

Return to Index

Typically these proposals are submitted through a request tracking system or the departmental Help Desk, although major proposed changes may be supplemented with additional material. Stakeholders should be informed of major proposed changes or releases.

Before new major releases, and any change to a production system, servers or a baseline, the proposed change should be evaluated, approved, tested, released and documented using the Help Desk system.

Changes to administrative, and financial packages will not be released into production until they have been tested and signed off by a member of the IS team other than the one implementing the change and the system owner.

Major change and release implementations should be authorized and follow established change and release management procedures, and utilize only documented, standard or licensed components.

Following resolution of a change request or a new release, notification should be sent to all affected users after the issue is resolved.

Patch Management Policy

Software installed on all networked devices belonging to or managed by Carnegie Headquarters will be patched with vendor provided security patches.

These patches will be applied as soon as possible following appropriate testing of the security patches by Carnegie staff, or other affiliated and partner organizations. Carnegie policies do allow the automatic installation of security related vendor patches on production systems without prior testing.

New systems must be patched to the current patch level, as defined by the system vendor.

Current patch status will be documented to the extent it is practical. Steps will be taken for devices that cannot be patched to mitigate the risk and to protect a device from a particular vulnerability.

Service Delivery

Domain Names

In general, all hosts on the Headquarters' networks should have a name that ends in ciw.edu. The principal domain name for the Carnegie Institution Headquarters is "ciw.edu." All services that are provided by members of the Carnegie Institution Headquarters as part of their official functions and as part of the mission of the institution will be registered within the ciw.edu domain.

In general, all services that are provided by either members or nonmembers of the Carnegie Institution Headquarters community, but that are not part of their official functions as members of the community or as part of the mission of the institution, must be registered outside the ciw.edu domain.

Existing hostnames or subdomains of the Carnegie Institution Headquarters that do not conform to this policy will be reviewed prior to any change, including considering of "grandfathered" status if that is most appropriate.

Headquarters Domain Name System (DNS) Standards Within the ciw.edu Domain

The format of DNS service entries is "hostname.unit.ciw.edu," where:

The naming structure is intended to follow the organizational affiliation.

Unit subdomains in the ciw.edu domain should be the names of departments, or certain organizational units that are officially recognized by the Institution.

The unit responsible for the computer may select the hostname component of the domain name.

Return to Index

The hostname component of the domain name may reflect generally accepted practices, used by the Internet-at-large and provided by sites internationally, including www and ftp. For example, the "www" in www.hq.ciw.edu.

The hostname component of the domain name may reflect the name of the service program or may follow a naming scheme within the unit. For example, the "gateway" in gateway.case.ciw.edu.

Exceptions for 'hostnames' or 'department' names within the ciw.edu domain will be allowed after consideration of various factors, such as:

The proposed name is for a group of different organizations.

The proposed name is the name of a service or service unit, center, or institute and not the name of a department or other organizational unit.

The proposed name is for an institution-wide service that is not easily identified with a single department or unit, or it is for a service that is being offered primarily to people or groups that are outside Carnegie and who are not likely to be familiar with the details of Carnegie's internal organizational structure.

The proposed name is not now, and is not likely to become, ambiguous if it is used as a hostname without other department or unit qualification.

The proposed name is not likely to change.

The placement of the proposed name as a hostname within ciw.edu has the explicit approval of the Chief Information Officer and the supervisor of the unit with which the name would otherwise be associated.

Headquarters DNS Standards Outside the ciw.edu Domain

Domain names outside ciw.edu may be allowed and may be required after consideration of criteria such as:

The proposed name should have either primary or secondary name service provided by ciw.edu hosts.

The proposed name will be used by many people from many different organizations outside the Institution.

The proposed name is not likely to be confused with the name of a Carnegie department or unit.

The proposed name signifies an organization or venture, commercial or noncommercial that is not explicitly part of Carnegie.

The proposed name is for a project with external funding.

The placement of the proposed name outside the ciw.edu has the approval of the Chief Information Officer, and the director of the department, center, institute, or equivalent unit to which the name would otherwise be associated.

WWW Policy

Contents of all Web pages under the jurisdiction of the Carnegie Institution's Headquarters (i.e., hosted by Carnegie servers or by other servers funded by Carnegie budgets, or managed by either members or nonmembers of the Carnegie Institution Headquarters community as part of the official Carnegie function) must comply with local, state and federal laws and with Carnegie's policies, rules, and regulations. Further, the reputation and image of the Carnegie Institution is determined, in part, by the quality of information published electronically by its staff, and affiliations.

All pages that reside on, or are linked from, CIW web sites should consider layout guidelines. These have been formulated to make the information viewable by as large an audience as possible, to make intra-site and inter-departmental navigation clear to web visitors, to provide contact information, and to encourage the use of the Carnegie logo. When developing new or revised web sites, Carnegie Headquarters units should strive to provide navigation that is consistent with the www.ciw.edu home page and subpages.

CIW web pages may not contain advertising for, or link to, commercial sites. Approval will be considered only if the

purpose of the advertising or link is consistent with the Institution's mission, the advertising or link is essential to the purpose of the site, and the advertising or link does not imply Carnegie endorsement of the product or service.

Non-Carnegie-related fundraising may not be conducted on any Web page - Carnegie mission related or personal - that is operated and administered by the Institution or is hosted on the Institution's network.

Information on Carnegie web sites is subject to intellectual property law. Except as permitted by law, written permission is required from the owner of copyrighted material (including graphics, video, audio, and text) before copyrighted information can be placed on any Carnegie web site.

All web servers associated with Carnegie Headquarters must be registered with information systems.

All web service providers are responsible for the currency, legitimacy, legality, and appearance of their pages. Web service providers must adhere to Carnegie's Web policies and are responsible not only for the content and appearance of their own pages but for those linked personal pages which branch from their pages.

Information Security

Information Classification and Handling

The Headquarters of the Carnegie Institution makes available to the general public a broad range of scientific and business data. If an employee has any question about whether certain information should be publicly available, he/she should consult with a supervisor and/or an official responsible for the function.

As a general rule, information that is not routinely made available to the public should be treated as being available for internal use. The distribution of, and access to, internal information is generally determined by the organization/unit responsible for the function.

The owner or creator of information used internally has responsibility to designate any appropriate labels, and the user or recipient of this information must consistently maintain such treatment. For example, a document intended only for another specific individual should be labeled as 'confidential' or 'eyes only.' Labels for sensitive information should be used in the subject field of electronic mail messages. Labels for sensitive information should also appear on the outside of disks, magnetic backup tapes, DVD-ROMs, audio cassettes, and other storage media. Owners may also designate additional controls to further restrict access to, or to further protect their information. All users must observe the requirements for handling information based on its sensitivity.

Financial Data

Financial data are managed within a framework of established rules and standards for financial management and reporting. In general, data are made available to employees in order that they may perform their responsibilities. Certain other information, such as annual audited financial statements and tax returns are made available to the public.

Access to the Agency's official accounting system and records is strictly controlled through a series of system and operational procedures. The Financial Manager, in conjunction with the Chief Information Officer, approves all requests for direct access to the information. The rights and authorities of individuals with respect to this information (e.g., read only/data entry/approval; modules) are determined by the Financial Manager.

Employee Data

Carnegie collects and maintains various data concerning employees in order to carry out a range of business related responsibilities and to comply with statutory and regulatory requirements, including tax laws. In general, employees themselves are the source of this information. Within Headquarters, access to employee-specific data is restricted to those having work responsibilities that necessitate such access, such as the Human Resources Manager, human resources staff, payroll staff, and certain accounting and financial management staff. All individuals with access to such information are required to treat it in a manner that protects the employee and is in compliance with applicable laws and regulations.

Carnegie occasionally receives requests from outside entities regarding employee data. These requests range from verifying

Return to Index

employment from loan companies to gathering statistical information about salaries by category of employment. Before responding to such requests, individuals within the organization are expected to consult with knowledgeable officials within the Human Resources office.

Access to the Institution's official records concerning employees, including any systems that exist for this purpose, is controlled by the Human Resources Manager.

Carnegie Institution personnel are encouraged to use common sense judgment in securing Carnegie Institution information to the proper extent. If employees are uncertain of the sensitivity of a particular piece of information, they should contact their manager.

Classification Categories

Insufficient security measures may allow resources to be damaged or stolen, or create a liability to the Institution. As a result appropriate security measures and procedures, commensurate with the identified level of acceptable risk, should be developed that define how to protect information at varying sensitivity levels. The categories below constitute a reference only, as it may be necessary to apply more or fewer measures of protection depending upon the circumstances and the nature of the information in question. Owners may also designate additional controls to further restrict access to, or to further protect their information. These categories may include Logical Access, Physical Access, Right to Grant Access, Types of Distribution within the Carnegie Institution, Types of Distribution outside of the Carnegie Institution, Electronic Distribution Protection, Storage Protection and Restrictions, Copying Restrictions, Faxing Restrictions, Procedures for Disposal/Destruction, Conditions for Release to Third Parties - Non-Disclosure Agreement, Labeling Requirements, Electronic Media Labeling Requirements, Hardcopy Labeling Requirements, Internal and External Mail Packaging Restrictions, Tracking Process by Log, and Penalty for deliberate or inadvertent disclosure. All users must observe the requirements for handling information based on its sensitivity.

Information Security Awareness and Training Policy

The Headquarters of the Carnegie Institution must develop, implement, and regularly review a formal, documented program for providing security training, education and awareness for all users who have access to its information systems. Users must understand how to protect the confidentiality, integrity, and availability of information systems.

In cooperation with the Director of Administration and Finance, the Chief Advancement Officer, and the director of CASE, the Chief Information Officer is responsible for managing the training and awareness program and for consulting with Headquarters employees on information security issues. This training shall include, but is not limited to security policies, procedures and standards and/or significant revisions to them; the secure use of systems; Carnegie's legal and business responsibilities for protecting its information systems and data; and security best practices.

The CIO is responsible for making information security policies and procedures readily available for reference and review by appropriate users.

Managers are responsible for seeing that their employees take advantage of available security awareness resources.

Users are responsible for becoming familiar with standard information security principles and procedures as they apply to the information resources under their care.

Information Security Roles and Responsibilities

Owners

Managers at Headquarters may have responsibility for information that is systematically gathered and maintained for the scientific and/or business activities of the institution. In general, such individuals will be known as the 'Owner' of the information. Information Owners do not legally own the information. They are instead members of the Carnegie Institution who make decisions on behalf of the organization. Information Owners should designate a back-up person to act if they are absent or unavailable.

Managers

An employee's immediate manager should approve a request for system access based on existing job responsibilities. When an employee leaves the Carnegie Institution, it is the responsibility of the employee's immediate manager to promptly inform the Information Systems department that the privileges associated with the employee's user ID must be revoked and/or retained in accordance with the policy described earlier. Shortly after separation from the Carnegie Institution, a manager is additionally responsible for reassigning the involved duties and files to other employees.

Custodians

In many instances the owner of an information system will rely on technical staff to support operations. These individuals, known as Custodians, are in physical or logical possession of information and information systems. Like Owners, Custodians are specifically designated for different types of information. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners. Custodians define the technical options, and information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to best meet business objectives. If requested, Custodians additionally provide reports to Owners about information system operations and information security problems. Custodians are responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.

Users

Users are defined as any employee with access to internal information or internal information systems. Users are required to follow all security requirements defined by Owners or established by the Information Systems department. Users also must participate in any information security training and awareness efforts. Users must request access from their immediate manager, and have responsibility to report any suspicious activity and potential security problems. Users should become knowledgeable about relevant security requirements and guidelines, and must protect the resources under their control, such as access passwords, computers, and data they download.

Information Systems Staff

Information systems staff should be contacted regarding systems security matters at the Carnegie Institution. Users will use their judgment in informing the responsible systems administrator. Systems staff help implement security standards, procedures, policies, and other requirements applicable to the organization. Specifically, Information Systems staff must oversee all access control administration activities, monitor the security of Carnegie Institution information systems, and assure information security training and awareness programs to Carnegie Institution employees. IS staff members are responsible for periodically providing management with reports about the current state of information security at the Carnegie Institution. While information systems contingency planning is the responsibility of information Custodians, information systems staff also provide technical consulting assistance related to emergency response procedures and disaster recovery. Information systems staff members are also responsible for promptly responding to virus infections, hacker break-ins, system outages, and similar information security problems.

It is the information systems staff's responsibility to create workable information security solutions that take into consideration the needs of Users, Custodians, and Owners.

It is the further responsibility of information systems staff and Custodians to

1. become knowledgeable regarding relevant security requirements and guidelines;
2. analyze potential threats and the feasibility of various security measures in order to provide recommendations to Owners and Managers;
3. implement security measures that mitigate threats, consistent with the level of acceptable risk established by Owners and Managers;
4. establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
5. establish procedures to implement relevant provisions of applicable laws and regulations for systems in support of the Institution's business administration; and

6. communicate the purpose and appropriate use for the resources under their control.

Risk Assessment and Treatment

The periodic identification and assessment of risk exposure is necessary to ensure that policies, procedures, standards and controls are effective.

Risk assessments can be conducted on any entity within Carnegie Headquarters or any outside entity that has signed a Third Party Agreement with the Carnegie Institution and is responsible for maintaining Carnegie Institution assets. Risk assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained with the goal to determine those factors that could affect confidentiality, availability, and integrity of Carnegie Institution's key information assets and systems.

Responsibility: The CIO is responsible for the periodic assessment of information systems risks. Such assessment may occur through formal reviews and studies or be based on knowledge of operations within the Institution. Staffs are expected to use their expertise in determining the frequency of assessment and the specific areas to review.

Use of Results: Risk assessment results are used in decision making in a variety of areas, including: budgeting, investment, and deployment decisions; contingency planning; the development of further policies and procedures; the establishment of internal controls; changes to staffing and expertise; insurance adjustments; and the establishment of work priorities for staff and units throughout the institution. Risk analysis results should be used to minimize risk exposures and establish mitigating controls for safe, sound, and efficient information systems operations appropriate to the culture, structure, scientific and business goals and complexity of the Carnegie Institution.

Cooperation: Employees are expected to cooperate fully with any risk assessments being conducted on systems which they use and for which they may have responsibility. Employees are also expected to cooperate with remediation plans.

Remediation: Risk analysis results are used to minimize risk exposures and establish mitigating controls for safe, sound, and efficient information systems operations appropriate to the Institution. In general, unit managers and the information systems staff are responsible for the execution, development and implementation of remediation programs. Remediation activities are to be coordinated, where appropriate, with the CIO.

Review: The process for reviewing risk should be assessed periodically, but no less frequently than every three years, to adapt to changes in the information systems environment. Management should also periodically review information systems risk mitigation activities to ensure that identified objectives are complete or in process.

Credit Card Processing and Security

The purpose of this policy is to establish guidelines for the Institution's processing charges/credits on credit cards. The Institution must protect against the exposure and possible theft of account and personal cardholder information that has been provided to the Carnegie Institution; and comply with credit card company requirements for processing, storing and/or transferring credit card information. This policy does not apply to electronic purchasing systems used by employees for a variety of purposes, such as buying equipment, purchasing airline tickets, and reserving hotel rooms. Cardholder data are any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, or Card Validation Code. This policy is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format.

All transactions (including electronic based) that involve the transfer of credit card information for the payment of monies to the Institution must be performed on the systems approved by the Director of Finance and Administration, after a prior compliance and security review from information systems staff. All specialized servers that have been approved for this activity must be administered in accordance with the requirements of the relevant Carnegie Institution policies and the Cardholder Information Security Program (CISP). The Financial Manager will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through Credit Card Terminals, while Web Based procurement of credit cards will be monitored by information systems staff. In addition:

1. No electronic credit card numbers should be transmitted or stored in any other system, personal computer, or e-

Return to Index

mail account. Encrypt transmission of cardholder data across open, public networks.

2. Protect stored cardholder data. Physical cardholder data must be locked in a secure area, and limited to only those individuals that require access to that data. In addition, restrict access to data on a “need to know” basis.
3. Store only essential information. Do not store the Card Validation Code, or the PIN Number. Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.)
4. Stored credit card information will be retained for a maximum of 60 days including all paper and electronic copies made for backup purposes. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.
5. Install and maintain a firewall configuration to protect cardholder data.
6. Do not use vendor-supplied defaults for system passwords and other security parameters.
7. Use and regularly update antivirus software.
8. Develop and maintain secure systems and applications.
9. Assign a unique ID to each person with computer access.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Carnegie units accepting credit card payments must comply with the Payment Card Industry Data Security Standard.

Units that need to accept credit cards need to contact the Financial Manager to execute the required paper work, receive any necessary training, and be given direction as how to document those transactions.

Units wishing to engage in electronic commerce using credit cards are required to contact the Financial Manager, and they will also be directed to the CIO who will provide them with technical instructions and documentation and will assist with creating their web site “storefront.”

It is not permissible to obtain credit card information, or transmit credit card information by e-mail.

Under no circumstances will any other payment mechanism other than those approved by the Carnegie Institution be permissible for electronic commerce on the web.

Segregation of Information Systems Duties

Whenever a Carnegie Institution Headquarters computer-based process involves sensitive, financial, valuable, personally identifiable or critical information, the system must include controls involving a separation of duties or other compensating control measures that ensure that no one individual has exclusive control over these types of information.

Whenever practical, every task involving sensitive, financial, valuable, personally identifiable or critical information, must require at least two people to coordinate their information- handling activities, including completing a task from beginning to end and approving the results of the work project.

Separate people should perform work in the following three areas: production application source code development and maintenance, production application staging and operation, and production application data manipulation.

No Information Systems staff member should authorize a transaction, receive, and maintain custody of the asset that resulted from the transaction. The request for the purchase of an item should be approved by a supervisor or appropriate budget authority or delegate, received and acknowledged by the user and payment entry processed by the departmental fiscal employee.

If segregation of duties is not practical then compensating control measures must exist and must be documented to mitigate

the risk resulting from a lack of segregation of duties.

Physical and Environmental Security of Facilities

Section I of the Institution's policies, Safety and Facilities, provides the overall policies to support the security and safety within Carnegie Institution Headquarters facilities. This section provides supplemental information to help ensure the physical security, integrity and stability of the Carnegie Institution data centers and telecommunications network.

Within a facility, access into data facilities requires adherence to additional protocols and restrictions. In general, employees must protect keys, lock combinations, access codes and badges in a manner appropriate to the value and sensitivity of the asset they protect.

Keys and access cards for server rooms, safes or containers must be safeguarded by the information systems staff in a manner consistent with the most sensitive information or asset to which the keys provide access. Keys must be changed when the lock has been, or may have been, compromised. Access cards must be promptly deactivated when an employee is no longer granted access to a facility.

Access to information technology facilities is granted only to authorized personnel whose job responsibilities require access to that facility. All facilities must track visitor access with a sign in/out log based upon the criticality of the facility being protected.

Physical security measures should be in accordance with standards specified by the National Fire Protection Association, Protection of Electronic Computing/Data Processing Equipment, and by Occupational Safety & Health Administration (OSHA) Safety and Health Standards. Further, no eating or drinking should be allowed in a data center or server room.

Environmental control measures (e.g., power supply, heating, ventilation, air conditioning, plumbing, and physical location) should be sufficient to protect Carnegie Institution information systems assets from preventable service disruptions or harm.

An access log to the systems facilities should be maintained by the systems administrator. The systems administrator shall periodically review these logs and record all findings (or the lack of) in the Help Desk system.

Continuity Management and Disaster Recovery

Information systems staff members are required to maintain a local disaster recovery plan and to update it periodically to assure its relevance. The CIO is responsible for the Headquarters' plan.

The planning process should include an assessment of vulnerabilities and the criticality of business systems and administrative data.

Information systems staff will set up and maintain off-site facilities, or contractual agreements, for data backup storage and redundant and reliable standby systems. Critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.

A written disaster recovery document should exist that defines the roles and responsibilities of the incident response team with the team member's contact information. The document should also describe which methods the incident response team members will use to communicate in the event of a disaster.

Copies of the written plans should be distributed to everyone involved and also stored in an off-site, fireproof vault.

Every critical production business application and every production information systems infrastructure component must have a contingency plan that permits the restoration of service within a reasonable period of time. Procedures for restoring service should be documented in formal contingency plans. To the extent practical and feasible, these plans should be reviewed, tested, and updated at least annually. Each such test must be followed by any remedial actions that need to be taken.

To the extent required, an overall framework for segmenting information resources will be established to allow the most critical information resources to be recovered first.

Support levels that will be provided in the event of a disaster or emergency should be documented. The document should also specifically assign responsibility for managing and facilitating the restoration of service.

Employees who participate in off-site recovery operations with Carnegie information systems should be rotated regularly so that at all times at least two people will have the technical knowledge needed to perform each essential recovery task.

Systems Audit

The Carnegie Institution Headquarters may also use internal auditors to periodically perform checks to ensure that all parties are performing their assigned duties, and to ensure that other information security requirements are being consistently observed. Internal systems audits related to information security are conducted under the authority of the CIO who shall consult with the Director of Administration and Finance and the President.

System controls

To the extent feasible, Carnegie Institution management must be periodically notified about the accuracy, timeliness, relevance, and other information integrity attributes that describe the information they use for decision making and for financial reporting.

Planning and execution of system audits

Any systems audit activities and requirements should be planned and executed in a manner that minimizes the chances of disruptions to regular business processes and scientific activities.

All audit procedures, requirements and responsibilities should be documented.

Protection of audit tools and results

Information systems staff should establish controls to help safeguard the integrity of audit software and data files and to prevent the misuse of audit software, audit results and related data files.

Programming source code for computer viruses, worms, Trojan horses and other routines used to compromise security should be disclosed only to those persons with a demonstrable need-to-know to prevent unauthorized persons from using this information to compromise systems security. Similarly, technical analysis of such software routines should also be disclosed only to those with a need-to-know.

Security policy compliance reviews

The Carnegie Institution will review the security of its information systems by examining how well its systems, the organization, third-party providers, owners of information, users and management comply with existing security policies, procedures, and standards.

Internal auditors may help to perform independent compliance checking related to information security policies, standards, and procedures.

Technical security compliance tests

To ensure that the Carnegie Institution Information Systems staff has taken appropriate preventive measures, all systems directly connected to the Internet or to Carnegie internal networks should be subjected to an automated risk analysis performed via vulnerability identification software. The results of these tests should be documented to include appropriate corrective steps taken.

All information systems with connections to the Internet, to Carnegie internal networks or accessible by the public should operate Information Systems approved active host based or network based intrusion detection software.

All host based and network based intrusion detection systems should be checked periodically and their logs reviewed.

Any technical security compliance test should ensure that the Institution's information systems comply with technical security standards, including the proper implementation of hardware and software controls

Periodic penetration tests should be carried out in order to detect security vulnerabilities in the Institution's Information Systems and to check whether the controls in place can prevent unauthorized access to information.

Procedures

Account Creation Procedure

Headquarters requires a written request sent to the Help Desk system for all account creation. This request shall include the user's first and last name, department, start date, expected termination date, and required network, data, and/or program access rights and privileges. The systems administrator will create accounts in Microsoft Active Directory, Open Directory, Google Applications and other necessary systems utilizing base templates. Once accounts are created additional access to resources may be granted through group memberships, including mandatory participation in certain mailing lists, and the creation of user home directories in the DFS structure. Account information, including temporary passwords will be provided to users.

Account Changes Procedure

In order to make changes to a user's account, Headquarters' policies require a written request sent to the Help Desk system by the user's supervisor/manager. The request must include the user's name, network, data, and/or program access rights to be added/removed. The user must be also notified prior to being granted additional rights and privileges. Once these prerequisites are met, the systems administrator will adjust the account accordingly and post all changes to the ticket. The systems administrator will also ensure that each underlying and/or related system properly reflects the changes (Active Directory, Open Directory, mandatory list memberships, along with other user and program access rights.)

Account Termination Procedure

Account Terminations must be submitted to the Help Desk system by the users supervisor/manager prior to termination. The request should include the user's full name and the list of accounts to be closed (Active Directory, E-Mail, Accounting or other software package requiring a separate login credentials.) In addition, a date of termination should be included to ensure that access is removed in a timely fashion. The systems administrator shall document all actions taken and disable all relevant accounts in each underlying system at the requested time. The systems administrator will also ensure that each related system properly reflects the changes (mandatory list memberships, along with other user and program access rights.)

Data Backup and Storage, Financial System

Carnegie Headquarters follows these particular guidelines with respect to its accounting system:

Data must be backed up daily or when requested by the system owner.

Active financial data must be backed up weekly using the tools provided by the financial system application.

Active data backups must be restored weekly to the hot backup server and tested periodically for quality. Such backups must be also copied to recordable DVD or CD media and stored in an on-site fireproof media safe.

On a weekly, monthly, and annual basis, full data, application and system backups to tape must be performed.

All weekly backup tapes must be rotated in/out of an on-site fireproof media safe.

Monthly Backup Tapes and copies of active data backups on recordable DVD or CD media must be shipped to the disaster recovery site, and maintained off-site in a fireproof media safe. When a perpetual annual tape arrives at the off-site location, the monthly tapes may return to their parent site and be re-admitted into the tape rotation.

Written documentation must be kept on all transfers of tapes and other media to off-site locations, including date and type of backup and all necessary labels to enable easy identification of the media necessary to restore data to a required point in

time.

Tapes and other media containing financial and administrative data must be transported to off-site storage via a secure method, requiring tracking and delivery conformations as well as some form of tamper evident seal or locking device to maintain the integrity of data stored on the tape.

User Account Management, Financial and Administrative System

All financial and administrative system access requests should be sent by the user's supervisor to the Help Desk system. The supervisor should request the level of access to be granted for the appropriate modules that will be used by that person. For financial users, the Financial Manager should review the information and make a determination based on such factors as the duties the user will perform, the user's organization, and the accounts and/or departments the user needs to be able to access. The Financial Manager forwards the request to the Systems Administrator.

The Systems Administrator should review the information to ensure that the request is valid and that it has been properly authorized and determine the type of network and systems access that should be given to the user. This determination is based on such factors as the duties the user will perform, the user's organization, and the accounts and or departments the user needs to be able to access.

The Systems Administrator should notify the user and the requesting supervisor when the access has been implemented. The Systems Administrator and the Financial Manager approving the access have the responsibility to ensure that the access given is in accordance with established policies and procedures.

Passwords on all financial and administrative system user accounts automatically expire when their Active Directory passwords expire. Prior to the planned expiration date, users will receive an electronic message at login, prompting them to change their password.

Passwords on all Active Directory Windows network user accounts automatically expire every 180 days. Prior to the planned expiration date, users will receive an electronic message at login, prompting them to change their password.

The department business manager is responsible for reviewing an employee's accounting system access if the employee transfers to another position within the same department to ensure that appropriate requests are submitted to change or cancel the employee's existing accounting system account. Requests to change or cancel the employee's existing accounting system access are submitted to the Help Desk system.

If an employee transfers to another department or division at Carnegie, the current supervisor is responsible for submitting a request to the Help Desk to cancel the employee's existing accounting system and user account. If access to the accounting system is required in the new position, the employee's new supervisor is responsible for submitting a request for the reactivation of the user's account. The Financial Manager and the System Administrator will review the request to determine the type of network and systems access that should be given to the user.

Systems Development Life Cycle Methodology, Administrative Systems

The Carnegie Institution's Chief Information Officer is responsible for installing and maintaining the administrative computing systems of the institution. In carrying out this responsibility, the CIO works with the appropriate Carnegie officials, including the Director of Administration and Finance and the Chief Advancement Officer. Administrative systems refer to the Agency's accounting and financial management, advancement, HR, procurement, and inventory systems and their support systems. In general, the Institution follows a systems development life cycle (SDLC) methodology, with adjustments based on the size and complexity of the system, in making decisions about such systems.

The key steps in the process are:

An initiation phase that identifies a business need and proposes a preliminary information systems solution. In this phase, a preliminary plan is developed and the business context of the project is determined. This is the phase where the scope is set, resources are planned, and the operational context for the new system is determined. Staff should conduct a sensitivity assessment, perform initial or preliminary risk assessment and review solicitation documents (e.g., Requests for Proposal).

Return to Index

An analysis phase that models the current business process, whether electronic or manual; conducts market research to assess software packages that will address requirements; analyzes the desired system, and reanalyzes the requirements in light of available packages.

A systems selection phase that may include formal proposals; product demonstrations; or some other process for response to the Institution's requirements and a decision-making process. See the Procurement section of policies and procedures for additional details. The contract is also a deliverable for this phase including the terms and conditions for the handling of interfaces; documentation, training, and support; and deadlines. At the end of this phase, a package is recommended for purchase, the recommendation and contracts are forwarded to the purchasing authority.

Fit/Gap Analysis phase that identifies any required functionality that is not included in the package, in addition to any changes to the package that are required. If necessary, the analysis phase may need to be revisited, to incorporate the functions of the package.

Logical and physical design phase for determining any additions or changes based on the implementation platform and the interface requirements of the package and completing the technical blueprints.

A development/installation phase that includes any business process re-engineering as well as any necessary data conversion. This phase includes acceptance testing and staff training. In some instances, a vendor or external contractor provides the primary support; however Carnegie support personnel should be assigned to co-ordinate the effort. When the system is running live, it is reviewed to ensure that all of the goals in the project plan were met satisfactorily.

The institution's policy is that all information systems that process, store, or transmit financial or sensitive information must go through a formal testing process before being moved into a production environment. The process must involve the Information Systems staff in and the Chief Information Officer. The type of testing will depend on the nature of the change. Movement to a production environment requires approval of the information systems staff and the owner of the particular system (e.g., change to accounting software requires approval of financial manager).

Disposal phase handles the disposition (move, sanitize, dispose, archive, etc.) of information, software, and hardware. The Institution must ensure long-term storage of cryptographic keys, consider legal requirements for records retention, consult with financial staff regarding retaining and archiving federal records, and sanitize media (overwrite, degauss, or destroy) that are being disposed of.

In-house Development of Software

On occasion, there may be a need for specific in-house programming and software development. To the extent that these efforts require support from information systems staff, they will follow an abbreviated review and development cycle as described in the preceding section, particularly for small projects.

Production Systems

A production system is a system that is regularly used to process information critical to Carnegie Institution business. Any software developed in-house that runs on production systems should be developed according to the information systems development life cycle methodology (SDLC). Modification to all production systems should follow the change and release management processes. All production systems must have an access control system to restrict who can access the system and restrict the privileges available to these users.

When possible, there should be a separation between the production, development, and test environments. A formal and documented process should be used to restrict and approve changes to production systems. All known application program-based access paths (backdoors) other than the approved user access paths must be deleted or disabled before software is moved into production.

Users should not write production computer programs to process sensitive or financial information unless specifically directed and approved by the CIO.

Guides and Best Practices

Guide for Appropriate Use of Information Systems Resources

Examples of acceptable use of the Institution's computers for personal purposes include:

For educational purposes if the course work is for an approved degree program.

Use of information technology to check credit union or retirement plan accounts.

Retention of limited personal data in electronic files.

Use of the Internet to obtain information or conduct research, such as reading newspaper and magazine articles, checking airline prices and schedules and purchasing tickets, browsing sales catalogs, or obtaining road maps.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the Carnegie Institution authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Carnegie Institution-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Carnegie Institution.

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 Carnegie Institution or the end user does not have an active license is strictly prohibited.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs.)

Revealing an account password to others or allowing use of an account by others. This includes supervisors, colleagues, friends, family and other household members when work is being done at home.

Using a Carnegie Institution computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Making fraudulent offers of products, items, or services originating from any Carnegie Institution account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

Circumventing user authentication or security of any host, network or account, except as required by the IS staff in the performance of their responsibilities.

Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

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 via the Internet/Intranet/Extranet.

Return to Index

Providing information about, or lists of, Carnegie Institution employees to parties outside the Carnegie Institution unless authorized to do so.

Providing information about, or lists of Carnegie Institution donors and friends to parties outside the Carnegie Institution unless authorized to do so.

Computer usage that reasonably offends other employees, users, or outsiders, or results in public embarrassment to the Institution.

Computer usage that is not specifically approved and which consumes significant amounts of computer or network resources not commensurate with its benefit to the Institution's mission or which interferes with the performance of an employee's assigned job responsibilities.

Sharing or transferring of an individual's Carnegie account, including network ID, password, or other access codes to allow unauthorized personnel to gain access to Carnegie information systems resources.

Operation of a private business or social activity unrelated to the Carnegie Institution.

Violation of license and other computer related contract provisions, particularly those that expose the Institution to significant legal costs or damages.

Guide for Appropriate Use of Email

Limited use of e-mail for non-official communications is permitted.

Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages.

Unauthorized use, or forging, of email header information, or solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is not allowed.

Carnegie employees must not send unsolicited email messages, including the sending of "junk mail" or other advertising material, or promotional material to individuals who did not specifically request such material (email SPAM).

Users must not misrepresent, obscure, suppress, or replace their own or another user's identity in email messages or on any other Carnegie Institution information system. In all instances, the user name, electronic mail address, organizational affiliation, and related contact information must reflect the actual originator of a message. The use of anonymous re-mailers or other identity-hiding mechanisms is forbidden.

Users must not send any sensitive parameters such as credit card numbers, telephone calling card numbers, fixed passwords, social security numbers, background check results in emails or through the Internet unless the message is properly encrypted.

Guide for Secure Removal of Data

Computer systems and other electronic devices store information on a variety of media. It is important to ensure that all licensed software and all confidential information are securely removed from devices before ownership is transferred. Commands such as 'delete' and 'remove' do not erase data, they simply remove the directory pointers to the data's location on the physical storage media. Emptying the Recycle Bin or Trash Folder does not erase files. Similarly, 'fdisk' and 'format' commands modify the file system but do not actually remove data from the disk.

In order to securely remove data from a device, disk wiping programs have been developed. These programs repeatedly write a (usually random) series of 1's and 0's over the storage, in an effort to securely erase information contained on it so that it is not recoverable. Many disk wipe programs let you decide how many times to overwrite the storage. The best practice is to use from three to seven passes. For transfers within Carnegie departments, a single pass wipe is sufficient.

You are recommended to destroy media that cannot be wiped, such as CD-ROMs, inoperable/broken disk drives, DVD's, tapes, or other damaged media devices. Contact Helpdesk to discuss specifics if you have media you believe is unable to be securely wiped.

Guide for Laptop and Portable Device Use

Laptops, portable computers, mobile phones and PDA's present their own unique set of security concerns due to their portability. They are used in office settings, but just as often are used away from the office. One must consider the physical security of these devices and the protection of the confidential and/or sensitive information that is often stored on them.

Employees should follow these general rules:

Unless absolutely necessary, do not leave laptop or portable computers unattended. To discourage computer theft, use cables to lock computers to work surfaces that are often used. Consider using products that use tracking devices that may help recover lost or stolen devices. Record and keep serial numbers or other unique identifiers that may help identify lost or stolen computers.

Use good judgment about the amount of institutional or other sensitive data that you store. In general, personally identifiable, sensitive and confidential data should not be stored on laptop computers. If your laptop or portable contains personally identifiable, confidential and/or sensitive information, consider using a product that will encrypt the entire hard disk of your laptop computer, so that the computer cannot even be booted up by anyone who does not have the password, or choose to encrypt only specific files or directories, so that no one else can get into your sensitive data without knowing your password.

Use power-on passwords to prevent unauthorized use of the device. Use firewall programs to prevent unauthorized access to your device from other network nodes.

Email list manager and owner responsibilities

The mailing list manager is responsible for:

Managing the mailing list. This includes learning to use the web interface to review the list and deal with any problems with subscriptions.

Responding to questions about the list's use, its content and routine functions such as subscribing and unsubscribing.

Monitoring the list for appropriate use. Any discussion that is not within the scope of the list's declared purpose should be referred to another list. Abuse of others on the list by one or more members should not be tolerated.

Monitoring the list for correctness of e-mail addresses. Mailing list managers will receive error messages for broken or incorrect e-mail addresses. They should unsubscribe any addresses that can not be fixed expeditiously. Broken or incorrect e-mail addresses cause wasted time for others and wasted resources on the network.

Sending periodic reminders to subscribers. These reminders, which should be issued at least annually, should include a statement of purpose for the list and information on how to unsubscribe from the list. This requirement may be waived for certain lists by the list manager.

Providing for continuance or disbandment of the list before relinquishing the list manager role. Before disbanding an active list, list managers should provide appropriate notice to subscribers.

Confirming that the mailing list is being used for its declared purpose by responding to periodic e-mail requests issued by Information Systems staff.

List Sponsors are responsible for:

Authorizing creation of new mailing lists.

Periodically reviewing the appropriateness of mailing lists that they sponsor and informing IS staff of any lists they no longer wish to sponsor.

Assuring that a responsible list manager is assigned to each list they sponsor.

Information systems staff is responsible for:

Return to Index

Maintaining mailing list software and corresponding web pages.

Providing documentation and training materials for mailing list managers.

Assisting mailing list managers in dealing with special problems such as security and mail bombing.

Setting up new mailing lists.

Periodically (but no more than once each calendar year) notifying sponsors of lists that they sponsor and offering them an opportunity relinquish their sponsorship.

Periodically (but no more than once each calendar year) issuing e-mail requests asking mailing list managers to confirm that each mailing list they manage is being used for its declared purpose.

Removing any list that is no longer being used for its declared purpose.

Removing any list that is no longer sponsored.

Removing or limiting any list that is managed inappropriately.