February 26, 2010

Professor Philip A. Patston, Chair
UIC Senate Executive Committee
Dept. of Oral Medicine and Diagnostic Sciences
Room 558 DENT MC 838

Professor Joyce L. Tolliver, Chair
UIUC Senate Executive Committee
Dept. of Spanish, Italian, and Portuguese
4080 Foreign Languages Building MC 176

Professor Tih-Fen Ting, Chair
UIS Campus Senate
Dept. of Environmental Studies
PAC 308

Re: University Information Security Policy (USC OT-260)

Dear Colleagues:

The University Technology Management Team (UTMT) has approved an interim University Information Security Policy. UTMT will coordinate this policy, which requires implementation at the campus level. Professor Roy Campbell is the faculty representative to this group. The UTMT website is at https://www.utmt.uillinois.edu/home.

The Senates Conference sends the interim policy to you for information and to help guide the implementation process for the campuses.

Sincerely,

Kathryn E. Eisenhart, Chair
University Senates Conference

Enclosure

cc: Robert C. Damrau
    Elizabeth A. Dooley
    Mrinalini C. Rao
    Kathy L. Rutherford
    Members, University Senates Conference
Information Security Policy Team: Policy Outline

This page last changed on Sep 09, 2009 by mcorn.

Approval Status: Approved as Interim by UTMT
Approval Date: 9/8/2009
Last Edit Date: 9/3/2009

Scope

This policy applies to all campuses, units, and individuals of the University of Illinois. Many aspects of this policy are also in effect for organizations connecting to any portion of the computer networks owned or managed by the University of Illinois. Many aspects of this policy also govern individuals using information assets, resources, or services provided by the University of Illinois.

Introduction and Purpose

The purpose of this policy is to establish a University-wide framework for the protection of the information assets of the University of Illinois. These assets include not only specific data elements, but the technological tools that support them and the business, research, and pedagogical processes that produce, maintain, and consume them. This framework also aids in the University meeting its obligations towards regulatory compliance with regard to information security.

As mere policy this document does not intrinsically provide these protections. Rather it obligates each Chief Information Officer to create local policies, standards, and procedures that address each of the security controls identified. In order to guide this implementation process it provides three primary tools:

- identifies a number of core information security principles
- clearly delineates roles and responsibilities
- provides clear metrics by which compliance with each control will be measured.

Readers familiar with the previous information security policy may wonder where the specific technological requirements spelled out in that document have gone (such as the requirement that all computers run antivirus software). This and similar items have been moved out of this policy and will be articulated within campus specific policies and standards. In situations where no analogous standard has yet been created, it should be assumed that the previous policy’s statements remain in effect.

Definitions

Chief Information Officer role: The Chief Information Officer is the senior administrator with responsibility for information policy, systems and processes for a specific branch of the University’s organization. Due to inconsistencies in titles, as referenced within this policy, the CIO is a role whose specific domain of responsibility is agreed upon by the members of the University’s Technology Management Team (UTMT) and their respective campus executives.

Chief Security Officer role: The Chief Security Officer is the senior administrator responsible for the operational implementation of the Information Security Policy within each CIOs domain. As with the CIO, inconsistencies in titles require that this position is considered a role within the context of this policy and each CIO will designate this position.

Unit Executive: The senior executive within each unit, typically a Dean or Department Head, responsible for the operation and leadership of the unit.

Control: A domain of practice for which specific policies, procedures, and standards must be created to minimize risk to an organization. For example, "remote computing" or "identity management". Controls all share the following characteristics: oversight responsibility can be assigned; it is possible to collect evidence of compliance; they are areas of long standing concern (i.e., they change only slowly over time); a specific risk related rationale for their existence has been articulated.
Compensating Control: In situations where a specific requirements of a control cannot be met, the objective of the control may be met through differing mechanisms. For example, if a specialized piece of computing equipment relies on an embedded operating system that does not meet an established standard for operating systems, an appropriate compensating control may be to isolate the equipment via private IP space. Compensating controls are more specifically addressed at an operational level but are defined here in the interest of completeness.

Data Center: A physical space for the location of information assets that provides for restricted access and environmental control.

The following 'data' definitions are not consistently used across the 3 campuses and UA. Note that there is a hierarchy of authority defined here: Owner (has authority) -> Steward (delegated authority) -> Custodian (local responsibility).

Data Owner: The unit with primary responsibility for determining the purpose, function, and appropriate use of a data resource. Sometimes referred to as the Data Proprietor.

Data Steward: Role delegated by the data owner to one or more individuals that have the responsibility of the maintenance and protection of the organization's data. Typically an individual assigned by the data owner to classify data according to risk and to provide and maintain meta data. (See Information Classification under Controls)

Data Custodian: Any individual possessing data belonging to the University. Data Custodianship is a role which follows data as it is transferred to an individual or system and obligates the individual to use, maintain, and protect the data in accordance with University and Campus policy and standards.

Guidelines: A guideline describes what should be done in order to comply with generally accepted best practices.

Implementation Policy: A localized version of a system-wide policy. For example, each University of Illinois campus may need to define slightly differing standards in order to meet control objectives. The campus' implementation policy would document where such standards were available and which campus office had responsibility for their creation and maintenance.

Informational Assets: An informational asset is here defined as data or information that is of value to the University. This is situationally extended to include the network, systems, and applications that store, access, or manipulate them.

Malware: Software designed to infiltrate or damage a computer system or network without the owner's informed consent.

Policy: A policy describes specific objectives for the University of Illinois; it defines governance and responsibility for the objectives.

Procedures: A procedure describes the specific processes used in order to implement a control objective.

Standards: A standard describes what must be done in order to comply with a policy.

Governance and Responsibility

The Chief Executive Officer of each campus and University Administration will formally assign responsibility for Information Security to a senior administrator within each campus and University Administration, typically the Chief Information Officer. The responsibility for Information Security includes the authority to assume leadership and responsibility to develop, implement, and monitor for compliance the policies, standards, and procedures necessary to achieve the objectives detailed within this policy.

Collectively the Chief Information Officers are assigned the responsibility to ensure the timely maintenance of this policy and to regularly report to each other on their compliance efforts. This body, currently known as the University Technology Management Team (UTMT) is considered the owner of this policy for operational purposes.
In general, this policy will require updating when there have been:

- significant new or modified business processes and/or IT and communication systems affecting the University's risk profile;
- changes to legal and regulatory requirements; or
- new technological developments such as new encryption and data security technologies.

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive Officer</td>
<td>The three campus Chancellors and University President (see: <a href="http://www.uillinois.edu/trustees/statutes.cfm#sec13">http://www.uillinois.edu/trustees/statutes.cfm#sec13</a>)</td>
</tr>
<tr>
<td>UTMT</td>
<td>Coordinate the development and maintenance of the Information Security Policy in order to provide a consistent information security policy across the University.</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>Oversee the development, implementation and maintenance of the Information Security Program as designated by the relevant Chief Executive Officer.</td>
</tr>
<tr>
<td>Campus Faculty Senate</td>
<td>Represent the University faculty through membership on UTMT and as stakeholders in the implementation of the University Information Security Policy on each campus.</td>
</tr>
</tbody>
</table>
| Chief Security Officer            | • Provide leadership in directing and governing the campus Information Security Program.  
• Ensure development of a consistent set of IT risk controls and security solutions, including, but not limited to the security controls identified in this policy.  
• Provide consistent alignment and interpretation of regulatory requirements associated with Information Security Policies, standards, and processes.  
• Provide oversight of a risk-based security monitoring program. |
| Chief Privacy Officer             | Represent the privacy interests of constituents during the creation and implementation of this and related policies.                             |
| Unit Executive Officer            | Accountable for compliance with Information Security Policies and Standards within responsible domain. Unit Executives are responsible for the uses of their local area networks and all devices connecting to campus or University networks through their local area network.  
• Ensure participation in governance forums for reviewing information security policies, standards, and procedures.  
• Typically a Dean and/or Department Head. |
Principles

The objectives guiding the creation and implementation of this policy are:

- Privacy - Ensure that the use and protection of personally identifying information respects individual privacy.

- Confidentiality - Identify and protect information that is considered to be confidential or private and ensure that it is not disclosed to unauthorized parties.

- Integrity - Ensure the soundness of the information (i.e., it has not been inappropriately created, modified, or deleted).

- Availability - Ensure information is present, accessible, and able to be used.

- Accountability - Ensure that all actions taken with or performed on data can be tracked to specific individuals.

- Assurance - Ensure that security policies are met.

These objectives encompass the application of the following principles:

- Respect for Academic Freedom.
  No aspect of this policy is intended to diminish this principle or its execution.

- Individual Responsibility
  The responsibility for information security is one that is born by every member of the campus community; in particular, individuals given privileged access to data will be held accountable for the use and protection of this data.

- Shared Governance and Campus Fraternity
  Each campus is a stakeholder in the other campuses' practices and implementation of this policy. Significant modifications to campus standards and implementation policies must be vetted by the UTMT Security Working Group.

- Least Privilege
  Individuals, systems, and business processes will be granted only the minimum access rights necessary for the completion of University functions.

- Multiple Overlapping Security Controls
  Security controls will be implemented in a redundant fashion such that, wherever possible, the failure of any single control will not result in the exposure or compromise of University assets.

- The Use of Compensating Controls
  In situations where a preferred or optimal security control cannot be met, alternative means for controlling risk will be explored and implemented.

- Education
  Effective policy requires a concerted education program to bring awareness of policy and the tools for compliance with it.

Accountability

Accountability as a security control objective means that we take responsibility for our individual actions as well as the management and stewardship of the University information resources and other assets entrusted to our care.
Accountability allows controls to be focused where needed based upon the sensitivity of data. Within the academic environment, ensuring accountability helps:

- protect individuals from violations of their privacy
- guarantee the accuracy of information such as grades or degrees
- prevent the theft or loss of intellectual property

Accountability, however, must be informed by consequences of academic freedom and a growing awareness that maintaining privacy takes on a new urgency in our highly networked world. Though few or no legal protections exist that protect the privacy of University business from agents of the University, collectively the Chief Information Officers must ensure that the implementation of this policy creates accountability at an individual level. Further, that the information necessary to do so is used only as required for the provision of services and the prevention, response, and remediation of security incidents.

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.

Auditability

All controls should be implemented in a fashion that is auditable, providing transparency in the validity and reliability of the protection of information assets. Well designed and implemented controls should allow consistent independent evaluation of the controls' effectiveness.

Compliance

This security policy and all campus implementation security policies and standards are written with specific and precise language intended to ensure that the policies and standards contain identifiable and auditable requirements that facilitate compliance.

Unit Executive Officers are responsible for ensuring compliance with this policy within their units.

All University agreements that engage contractors or vendors are responsible for ensuring that service agreements covering outside service providers include provisions requiring protection appropriate with the sensitivity of the information. Outsourced services must provide at least comparable degrees of security as the information involved would receive from campus provided services.

Exemptions

There will be no exemptions granted to the principles outlined in this policy. However, as discussed above, in situations where strict adherence is not possible, control objectives may be met through the use of compensating controls. Exemptions to use compensating controls must be reviewed by the Chief Security Officer and may only be approved by the Chief Information Officer appropriate for the unit requesting the exemption. Each Chief Security Officer must produce guidelines for the appropriate use and development of compensating controls. A permanent record of the exemption must be maintained by the approving Chief Information Officer.

Controls

The following control objectives shall be addressed by implementing policies, standards, and guidelines.

Information Risk Assessment

An Information Risk Assessment examines essential functions of an organization, identifies key information assets that the function depends upon, and assesses the impact from unauthorized use, disclosure, modification, or destruction.

- A periodic assessment shall be performed of essential business functions to identify key information assets.
• A Risk Management Plan shall be developed that identifies controls over information assets and mitigation of risks to acceptable levels.

Information Classification

It is essential that all University information 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.

All University data will be classified into one of the following four classes:

• Highly Sensitive - Information that if disclosed or modified without authorization would have severe adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information in this class includes, but is not limited to:
  • Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, such as credit card information (covered by PCIDSS)
  • Covered by federal and state legislation, such as HIPAA or the Data Protection Act
  • Payroll, personnel, and financial information with special privacy requirements.

• Sensitive - Information that if disclosed or modified without authorization would have serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information that is covered by FERPA, Non-Disclosure Agreements (NDA's), and other intellectual property are, as a minimum, in this class.

  note: Non-Disclosure Agreements may fall into the Sensitive or Highly-Sensitive categories and should be individually evaluated.

• Internal - Information that if disclosed or modified without authorization would have moderate adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

• Public - Information intended for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

Data owners and data stewards shall be identified for all information assets. It is the responsibility of the data owners and stewards to perform a risk assessment to determine appropriate classification of information. Information assets shall be protected appropriately during storage, transmission, retention, recovery, and destruction.

The University will maintain a catalog of categorized data elements and include this in its security awareness training. Each campus will, in collaboration with the data stewards, develop policies and standards that address the creation, maintenance, and destruction of information assets as appropriate to the information's security classification.

Identity and Access Management (IAM)

Identity proofing and credentials are fundamental to properly manage access to information assets commensurate with the sensitivity level. Proof of identity can range from none, to presentation of a valid i-Card or a official government Passport. Credentials can range from passwords to biometrics.

• Appropriate proof of identity shall be required of individuals before being granted access to information assets at the University.
• Identity management systems must retain a record of the type(s) of credential(s) used to validate identity.
• Unique computer account Identity (traditionally the netid) for an individual shall be created and assigned based on the proof of identity.
• University systems shall require appropriate credential verification before allowing access to information assets.
• Periodic reviews shall be performed to ensure that only authorized individuals are granted access to information assets.
We originally included something here to reflect the requirement that passwords will change regularly as appropriate but now recognizing this as belonging to a standard, have removed it.

- Guest access credentials for University information resources will be subject to the same controls as ordinary identity credentials.
- Guest access credentials must be valid for a finite period of time as defined in the campus standards.
- Guest access credentials must be traceable to a specific individual at all times.
- Anonymous access to services will be strictly limited to information assets of the public data classification.
- The University reserves the right to examine for the purposes of verification and adherence with policy all credentials provided for access to electronic systems.

**Portable Computing Devices**

Information stored on mobile computers (such as laptops and netbooks), Personal Digital Assistants (PDAs), cell phones, and other digital media (such as USB storage devices) present significant risks for the University.

- University information assets shall not be transmitted or stored on portable computing devices unless sufficient controls are in place to protect the information in the event of theft or other loss of the portable computing device.
- If data encryption is employed as a protection mechanism, appropriate key management practices shall be implemented to ensure the University's ability to recover information as necessary.

**Remote Computing Services**

When information assets are accessed from locations remote from the University networks, extra precautions need to be implemented to ensure information is protected similar to trusted University network access. A Remote Computing Service, such as a VPN, SSH, or remote desktop connection must meet the following generic criteria.

- User access to a Remote Computing Service (RCS) shall be securely authenticated and should log user, date, time, and duration of access.
- All data transmitted over an RCS shall be secured to levels corresponding to local access.
- Access to an RCS shall only be permitted from remote computing platform meeting approved security levels.

**Infrastructure / Network**

The network infrastructure is the foundation for all electronic communications and computing on campus. Maintaining the integrity of the network itself and the devices attached to it are essential to maintain a secure environment for the University.

- All devices connected to the University network must be maintained on a regular basis to ensure that they are current on all security related patches.
- Each organizational unit will implement a change control process for any portion of the Network Infrastructure
- Each organizational unit with infrastructure responsibilities will document its network security architecture
- Periodic audits of infrastructure and general network security configurations must be performed
- Wireless network access will only be allowed to authorized individuals and must be trackable to a specific individual.
- Wireless network traffic must be encrypted for all staff, faculty and students.
- Any device connecting to the network must comply with all campus policies and standards
- Access to the University network should be allowed only to authorized users or machines.
- Log(s) of network access must be maintained to insure accountability according to campus standards.
- The use of the University network to perform any criminal action is strictly prohibited.
- The deliberate introduction of malware or use of University resources to improperly access local or remote computing resources is prohibited.
• Monitoring of the network and computing environment for its general health must be performed sufficient to meet the requirements of this policy.
• Network interfaces must be configured in a secure fashion that maintains the integrity of the originating subnet information (e.g., anti-spoofing).

Physical Security

Personnel safety and physical protection of information assets both are important aspects of physical security. Where possible, physical security controls to protect information assets should be leveraged for personnel safety.

• Units must implement safeguards such that information assets within their department are protected from physical access by unauthorized individuals, and that environmental safeguards are in place to protect the confidentiality, availability and integrity of the protected information as commensurate with data criticality and risk assessment.
• The campuses will develop standards that identify what types of information assets must reside in a Data Center.
• Every Data Center shall establish a Physical Facility Security Plan that addresses restricted access, environmental safety, asset inventory/control, and backup, recovery and disposal of assets.
• Personnel with access to a Data Center must be provided appropriate notice and/or training regarding their responsibilities.
• Portable Computing Devices should be secured to prevent theft when unattended. (See Portable Computing Devices control)
• Procedures for the proper disposal of data storage equipment that minimized the likelihood of data disclosure, loss, or theft must be documented, maintained and enforced.
• Printed materials and computer media shall be protected commensurate with the sensitivity of the information they contain.

Education & Awareness

• Each campus will have an Appropriate Use Policy that provides guidance to campus personnel who utilize University data assets, computer data systems, and electronic communication regarding their appropriate use.
• Periodic training on information security must be provided to faculty and staff
• Formal communication to faculty, staff, and students about information security policies and standards must be made

Purchase of Computer Products and Services

The pervasive nature of information security issues requires that security is considered during the purchase process for computer systems, software, or services. This obligation falls to the unit acquiring information technology systems or services. Units are further encouraged to engage the relevant security office for assistance or guidance.

• Acquisition of Computer systems shall include consideration of the intended operating environment to ensure it will meet security requirements.
• When purchasing services of third-party service providers, evaluation of their protection mechanism shall be performed (including SAS 70 review, if appropriate).
• Any export control restrictions on computer technology shall be identified before purchase and an Export Protection Plan developed when appropriate.
• Appropriate security requirements shall be included in all Requests for Proposals.
• Security domains that must be addressed in all contracts for electronic services include (but are not limited to): data protection, Intellectual property protections, notification in cases of security incidents involving the University's data, and defined use or limits thereof involving University data or members of the University community.

Telecommunications

Modern telecommunication systems are often integrated or intermingled with computer data systems. Care must be exercised to protect the telecommunication systems in the networked computing environment.
• Enterprise VOIP shall insulate its system components from general data network computing environments.
• Peer-to-peer VOIP systems on University workstations and laptops shall be managed to protect against data compromise.
• The installation and use of VOIP servers shall be approved by the organization's CIO.

Disaster Recovery, Business Continuity, Data Retention

• Disaster Recover Plans (DRP) and Business Continuity Plans (BCP) shall address the secure recovery and operation of information services.
• Data retention policies must be established by the appropriate data stewards.
• All information assets must be accessible by at least two authorized individuals.
• If data encryption is employed as a protection mechanism, appropriate key management practices shall be implemented to ensure the University's ability to recover information as necessary.

Record Keeping and Reporting of Security Incidents

• Each CIO shall establish an Incident Response capability with designated resources and procedures.
• The CIO's shall track significant security incident activities.
• The UTMT shall periodically publish statistics on security incidents.

Application Development

• Computer applications developed by or for the University that will access sensitive or highly sensitive information must identify the security protections it is implementing.
• Computer applications that create, read, update, or delete data classified as sensitive or highly sensitive must be formally assessed for security sufficiency before being placed into production.
• Secure development practices must be codified by each campus.

Transfer of Information Custody

• University personnel that receive information from authorized individuals shall protect the information in accordance with the original protection requirements.
• Before information assets are transferred to non-University entities, agreements shall be established to protect the information assets after transfer.
• Agreements for protecting transferred University sensitive and highly sensitive data shall be approved by University Counsel before transfer.