The Campus Senate of the University of Illinois at Springfield approves the attached amendments to the Information Security Policy.
### SECTION 19.5 - Information Security Policy - The University of Illinois

Date: 22 August 2002 - Modifications: 8 April 2003
Approved: University Technology Management Team

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Purpose of this Policy</th>
<th>Reponsibility</th>
<th>General Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Classification Policy</td>
<td>Access Control Policy</td>
<td>Virus Prevention Policy</td>
<td>Intrusion Detection Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix A</th>
<th>Appendix B</th>
</tr>
</thead>
</table>
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 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 the 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 its 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 appropriately designated University official(s).

Throughout this 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.
• To preserve academic freedom and encourage the free exchange of ideas using computer based systems and networks consistent with federal and state constitutional and legal rights and responsibilities.
• To balance security requirements with personal privacy, academic freedom, and the ability of the University to conduct its business affairs.

RESPONSIBILITY

The chair of the University Technology Management Team (UTMT)\(^1\) is responsible for implementing the policy in collaboration with appropriate University officials and faculty governance and administrative committees as determined by each campus.

Working in conjunction with appropriate University officials and committees on each campus, 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 with relevant campus officials, units, and committees.

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. Reviews must include monitoring access logs and

\(^{1}\) 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.
documenting the results obtained from monitoring software, including intrusion
detection software.

- The University must regularly back up all data that are considered high risk,
  confidential, or necessary in conducting the business of the University. All
  appropriate data must be backed up, and backups tested periodically, as part of a
  well-documented process. Backups of data must be handled with the same
  security precautions used when handling the data themselves.

**Recommended Practices**

- Vulnerability and risk assessment audits of systems, networks, and network
  connections should be conducted on a regular basis. At a minimum, audits should
  be performed on an annual basis. Audits should include the review of hardware
  systems, software systems, distributed infrastructure, and user access procedures.
- A systematic and continuing program of education should be implemented to
  ensure that users understand University security policies and procedures. A
  program of education should include, but not be limited to, information on
  systems security, confidentiality, acceptable use, and the protection of data
  integrity. Educational programs should be tailored to the specific roles and
  responsibilities among different members of the University community.
- 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**

All University data must be protected. However, there are different levels of security
required for different types of data. All data should be reviewed on a periodic basis and
classified according to their use, sensitivity, and importance. We have specified three
classes below:

**High Risk** – High risk data include 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, medical, human subjects, 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 they
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 procedures and related measures.
Confidential – Confidential data include information assets that would not expose the University to loss if disclosed. Confidential data should be protected to prevent unauthorized disclosure. It is the data owner’s responsibility to implement the necessary security procedures and related measures.

Public - Information assets that may be freely disseminated

All information resources should be categorized and protected according to the requirements set forth by the classification and associated data categories identified above. The data classification and its corresponding level of protection should be consistent when the data are replicated and as data flows through the University.

- Data owners must determine the classification of the data according to the three categories identified above and must ensure that the data custodian protect the data in a manner appropriate to its classification.
- All University-owned systems that are connected to the Internet must have the means to protect data on those systems consistent with the classification and data use categories specified above.
- Data custodians are responsible for creating data repositories and data transfer procedures to protect data in a manner appropriate to the classification.
- High risk data must be encrypted during transmission over insecure channels. When possible, high risk data should be physically isolated from public access.
- Confidential data should be encrypted during transmission over insecure channels.
- All appropriate data must be backed up, and the backups must be tested periodically, as part of a systematic, documented, regular process.
- Backups of data must be handled with the same security precautions as the data themselves. High risk data backups must be stored in a remote, secured location. Confidential data backups should be stored in a remote, secured location when feasible.
- When systems are disposed of or reassigned data must be deleted or storage media destroyed consistent with industry best practices in a manner appropriate to the classification of the data.

ACCESS CONTROL POLICY

- Systems security must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between maintaining system security and permitting authorized access without compromising convenience and ease of. This balance should be recognized.
- Where possible and financially feasible, more than one person should have full rights to any university owned server storing or transmitting high risk data. The campuses and University Administration (UA) must have a standard policy that
applies to user access rights. A standard policy will suffice for most instances. Data owners or custodians may enact more restrictive policies for end-user access to their data, where such policies do not violate state or federal laws.

- Access to the network servers and systems should be achieved by using individual and unique logins. Such logins must require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- As stated in the Appropriate Use (Acceptable Use at UIS) Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
- There are a set of contingent circumstances, which require access by designated University officials to a particular system or to University workstations of specific users. Such circumstances and authorization of University officials should be included as part of each campus’ Appropriate Use (Acceptable Use at UIS) Policy.
- 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 University 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 of University systems are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with the devices that will be used to access the University’s network or system resources. If an authentication token 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.
- System access by terminated employees must be reviewed and adjusted as necessary. Terminated employees must have their accounts disabled upon transfer or termination. Periodic reviews of user access to University systems appropriate University officials.
- Access by transferred employees to university systems, networks, and data must be reviewed and adjusted as necessary and on a regular basis.
- Where possible and financially feasible, monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

---

2 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.
Activities performed as administrator or super-user must be logged where it is feasible to do so. There should be a documented procedure for reviewing system logs.
Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.

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 in accordance with federal and state laws as well as University disciplinary policies, procedures, and codes of conduct.
When technically feasible, servers and desktop systems that are connected to University networks, which are not physically isolated, must be protected with an approved, licensed anti-virus software product that is updated according to industry best practices.
Incoming electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
Where feasible, system or network administrators should inform users when a virus has been detected. System administrators reserve the right to temporarily disconnect or isolate systems that are infected.
Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

INTRUSION DETECTION POLICY

Intruder detection must be implemented on all University systems 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 are classified high risk. Considering the technical limitations of securing high risk data for systems that connect to the Internet, periodic reviews of the University’s Information Security Policy should consider the costs and impacts of purchasing and installing more secure connections.
- All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data are classified confidential.

SYSTEM SECURITY POLICY

- All systems should have current, legal, and supported versions of operating systems installed.
- All systems connected to the Internet must be current with verified security patches.
- System integrity checks of host and server systems should be performed for systems containing high risk data.

ACCEPTABLE USE POLICY

Each Campus and UA must have an acceptable use policy that includes these requirements:

- University computer resources must be used in a manner that complies with University policies and state and federal laws and regulations. It is both illegal and against University policy to install or run licensed software without a valid license.
- Use of the University's computing and networking infrastructure by University employees unrelated to their University positions must not interfere 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 may use such tools in the performance of their duties. In addition, these tools may be used for instructional purposes, on systems that are physically isolated from other University systems and networks. These tools must not be used to monitor or track any individual’s network activity except under special authorization as defined by federal and state laws, and campus policies that protect the privacy of individuals in their use of information.

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. Explanations and plans must be submitted to the appropriate university officials or campus CIO for written approval.
# Appendix A - Current U of I Information Security Related Policies and Resources

<table>
<thead>
<tr>
<th><strong>General University</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AITS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Business and Finance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td></td>
</tr>
<tr>
<td>UIC HR Policies and Procedures, Official Personnel Records</td>
<td><a href="http://www.hr.uic.edu/quicklinks/policies/HRPP1300/1301.PDF">http://www.hr.uic.edu/quicklinks/policies/HRPP1300/1301.PDF</a></td>
</tr>
<tr>
<td><strong>Information Warehouse</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FERPA Resources and Source Documents</strong></td>
<td></td>
</tr>
<tr>
<td>FERPA - see Subpart D in particular</td>
<td><a href="http://www.ed.gov/offices/OM/fpco/ferpaonline.html">http://www.ed.gov/offices/OM/fpco/ferpaonline.html</a></td>
</tr>
<tr>
<td>FERPA is evolving (like case law). For the latest regs, see Additional FERPA Rulings</td>
<td><a href="http://www.ed.gov/offices/OM/fpco/ferpaonline.html">http://www.ed.gov/offices/OM/fpco/ferpaonline.html</a></td>
</tr>
<tr>
<td><strong>UIUC</strong></td>
<td></td>
</tr>
</tbody>
</table>
UIUC OAR FERPA Tutorial
Completion of this tutorial is required of anyone seeking access to UIUC Student Web Reports (online canned reports).

UIUC Campus Code of Policies and Regulations Applying to All Students

U Of I Direct Course And Student Data Access Guidelines

UIUC OAR Statement of Access Guidelines

Interim Policy On Appropriate Use Of Computers And Network Systems At The University of Illinois at Urbana-Champaign

Suppressing UIUC Electronic Directory Information

Electronic Directory

Appropriate Use Policy

<table>
<thead>
<tr>
<th>UIIC</th>
<th>ACCC Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.uic.edu/depts/accc/policies/">http://www.uic.edu/depts/accc/policies/</a></td>
</tr>
<tr>
<td></td>
<td>UIC Campus Policy on the Release of Information Pertaining to Students Confidentiality of Student Records</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.uic.edu/depts/oar/rr/confidential.shtml">http://www.uic.edu/depts/oar/rr/confidential.shtml</a></td>
</tr>
<tr>
<td></td>
<td>Student Records Policy</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.uic.edu/depts/oar/rr/records_policy.shtml">http://www.uic.edu/depts/oar/rr/records_policy.shtml</a></td>
</tr>
<tr>
<td></td>
<td>UICMC Information Security Standards and Guidelines</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.hospital.uic.edu/its/faq/security/overview.htm">http://www.hospital.uic.edu/its/faq/security/overview.htm</a></td>
</tr>
<tr>
<td></td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.uic.edu/depts/accc/policies/uicpol.html">http://www.uic.edu/depts/accc/policies/uicpol.html</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UIS</th>
<th>Technology-Related Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.uis.edu/technology/policies.html">http://www.uis.edu/technology/policies.html</a></td>
</tr>
<tr>
<td></td>
<td>Student Record Policy</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.uis.edu/registration/srp.htm">http://www.uis.edu/registration/srp.htm</a></td>
</tr>
<tr>
<td></td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.uis.edu/technology/policies.html">http://www.uis.edu/technology/policies.html</a></td>
</tr>
</tbody>
</table>
Appendix B - Frequently Asked Questions

Introduction
Purpose of this Policy
Responsibility
General Policy
Data Classification Policy
Access Control Policy
Virus Prevention Policy
Intrusion Detection
Internet Security Policy
Systems Security Policy
Acceptable Use Policy
Exceptions