Text to be deleted is in [square brackets] and text to be added is underscored.

INFORMATION SECURITY POLICY

INTRODUCTION

Storage of university data on computers and transfer across the network eases use and expands our functionality. Commensurate with that expansion is the need for the appropriate security measures. Security is not distinct from the functionality.

The Information Security Policy (Policy) recognizes that not all communities within the University are the same and that data are used differently by various units within the University. The principles of academic freedom and free exchange of ideas apply to this policy, and this policy is not intended to limit or restrict those principles. These policies apply to all units within the University.

Each unit within the University should apply this policy to meet their information security needs. The Policy is written to incorporate current technological advances. The technology installed at some units may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the chief information officer or the equivalent officer(s).

Throughout the document the term *must* and *should* are used carefully. "Musts" are not negotiable; "shoulds" are goals for the university. The terms *data* and *information* are used interchangeably in the document.

The terms *system* and *network* administrator are used in this document. These terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty. Many students, faculty and staff members are the system administrators for their own machines.

PURPOSE OF THIS POLICY

By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- To establish a University-wide approach to information security.

- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks and computer systems.

- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.

- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

RESPONSIBILITY

The chair of the University Technology Management Team (UTMT) is responsible for implementing the policy. UTMT, chaired by the Vice President for Administration, is a coordinating group comprised of chief information officers from the three campuses, the university administration, and the hospital.

UTMT must see to it that:

- The information security policy is updated on a regular basis and published as appropriate.

- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.

- Each unit appoints a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Members of UTMT are each responsible for establishing procedures to implement these policies within their areas of responsibility, and for monitoring compliance.

GENERAL POLICY

Required Policies

- The University will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the University's data, network and system resources.

- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Recommended Practices

- Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.

- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, data custodian, and users.

- Violation of the Information Security Policy may result in disciplinary actions as authorized by the University in accordance with University and campus disciplinary policies, procedures, and codes of conduct.

DATA CLASSIFICATION POLICY

It is essential that all University[’s] data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. We have specified three classes below:

High Risk [-] : Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified. The data owner should make this determination. It is the data owner’s responsibility to implement the necessary security requirements.

Confidential [-] : Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner’s responsibility to implement the necessary security requirements.

Public [-] : Information that may be freely disseminated

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.

•Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

•No University-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

•Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.

•High risk data must be encrypted during transmission over insecure channels.

•Confidential data should be encrypted during transmission over insecure channels.

•All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

•Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

ACCESS CONTROL POLICY

•Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.

•Where possible and financially feasible, more than one person must have full rights to any university owned server storing or transmitting high risk data. The campuses and University Administration (UA) [will] must have a standard policy that applies to user access rights. This will suffice for most instances. Data owners or custodians may enact more restrictive policies for end-user access to their data.

•Access to the network and servers and systems [will] should be achieved by using individual and unique logins, and [will] should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

•As stated in the [Appropriate Use Policy] current campus policies on appropriate and acceptable use, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. When limited access to university-related documents or files is required specifically and solely for the proper operation of University units and where available technical alternatives are not feasible, exceptions are allowed under an articulated unit policy that is available to all affected unit personnel. Each such policy must be reviewed by the unit executive officer and submitted to the CIO for approval. All users must secure their username or account, password, and system access from unauthorized use.

•All users of systems that contain high risk or confidential data must have a strong password- the definition of which will be established and documented by UTMT after consultation with the community. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by UTMT.

•Passwords must not be placed in emails unless they have been encrypted.

•Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.

•Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

•Users are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the University's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.

•Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.

•Transferred employee access must be reviewed and adjusted as found necessary.

•Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

•Activities performed as administrator or superuser must be logged where it is feasible to do so.

•Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

VIRUS PREVENTION POLICY

•The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.

•All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

•All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

•Headers of all incoming data including electronic mail [will] must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail [will] should be scanned where such capabilities exist.

•Where feasible, system or network administrators should inform users when a virus has been detected.

•Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

INTRUSION DETECTION POLICY

•Intruder detection must be implemented on all servers and workstations containing data classified as high risk.

•Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.

•Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.

•Intrusion tools should be installed where appropriate and checked on a regular basis.

INTERNET SECURITY POLICY

•All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.

•All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified confidential.

SYSTEM SECURITY POLICY

•All systems connected to the Internet should have a vendor supported version of the operating system installed.

•All systems connected to the Internet must be current with security patches.

•System integrity checks of host and server systems housing high risk University data should be performed.

ACCEPTABLE USE POLICY

Each Campus and UA must have a[n acceptable use] policy on appropriate and acceptable use that includes these requirements:

•University computer resources [will] must be used in a manner that [is compliant] complies with University policies and State and Federal laws and regulations. It is against [u]University policy to install or run software requiring a license on any [u]University computer without a valid license.

•Use of the University's computing and networking infrastructure by University employees unrelated to their University positions must be limited in both time and resources and must not interfere in any way with University functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.

•Uses that interfere with the proper functioning or the ability of others to make use of the University's networks, computer systems, applications and data resources are not permitted.

•Use of University computer resources for personal profit is not permitted except as addressed under other University policies.

•Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations. Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Auditors or security officers in the performance of their duties may also use them. They must not be used to monitor or track any individual’s network activity except under special authorization as defined by campus policy that protects the privacy of information in electronic form.

EXCEPTIONS

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

•Required commercial or other software in use is not currently able to support the required features;

•Legacy systems are in use which do not comply, but near-term future systems will, and are planned for;

•Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, units must develop a written explanation of the compliance issue and a plan for coming into compliance with the University's Information Security Policy in a reasonable amount of time. [and submit them to the appropriate] Explanations and plans must be submitted to the campus CIO or the equivalent officer(s) [university of campus CIO for written approval].