Approved for referral
to the Academic Senate
9-27-11

Memorandum

To: Interim President Lorris Betz

From: Eric Denna, Chief Information Officer. University Information Technology

Date: September 12, 2011

This is a proposal to revise University of Utah Policy 4-004 regarding the implementation of a sound information security program. This Policy applies to all staff, faculty, students and others affiliated with the University of Utah.

The proposed revisions reflect changes in Information Security requirements and regulations since the latest extensive revision of the Policy in 2004. They also reflect the University's adoption by the Information Technology Council of the ISO 27002 standards. These standards are considered the international best-practices for information security and have been mapped with US standards, such as those developed by the National Institutes of Standards and Technology.

The Policy would also be rewritten to reflect the new regulation approach adopted by the University. That is, the Policy will now be focused on high-level requirements. Additional Rules, Procedures, and Guidance will subsequently be developed to for details of implementation of the Policy. We are *not* proposing any changes to existing University Rule 4-004A (PROTECTED HEALTH INFORMATION DATA BREACH NOTIFICATION RULE), which is associated with this Policy. The Rule 4-004A was established to ensure compliance with federal regulations regarding information security breach notifications and will remain in effect and unchanged until further notice.
http://www.regulations.utah.edu/it/rules/rule4-004A.pdf

The proposed revisions to Policy 4-004 have been approved by myself, after being reviewed and approved by the Campus Information Technology Council at their meeting on February 10, 2011, and by other Stakeholders as recommended by the Institutional Policy Committee and the committee that worked on the policy.

For further information, please contact Kevin Taylor Director of Planning and Policy, at 585-3314.

If you approve of this proposal, it will then be forwarded to the Academic Senate Executive Committee for its review. It will be recommended that the Executive Committee classify this as a Policy that does *not* "directly or significantly affect the University's academic missions," under U-Policy 1-001, and therefore should be treated as an item for the "information" rather than the debate and approval of the Academic Senate. It should then be forwarded to the Board of Trustees for final approval. It is proposed that this Policy become effective immediately upon approval by the Board of Trustees.

Memorandum

To: Eric L. Denna, Chief Information Officer

From: Kevin Taylor, Director, Planning and Policy

Date: September 12, 2011

RE: Revision 3 of University Policy 4-004 (University of Utah Information Security Policy)

Attached for your consideration and approval is a proposal for a revised University Policy 4-004, University of Utah Information Security Policy.

The proposal has been reviewed by the University Institutional Policy Committee (IPC), the Information Technology Executive Committee, the Office of General Counsel, the campus Information Technology Council, University of Utah Health Sciences and Hospitals and Clinics leadership, and various stakeholders identified by the IPC.

A “Hitchhiker's Guide” to Policy 4-004: University of Utah Information Security Policy. Revision 3

Old Version (Policy Sections)	New Version (Policy Sections)	
Campus Protect private sensitive information Preventing loss of critical resources	Users All of us have responsibility for preventing unauthorized access to IT resources and data	
	Security Liaisons VP level responsibility for coordinating security and privacy related activities	
Users No private sensitive Info on personal computers without permission Defines sensitive info that does not require permission	Info Security & Privacy Advisory Committee – sub-committee of the campus IT Council. Represent end-user interests when developing policies and rules for IT security and privacy	
Prevent loss of "critical resource" by implementing security as required by UIT.	Implementing security as required by policy, based on risk, and as required by University Leadership.	Risk Assessment Define and prioritize risks and conduct risk assessments if things change
		Data Management Protect confidential information Restricted data cannot be stored unless 1) need, 2) VP/steward permission, 3)compliance Classify data as Public / Sensitive / Restricted Handle data according to classification
		Access Management Authorization by need to know, relation to job requirements
		Change Management When system changes occur, a security review should take place.
		Physical & Environmental Security Lock stuff up and protect it from, break in, power outages, fire, disasters, etc. If HIPAA, document repairs
		IT Resource Security Protections should be commensurate with risk. Anti-virus/malware, security patches Time-out with no activity on a system Configure to minimize risk Check logs for suspicious activity

		Cooperate with central Security to perform penetration test, intrusion detection
		Remote Access Privacy and security policies apply wherever you are.
		Vendors and Third Party access to data OK with an agreement in place. All policy applies to them.
		Network Security Manage access commensurate with risk. Protections in place between campus and other networks.
		Log Management & Monitoring Record and monitor security incidents, events, weaknesses. (Log data does not include content) Must follow Policy 4-002
		Backup and Recovery Backups- user, application, system levels. Test ability to restore from backups
		IT Resource Media Handling Protect data regardless of media Store media in controlled areas, make sure off-site storage is secured at same level as on-site. Media to be transported by authorized personnel.
		Business Continuity and Disaster Recovery Planning Have a plan in place to ensure University operations can continue when IT resources are impacted or unavailable.
Security Breaches Must be reported Assess level of threat of compromised data Notify individuals whose data has been breached	Information Security Incident Management Must be reported Assess level of threat of compromised data Notify individuals whose data has been breached when risk threshold reached Respond to security events and disseminates remedies and preventative measures	
Incident Response Team Responds to security events and disseminates remedies and preventative measures		

Not referenced in existing policy.	Information Security Awareness and Training Staff, faculty, students should be aware of basic threats to data. Staff, faculty, students should be provided with routine education on how to protect data.
	Exceptions to Policy Data stewards may review and grant exceptions to the policy.
Sanctions Discontinue IT service to violators if violation threatens other resources Users may lose access if they individually violate policy Disciplinary action defined in other policies Appeal procedures defined in other policies	Violations Discontinue IT service to violators if violation threatens other resources Users may lose access if they individually violate policy Disciplinary action defined in other policies Appeal procedures defined in other policies
IT Systems Administrator Performs day to day operations under direction of the Custodian	IT Resource Administrator The individual who has day-to-day operational responsibility for an IT resource. Implements security as required by policy and under the direction of a data steward or designee.
University Information Security Office Reports to CIO and ITC Develops, educates, assists, implements, monitors audits security “best practices”	Moved to the definitions section of the new policy.
OIT (not University IT) Manages and maintains campus backbone network	Removed
IT Resource Steward Overall responsibility for IT resources in a particular domain Assess risks Determine appropriate access Comply with federal and state laws	Removed - role conflicted with the data steward role in data management policy.
IT Resource Custodian Implements security measures in a particular domain Prepares for disaster recovery Monitors traffic to identify security events Implements Data Steward directions	Removed - role conflicted with the data custodian role in data management policy.