

University of Tulsa Information Security Policy
approved by the President's Executive Council, March 3, 2004
(based in its entirety on the Georgetown University Information Security Policy,
approved on May 13, 2003)

Table of Contents	Page
I. STATEMENT	2
Purpose	2
Scope	2
II. PHILOSOPHY	3
III. RESPONSIBILITIES	4
Stewards	4
Users	5
Managers (of Users)	8
Information Service Providers	9
University Information Security Officer	11
Local Information Security Personnel	12
Internal Auditor	12
University General Counsel's Office	13
IV. ENFORCEMENT	13
V. RESOURCES	13
VI. APPROVAL HISTORY	*****

1. **I. STATEMENT**

2. **Purpose**

3. The University of Tulsa Information Security Policy (the “Policy”) serves to create an environment that will help protect all members of the University of Tulsa community (the “University”) from information security threats that could compromise privacy, productivity, reputation, or intellectual property rights. The Policy recognizes the vital role information plays in the University’s educational, research, and operational missions, and the importance of taking the necessary steps to protect information in all forms. As more information is used and shared by students, faculty and staff, both within and outside the University, a concomitant effort must be made to protect information. The Policy serves to protect information resources from threats from both within and outside of the University by setting forth responsibilities, guidelines, and practices that will help the University prevent, deter, detect, respond to, and recover from compromises to these resources, and to foster an environment of secure dissemination of information.
4. This Policy is set forth in seven sections: (1) the purpose and scope of the Policy, (2) the philosophy underlying the University’s information security efforts, (3) the responsibilities and practices each member of the University community shares for information security, (4) enforcement of the Policy, and (5) the resources available to assist in complying with this Policy. Individuals and departments within the University may adopt additional information security requirements that are specific to their operations, provided that such requirements are consistent with this Policy. However, in the event that an applicable state or federal statute governs certain types of information, e.g., Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), or financial information under the Gramm-Leach-Bliley Act (GLBA), the state or federal statute will take precedence.

5. **Scope**

6. **Persons**

7. This Policy applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers and other members of the University community, including those who are affiliated with third parties, who access University computer networks. It sets forth specific responsibilities for those who have primary responsibility for information resources (“Stewards”), individuals who use those resources (“Users”), individuals who have management or supervisory responsibility (“Managers”), information service providers, the Internal Auditor, the University General Counsel’s Office, the University Information Security Officer, and Local Information Security Personnel. (See Section III: Responsibilities.)

8. **Information Resources**

9. This Policy applies to all University information resources, including those used by the University under license or contract. “Information resources” include information in any form and recorded on any media, and all computer and communications equipment and software.
10. All information covered by this Policy is assigned one of three classifications depending on the level of security required. In decreasing order of sensitivity, these classifications are Confidential, Internal-use-only, and Unrestricted. Information that is either Confidential or Internal-use-only is also considered to be Restricted.
11. **Confidential information.** This classification covers sensitive information about individuals, including information identified in the human resources policies, and sensitive information about the University. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include information about:

12. Current and former students (whose education records are protected under the Family Educational Rights and Privacy Act (FERPA) of 1974), including student academic, disciplinary, and financial records; and prospective students, including information submitted by student applicants to the University.
13. Research subjects, clinic clients, library patrons, donors and potential donors.
14. Current, former, and prospective employees, including employment, pay, benefits data, and other personnel information.
15. Research, including information related to a forthcoming or pending patent application, and information related to human subjects. Patent applications must be filed within one year of a public disclosure (i.e., an enabling publication or presentation, sale, or dissemination of product reduced to practice, etc.) to preserve United States patent rights. To preserve foreign patent rights, patent applications must be filed prior to public disclosure. Therefore, it is strongly recommended that prior to any public disclosure, an Invention Disclosure Form be submitted to the Office of Research for evaluation of the technology and determination of whether to file a patent application, thereby preserving U.S. and foreign patent rights.
16. Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.
17. Information security data, including passwords. Information about security-related incidents.
18. **Internal-use-only.** This classification covers information that requires protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for Confidential information. Examples of Internal-use-only information are internal memos, correspondence, and other documents whose distribution is limited as intended by the Steward.
19. **Unrestricted information.** This classification covers information that can be disclosed to any person inside or outside the University. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and destruction of information.
20. **Default classification.** Information that is not classified explicitly is classified by default as follows: Information falling into one of the Confidentiality categories listed above is treated as Confidential. Other information is treated as Internal-use-only unless it is published (publicly displayed in any medium) by the Steward, in which case it is classified Unrestricted.
21. **II. PHILOSOPHY**
22. The philosophy underlying this Policy is expressed by these principles:
23. Support University mission. The Policy is designed to support the mission of the University by protecting the University's information resources, reputation, legal position, and ability to conduct its operations. It is intended to facilitate activities that are important to the University.
24. Consistent with institutional policies, contracts, and laws. The Policy is meant to be consistent with and serve to enforce the University's policies regarding access, acceptable use and privacy, and other relevant University policies; contracts and license agreements governing software, copyrighted documents, and other forms of intellectual property; and laws governing student information, health care information, and other sensitive information.
25. Comprehensive. The Policy covers all information resources that are owned by the University or used by the University under license or contract. This includes information recorded on all types of analog and digital media, computer hardware and software, paper, computer networks, and telephone systems. The Policy aims to protect against intentional and unintentional acts that could compromise the

confidentiality, integrity, or availability of the University's information resources. It is intended to address both internal and external threats, including, but not limited to, error, fraud, embezzlement, unauthorized disclosure, unauthorized access, spamming, theft, sabotage, terrorism, extortion, privacy violations, service interruption, and natural disasters.

26. Privacy. Policies and procedures for determining that information is private is not covered by this University policy.
27. Appropriate and cost-effective. Not all information resources require the same level of security or protection mechanisms. Policy requirements were formulated with the objective that the application of security measures be commensurate with the sensitivity and value of information resources and the actual threats to those resources. The intent is not to dictate requirements whose implementation would impose unnecessary costs.
28. Best practices. The information security requirements articulated by the Policy are meant to be consistent with the best practices at institutions of higher education.
29. Shared responsibility. All members of the University community share in the responsibility for protecting information resources for which they have access or custodianship. The Policy recognizes that people will need adequate information, training, and tools to exercise their responsibilities and that these responsibilities must be made explicit.
30. Accountability. The Policy intends that members of the University community be accountable for their access to and use of information resources.
31. Flexible and adaptable. The Policy aims to mandate specific procedures and practices only where necessary to provide adequate protection. The goal is that members of the University community be able to exercise their discretion and best judgment when determining how to protect information for which they have responsibilities, subject to legal and other obligations of the University. Where procedures and practices are required, they are meant to be flexible enough to change as circumstances change.
32. Emergency preparedness. It is not possible to prevent all security incidents. The Policy is designed to ensure that appropriate measures are taken to prepare for possible incidents, including implementation of business continuity measures to protect critical information systems and processes.
33. Reassessment. The Policy recognizes that revisions may be required and that reassessment of the Policy is valuable.

34. **III. RESPONSIBILITIES**

35. All members of the University community share in the responsibility for protecting information resources for which they have access or custodianship. Most of the responsibilities set forth in this section are assigned to four groups of people: Stewards, Users, Managers (of Users), and Information Service Providers. In general, an individual will have responsibilities in more than one area, for example as Steward and User of information resources and possibly as Manager of a department. This section also articulates specific responsibilities for the University Information Security Officer, Local Information Security Personnel, the Internal Auditor, and the University General Counsel's Office. For more information relating to the responsibilities and recommendations set forth in this Policy, see the Information Security link at <http://www.is.utulsa.edu>.

36. **Stewards**

37. Stewards are those members of the University community who have the primary responsibility for particular information. All information covered under this Policy has a Steward. One becomes the Steward either by designation or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. For example, for purposes of this Policy, the

campus librarians are the Stewards of the library catalogs and related records; and the registrar of the University is the Steward of student data. For purposes of the Information Security Policy, faculty are considered the Stewards of their research and course materials; students are considered the Stewards of their own work.

38. The term Steward as used here does not imply ownership in any legal sense, for example, as holder of a copyright or patent. Indeed, information stored on University computers and networks may be legally owned by entities outside the University. This is the case, for example, with licensed software or data. In the context here, Steward means only the person with primary responsibility for an information resource. The Intellectual Property Policy discusses ownership of intellectual property.
39. Stewards have the responsibilities of Users of their information (see next subsection). In addition, they are responsible for the following:
 40. Establishing security policies and procedures. Stewards may establish specific information security policies and procedures for their information where appropriate. Stewards are responsible for the procedures related to the creation, retention, distribution and disposal of information. These must be consistent with this Policy, and policies for the retention of University records, as well as with other University policies, contractual agreements, and laws. Stewards may impose additional requirements that enhance security.
 41. Assigning classifications and marking information. Stewards are responsible for determining the classification of their information and any specific information handling requirements that go beyond this Policy, particularly as may be imposed by confidentiality agreements with third parties. Information that is Confidential or Internal-use-only shall be marked as such when it is presented or distributed to Users, especially when failing to do so could lead to a misunderstanding of the classification. Additional markings specifying handling and distribution requirements may be added.
 42. Determining authorizations. Stewards determine who is authorized to have access to their information. They shall make sure that those with access have a need to know the information and know the security requirements for that information. For Confidential information, they must also make sure that those given access have a need to know and have signed a confidentiality agreement that covers the information. This could be a general-purpose agreement that covers all Confidential information. Information may be disclosed only if disclosure is consistent with law, regulations and internal University policies, including those covering privacy. Except under unusual and specifically recognized circumstances, access shall be granted to individuals in such manner as to provide individual accountability.
 43. Record Keeping. Stewards shall keep records documenting the creation, distribution, and disposal of Confidential information. This process is also recommended for other types of information.
 44. Incident reporting. Stewards shall report suspected or known compromises of their information to their Managers, the University Information Security Officer, and/or Local Information Security Personnel. Incidents will be treated as Confidential unless there is a need to release specific information.
45. **Users**
 46. All members of the University community are “Users” of the University’s information resources, even if they do not have responsibility for managing the resources. Users include, for example, students, faculty, staff, contractors, consultants, and temporary employees. Users are responsible for protecting information resources to which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices (paper, reports, books, film, microfiche, microfilm, computers, PDAs, disks, printers, phones, fax machines, etc.) that are in their care or possession. They shall follow the information security practices listed below, as well as any departmental or other specific applicable information security practices.
 47. Familiarity with and adherence to University policies. Users are expected to adhere to all University

policies and exercise good judgment in the protection of information resources. They should be familiar with this Policy and other information-related policies, including but not limited to any University policies regarding acceptable use, access, and privacy. They should avail themselves of information security training opportunities where appropriate. They shall abide by any confidentiality statements and contracts they have signed through their association with the University. They must be aware that noncompliance with this Policy could lead to disciplinary action.

48. Physical security. Users shall provide physical security for their information technology devices. Doors shall be locked to protect equipment when areas housing them are unattended. External security devices shall be deployed in areas that cannot be effectively protected by other means. Portable equipment such as notebook computers, PDAs, and cellular phones should be registered, accounted for, and protected by University-designated anti-theft and recovery programs. Particular care is needed when traveling and at home to protect these devices.
49. Storage of information. Information that is classified Confidential must be kept in a place that provides a high-level of protection against unauthorized access and not taken outside the University unless it can be assured adequate protection. In general, this means storing the information behind a physical or electronic lock, for example, in an office, filing cabinet, or desk that is kept locked when the User is not present, or on a computer that provides strong access controls and encryption. Encryption consistent with University standards is strongly recommended for information stored electronically on all computers, especially portable devices such as notebook computers or Personal Digital Assistants (PDAs) that are vulnerable to theft or loss.
50. Information that is classified Internal-use-only shall be stored so as to provide a reasonable level of protection against unauthorized access, especially by persons outside the University. It is recommended that Internal-use-only information be kept behind a physical lock, and/or require electronic authentication for access. Similarly, access to restricted Web resources can and should be protected.
51. Unrestricted information may be stored anywhere, provided that measures are taken to prevent unauthorized modification and destruction. Users should be aware, however, that unmarked information may have a default classification of Confidential or Internal-use-only.
52. Distribution and transmission of information. Restricted information must not be distributed or made available to persons who are not authorized to access the information. This applies to originals, copies, and new materials that contain all or part of the information, and to oral communication of information. When Restricted information is distributed, it is distributed in such manner that the restrictions on its future distribution are clear.
53. Confidential information that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception. For electronic information, appropriate encryption is required for all restricted information, especially if that information is transmitted over public networks. In most instances, Information Services Providers are responsible for employing appropriate encryption in the services they provide to transmit restricted information; users must avail themselves of these services.
54. All classes of information may be signed or packaged in tamper-resistant containers to ensure integrity and authenticity. For electronic information, Users can consult the Information Security web page at <http://www.is.utulsa.edu> for software tools that provide integrity and authenticity. When distributing documents in electronic form, precautions shall be taken against distributing files and disks with viruses and other forms of malicious code (see virus protection below). Users should not forward e-mail messages with attachments without some level of confidence that the attachments do not carry malicious code.
55. Destruction and disposal of information and devices. Restricted information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. For physical documents, shredders are highly recommended, but at the very least, documents must not be placed in

trash or recycling bins.

56. When donating, selling, transferring, or disposing of computers or removable media (such as diskettes), care must be taken to ensure that Restricted data is rendered unreadable. For example, if used computers are given to a charitable organization, any Restricted information that is stored on the machines must be thoroughly erased. In general, it is not sufficient to “delete” the information, as it may remain on the medium. Software that rewrites random data on the medium, preferably several times, should be used instead. Alternatively, the medium may be physically or electromagnetically destroyed.
57. Passwords. Access to computers, software applications, and electronic information is frequently controlled through User identifiers and passwords. Users are responsible for creating and protecting passwords that grant them access to resources. Because shared passwords and identifiers present a major security risk, User identifiers and passwords must never be shared. Passwords that provide access to University resources must not be stored on personal computers and must not be displayed on sticky notes or scraps of paper sitting by computers.
58. Different applications will place specific requirements on passwords, but, in general, they must be 8 or more characters long. They shall include letters, numbers, and punctuation characters (where supported). They shall not be names, words in dictionaries, or permutations of personal data (birth dates or anniversaries, social security numbers, etc.). If Users are given initial passwords that deviate from this, they must change their passwords as soon as possible.
59. Computer Security. Users must take steps to protect their desktop and/or laptop computers, and/or PDAs from compromise either by external agents or members of the University community. They shall select operating systems and other software that is inherently securable, and modify default installation passwords and other configuration options to reduce vulnerabilities to a minimum. It is the user’s responsibility to ensure that security patches (software that fixes security vulnerabilities, often distributed by the vendors of the products with the vulnerabilities) are applied to their desktop, laptop or PDAs, or assure that an Information Service Provider installs current patches. They must cooperate with and avail themselves of any central services providing support for and/or review of these activities.
60. Remote access. Many personal computer operating systems can be configured to allow access across the Internet and other networks. Individuals must take care to ensure that their systems are configured so as to prevent unauthorized access. When remote access is allowed, special care shall be taken to select safe implementation options and ensure that passwords and other access controls are respected.
61. Remote access to a particular computer or device on the University network is likely to enable access, both proper and illicit, to other computers and applications on the network, so more is at stake than the individual’s own computers and devices. Dial-in modems on personal computers may also allow access to the University of Tulsa network, and their use is prohibited except when specifically authorized and when provisioned in accordance with the same guidelines established for University Information Service Providers (see below).
62. Logging out. Users shall log off from applications, computers, and networks when finished. If computers are located in secure offices or laboratories, Users shall not leave unattended personal computers with open sessions without locking office doors, locking the computer, or providing similar protection. If computers are located in the open or in a shared computer lab, Users shall complete their session and log off fully. The use of boot or other start-up passwords is recommended in environments where unauthorized persons may have physical access to computers. Shutting off computer monitors when not in use can also discourage such persons from attempting to use computers for snooping and other unauthorized activity (while also conserving energy). Many monitors have an automatic shut down feature that does this. Reactivating the monitor to use the computer must require a password, the same way a screensaver would.
63. Virus and malicious code protection. Users shall make sure that their personal computers employ

mechanisms that protect against viruses and other forms of malicious code, which may be distributed through e-mail or the Web. The University has licensed anti-viral software that may extend to home use. More information is listed in the Resources section of this policy. To ensure that virus protection remains effective, individuals must install new versions as they become available. They should verify that processes initiated by anti-virus programs to periodically reach across the Internet and update their virus definition tables actually run. If such processes are scheduled for times when the computer is powered off or the Internet site not reachable, they should be manually initiated.

64. Because anti-virus programs are not foolproof, individuals must exercise due caution when opening e-mail or downloading files from the Internet. The opening of unexpected or suspicious attachments shall be avoided. Users should configure their word processing, spreadsheet, and other applications to require User confirmation before macros, scripts, or other executable enclosures are opened. Confirmation shall be granted only if the source of the file is known and trusted.
65. Should a virus be detected, it must be immediately and completely eradicated before e-mail or files of any sort are sent to other users. After the contamination is eliminated, individuals to whom potentially infected e-mail or other files may have been sent should be informed. If the virus is particularly pernicious or if its removal is likely to be a lengthy process, affected individuals shall be informed as soon as possible by telephone or other non-electronic means. All potentially infected files, including those stored on network servers and back-up media, shall be examined (and treated if necessary) for infestation following the discovery of a virus.
66. Backups. Backups and records retention shall comply with University policies and procedures for records retention. Information that is stored on personal computers and not easily replaced shall be copied to removable media in order to protect against losses caused by a disk failure, virus, malicious activity, accidental deletion, or other act. Backup copies shall be made regularly and securely maintained in a different physical location to protect against physical catastrophes such as floods and fires. Care must be taken to store media under environmentally appropriate conditions. Because electronic media can degrade under any conditions, copies that may require long-term retention shall be periodically refreshed.
67. Information stored on departmental and University file servers is generally backed up automatically, following established procedures for off-site storage and business continuity readiness. Users should consider storing important files on these servers.
68. Regardless of where data is stored, Users should consider making additional backup copies of important data according to University procedures. University procedures must recognize that backup copies on CDs or desktop computers constitute additional security risks.
69. Incident handling and reporting. Users shall report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their Managers, the University Information Security Officer, and/or Local Information Security Personnel. They should cooperate with any investigation. Incidents will be treated as Confidential unless there is a need to release specific information.
70. **Managers (of Users)**
71. Managers are members of the University community who have management or supervisory responsibility, including deans, department chairs, directors, department heads, group leaders, supervisors, etc. Faculty who supervise teaching and research assistants are included.
72. Managers have all the responsibilities of Users and, where information resources originate, Stewards. In addition, they share responsibility for information security with the people they manage and supervise. They also are responsible for the following:
73. Establishing security policies and procedures. If Managers decide to establish specific information security policies and procedures for the people they manage or supervise, these must be consistent with

this Policy, as well as with other University policies, contractual agreements, and laws.

74. Managing authorizations. Managers must make sure their people have the access authorizations needed to perform their jobs. The authorizations themselves are acquired from the Stewards of the information resources. Managers should make sure their people lose access when they are terminated or job responsibilities change. Managers are responsible for administering and retaining confidentiality statements for the people they manage or supervise if confidentiality statements are required by the Steward(s) of the information.

75. User training and awareness. Managers shall provide an environment that promotes security. They shall make sure their people have the training and tools needed to protect information.

76. Incident handling and reporting. Managers shall report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their Managers, the University Information Security Officer, and/or Local Information Security Personnel. They shall cooperate with the investigation of and recovery from security incidents, including taking any disciplinary action deemed necessary by the appropriate University authorities. Incidents will be treated as Confidential unless there is a need to release specific information.

77. Information Service Providers

78. Information Service Providers (“Service Providers”) are those campuses, schools, departments and individuals that manage significant information resources and systems for the purpose of making those resources available to others. They include University Information Services, the four Colleges as well as other entities that operate at a school, division, department, or sub-department level.

79. Service Providers face more extensive requirements than individuals for information security. Beyond controlling access and protecting against unauthorized access and physical threats, they must play a more pro-active role in implementing and enforcing security policies and procedures; participating in integrated business continuity planning; auditing access, threats, and vulnerabilities; and developing and/or conforming to University-wide access, authentication, and authorization standards and policies.

80. Establishing security policies and procedures. Service Providers may establish specific information security policies and procedures governing the information resources they manage. These must be consistent with this Policy, as well as with other University policies, contractual agreements, and laws. Service Providers must designate Local Information Security Personnel to maintain and assure the integrity of the information resources, systems and networks for which they are responsible, or assign this responsibility to the University Information Security Officer. These Local Information Security Personnel will work closely with the University Information Security Officer, in a manner that is consistent with this Policy.

81. Physical security. Computer systems (servers, desktops, portable devices, etc.); network components (switches, routers, etc.); the cable infrastructure; and other facilities must be physically protected commensurate with the level of risk faced by the University should they be compromised. Power, temperature, water and fire monitoring devices shall be deployed as appropriate. Locks, cameras and alarms, etc., must be installed in technology centers and technology closets to discourage and respond to unauthorized access to the electronic or physical components contained in these areas. Service Providers are responsible for ensuring that components required to conduct mission-critical business are incorporated into the physical planning component of any University business continuity plan.

82. Computer security. Service Providers must take steps to protect their servers and mainframes from compromise either by external agents or members of the University community. They shall select operating systems and other software that is inherently securable and modify default installation passwords and other configuration options to reduce vulnerabilities to a minimum. They must install relevant security patches to fix software security problems on a continuing basis. They shall periodically verify audit and activity logs, examine performance data, and generally check for any

evidence of unauthorized access, the presence of viruses or other malicious code, or any other indicators of integrity loss. They shall cooperate with and avail themselves of any central services providing support for and/or review of these activities as well as performing more sophisticated procedures such as penetration testing and real-time intrusion detection.

83. Service Providers who develop, maintain, or modify key applications relating to financial data, human resources, student records, etc., must deploy adequate procedures for change control, separation of test and production environments, and separation of responsibilities for staff involved in these functions. They shall cooperate pro-actively with the Internal Auditor and the University Information Security Officer to ensure that policies are respected and that adequate procedures are in place.
84. Network security. Service Providers who support authorized access to University information must implement designs, policies, and procedures that protect the integrity of those services. Network security is to be maintained through a combination of technologies including, but not limited to, switched networks, strong authentication, encryption, and firewalls where appropriate. All Service Providers must respect the University physical network strategy and deploy University of Tulsa standard equipment. Network access, including modem and other remote access, must be implemented utilizing University standards, for hardware, software, authentication protocols, and access control. The Vice Provost for Information Services, and the appropriate Executive Officer of the Information Services Provider making the request for the exception must approve exceptions to this requirement.
85. Because the loss of integrity of any device or server on the network provides a platform for launching attacks on the integrity of the entire network, University Information Services, in collaboration with the Internal Auditor, will periodically probe the network and network servers for vulnerabilities, using software tools designed for this purpose. Service Providers and Local Information Security Personnel are expected to participate in and cooperate with this process, review reports, and take corrective actions as appropriate.
86. Access Controls. In granting individuals access privileges to information resources, Service Providers must adhere to policies established by the data Stewards and the University. Information specifying access authorizations shall be producible in an easily auditable format, and audit trails must be maintained on appropriate levels. User identifiers must respect the centrally generated assignments, and systems and applications must support, to the extent possible, available University-wide standards and facilities supporting authentication, authorization, and single sign-on.
87. Shared, guest, and anonymous accounts shall be avoided. Guests shall be incorporated into the central User identifier facility when possible. Any anonymous accounts must be restricted to servers containing Unrestricted data, and not residing within a firewall zone or behind a similar barrier protecting servers containing Restricted data.
88. Service Providers shall periodically review User identifiers and access privileges, and revise them as required by changes in job function, transfers, and affiliation with the University. Where University-wide facilities are deployed to aid User identifier management, individual systems and applications shall interface with them whenever possible.
89. Passwords. When passwords are used for authentication, Service Providers shall install password mechanisms that provide strong security while also aiding Users with the selection and management of strong passwords (see section on Users). Where independent password files must be maintained, they must be protected by encryption as well as access restrictions. Appropriate restrictions regarding password lengths and the use of personal data or dictionary words for passwords must be implemented, using software enforcement where possible. The initial passwords assigned to Users may deviate from this as long as their lifetime is short and Users are forced to change them upon first use. Administrators and help desk personnel should be able to reset passwords following established procedures, but shall never be able to view them. The assignment of "root" access or similar powerful capabilities must be strictly controlled and limited as much as possible. Passwords to accounts with privileges that may be needed in emergency recovery situations shall be made available via "lock boxes," rather than distributed on an anticipatory basis.

90. Contingency planning. Service Providers are responsible for ensuring the continued availability of University information resources, and for planning for the resumption of mission critical business information services following the loss of equipment, data, and/or technology rooms due to flood, fire, equipment failure, natural disasters, etc. Two principal responsibilities result from this requirement. One is to participate in any integrated University-wide business continuity planning process. The other is to provide effective procedures for backing up University data.
91. Appropriate schedules shall be established for backing up servers and other devices containing important data, retaining copies, and refreshing media. Schedules and retention periods should support requirements for restoring data after accidental loss or corruption, restoring entire services following disasters, and record keeping requirements as identified by the data Stewards.
92. To ensure the availability and usability of backups, copies shall be stored in secure, environmentally controlled, off-site locations. Encryption/decryption applications and copies of cryptographic keys shall be stored in safe locations if they are required to restore backed-up data to a usable form. Archived data that is to be retained for historical/legal purposes should be recopied periodically. When applications change, either the original application shall be retained so as to be able to usefully access the archived data or the archived data should be converted to a format and medium that is usable by the new or another available application.
93. Incident handling and reporting. Service Providers must report suspected or known compromises of information resources to Managers, the Local Information Security Personnel, and/or the University Information Security Officer. They shall preserve and protect evidence and cooperate with any investigation. Where appropriate, they must repair vulnerabilities and install additional security measures to protect against future compromises. Incidents will be treated as Confidential unless there is a need to release specific information.
94. **University Information Security Officer**
95. The University Information Security Officer, or the individual(s) designated in writing by the Vice Provost for Information Services to fulfill such duties, has primary responsibility for oversight of information security, networks and systems, security policy, and educating the University community about security responsibilities. The University Information Security Officer shall report to the Vice Provost for Information Services, and his/her responsibilities include the following:
96. Policy Oversight. The University Information Security Officer must stay abreast of Federal and local legislation and how it affects security policy and planning. In addition, the University Information Security Officer must monitor activities and best practices relating to security at other institutions and follow the activities of organizations in higher education such as Educause.
97. User training and awareness. Effective information security requires a high level of participation from all members of the University and all must be well informed of their responsibilities as Information Stewards, Users, Managers, and Service Providers. In cooperation with Managers, the University Information Security Officer is responsible for managing a University training and awareness program for all members of the University community and for consulting with members of the University on information security issues. The first step should include distribution of this Policy to the entire University community. In addition, training classes and materials should be offered to instill the importance of appropriate information handling and to explain the implications of this Policy. Training should include specific information on the use of security precautions such as encryption, anti-viral tools, and backup procedures. The University Information Security Officer is responsible for maintaining the Information Security web pages, which makes the information security resources described in Section V of this Policy available to the University community.
98. Oversight authority for University networks and systems. The University Information Security Officer is responsible for overseeing network and system security for all resources of the University, with especially direct responsibility for all resources managed by and/or connected to resources managed by University Information Services. The University Information Security Officer also has approval

authority for any campus wide resource implementations that deviate from this Policy when those resource implementations contain Restricted data or could have a University-wide impact. For example, the University Information Security Officer must approve mechanisms installed to provide remote access to University information services if they do not follow University standards and guidelines. In addition, the University Information Security Officer is responsible for coordinating the communication and activities of the Local Information Security Personnel.

99. Policy enhancements and revisions. In cooperation with other members of the University, the University Information Security Officer shall periodically reassess this Policy to determine if revisions are needed to accommodate the fast changing nature of information technology or weaknesses in the Policy. If such revision becomes necessary, the University Information Security Officer shall convene an Information Security Policy Committee that includes, but is not limited to, representatives from the faculty, University Information Services, the University General Counsel's Office, and the Office of Student Affairs. This Committee shall also seek input from all relevant constituencies within the University. The revised Policy must be consistent with other University policies, laws, and agreements. It requires the same approval as any University-wide policy.

100. Incident Handling and Reporting. If information resources are compromised in violation of University's policies, the University will take steps to remediate, respond to and recover from the security incident. Depending on the nature of the incident, this can involve collecting and analyzing evidence, determining the responsible party, assessing damages, restoring data from backup files, closing security holes, installing stronger security measures, revising security guidelines and procedures, taking disciplinary action in accordance with appropriate University policies, reporting incidents to law enforcement, and interacting with the media. The University Information Security Officer will further investigate incidents and coordinate with all other necessary members of the University community, such as campus executive offices, Deans' offices, the Office of Student Conduct, the University General Counsel's Office, the Internal Auditor, Public Relations, other senior administrators, and with law enforcement officials.

101. Local Information Security Personnel

102. Local Information Security Personnel are appointed by Information Service Providers from those campuses, schools, departments and individuals that manage significant information resources and systems for the purpose of making those resources available to others. University Information Services and the Colleges must appoint Local Information Security Personnel. Other entities that operate at a school, division, department, or sub-department level, may do so at their option. Local Information Security Personnel are responsible for:

103. Local Security Responsibilities. Local Information Security Personnel are responsible for extending information security within their organization to systems and networks that they manage. Often they will have first-hand knowledge of their specific configurations and applications that will necessitate further definition of policies and procedures at their organizational level. They will provide user education and training.

104. Coordination with the University Information Security Officer. These Local Information Security Personnel will work closely with the University Information Security Officer to ensure that this policy is implemented and enforced consistently across the University.

105. Incident handling and reporting. Consistent with this Policy and other University policies and procedures, Local Information Security Personnel will take steps to remediate, respond to and recover from a security incident, similar to the way the University Information Security Officer is authorized to do so. Local Information Security Personnel must notify the University Information Security Officer of all incidents and actions taken.

106. Internal Auditor

107. The University's Internal Auditor is responsible for determining whether information is being

protected in conformance with this Policy and with departmental-level policies. Any inadequacies in the Policy shall be brought to the attention of the University Information Security Officer.

108. In accordance with University audit procedures, the Internal Auditor will conduct audits of the University's information security procedures and practices when this policy is initially adopted, and thereafter on a regular, periodic basis.

109. University General Counsel's Office

110. The University General Counsel's Office is responsible for interpreting the laws that apply to this Policy and making sure that this Policy is consistent with those laws and other University policies. Any inadequacies in the Policy shall be brought to the attention of the University Information Security Officer who will consult University General Counsel and others within the University as appropriate. University General Counsel is also responsible for reporting any criminal offense to the appropriate law enforcement agency.

111. IV. ENFORCEMENT

112. Violations of this policy will be handled consistent with University disciplinary procedures applicable to the relevant persons or departments. Consistent with the Ethics Code and Policy for Computer Use, the University may temporarily suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University resources or to protect the University from liability. The University may routinely monitor network traffic to assure the continued integrity and security of University resources in accordance with applicable University policies and laws; policies and procedures are subject to Internal and External Audit review. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

113. V. RESOURCES

Information resources supporting this Policy, including anti-virus software, are available by following the Information Security link at <http://www.is.utulsa.edu>.