



University of Utah
Information Technology
Security Plan

September 11, 2003

Executive Summary

The management and operation of the University's information technology systems and networks is extremely distributed. This distributed environment presents unique security challenges, many of which can only be satisfied through centralized coordination and the collaboration of a broad campus constituency.

This plan was developed, in part, to address issues identified in security audits that were conducted in 1995 and 1999. Many of the issues that were raised in the audits have already been addressed with the establishment of the University's Institutional Security Office (ISO) and policies and procedures managed by ISO. This plan moves beyond the reactive state that was a result of the aforementioned audits, moving proactively into the future.

The University's Integrated Information Technology Plan addresses general issues of broad campus-wide impact. Issues addressed therein were selected by consensus among campus organizations. It outlines strategic goals and projects to address security and identity management issues including directory centralization and synchronization, authentication and authorization, and digital approval methods. This plan is more granular and breaks broad strategic initiatives into tangible and tactical security projects.

Needs Assessment

Specific IT security needs have been identified by the 1995 and 1999 audits, and the subsequent experience of ISO and the campus IT community. These needs include:

1. Definition of risk assessment criteria and consistent security and disaster recovery plans.
2. Adoption and documentation of accepted industry practices, minimum security requirements and best practices, including current "fixes" and "patches."
3. Availability of basic tools (hardware and software) to ensure the adoption of minimum security requirements and best practices.
4. Security awareness, orientation and training for faculty, staff, and students and IT professionals.
5. Development of audit requirements, self-audit procedures/guidelines, and clear lines of authority for enforcement of security policies.
6. Design of a comprehensive campus security system(s), including perimeter, network backbone, and edge security, system/network monitoring capabilities, and secure physical facilities including network hubs and wire closets
7. Continued development of centralized directory resources, meta-directory and password synchronization systems, and roles based authentication/authorization capabilities.
8. Adoption of electronic approval methods and the introduction of a central certificate authority.
9. Improvement of password transmissions security and adoption of a consistent password policy.

Business Case

The University must balance appropriate business practices with the freedom of information that is required in a University setting. However, if academic freedom is not properly balanced with proper security safeguards, then the University could suffer dire consequences.

The University is an information center. The University's information assets must be protected in order to ensure continuation of the University's core education and research missions. Security breaches can result in identity theft, loss of database information, loss of research data, defacement of University web sites, the loss and/or corruption and destruction of information resources, and the inability to continue the essential operations of the University.

The University faces a very real threat of financial loss that could result from the loss of intellectual properties. Legal risks become significant with the requirement to protect the privacy of patient records. The University stands to suffer significant loss of reputation if security breaches are not minimized.

The University cannot afford to defer security plans and projects.

Strategic Plans

1. Formulate and maintain an IT disaster recovery plan for the University. Develop criteria for performance of IT resource risk assessments based on information resource sensitivity and criticality.
2. Develop, update, and publish IT security best practices. Best practices will include minimum security requirements to protect assets that reside on specific computing platforms as well as to protect critical and sensitive information. Provide access to security tools and technologies outlined in best practices and minimum security requirements.
3. Strengthen University wide security architectures: Intrusion Prevention; Intrusion Detection; Incident Response; and Policy Compliance. Proactively engineer security into developing applications. Audit applications and systems for compliance and changing technologies.
4. Elevate understanding of security and privacy issues through awareness and education tailored to target populations: University administration; faculty and staff; students; and IT managers.
5. Develop comprehensive Identity Management infrastructure, processes and tools.

Operational Plans

Security Guidelines and Procedures

<p>1. Publish and monitor a set of minimum (baseline) security requirements for networked devices, services and applications.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: Draft requirements are available on www.iso.utah.edu. These need to be taken from draft to OIT policy. The collection of requirements needs to be reviewed for completeness.</p>
<p>2. Publish a set of security best practices for: operating system configurations, authentication services, network service applications, certificates, encryption, network devices.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: Some best practices published on www.iso.utah.edu. Need to coordinate with specific manager groups. The collection of best practices needs to be reviewed for completeness.</p>
<p>3. Publish a set of best practices for access and privacy including: standards for role based authorization, authentication based on risk, and procedures for handling sensitive data, passwords and identity management .</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: Not started.</p>

Security Infrastructure and Implementations

<p>1. Implement a campus network level Intrusion Detection System incorporating automated reporting.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: IDS system in place on the network, automated reporting in beta phase.</p>
--	---

<p>2. Architect NetFlow processing for accessibility, reliability, and access to real time flows. Enhance tools available for analyzing flow data.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: NetFlow have been used for some time – new architecture has been determined</p>
<p>3. Supplement intrusion technology with appropriate stealth technologies such as ‘tarpit’ or ‘honeypot’.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: Conceptual phase.</p>
<p>4. Implement campus network level perimeter security incorporating firewall and router ACL technologies. Evaluate and recommend ‘edge’ firewall technology.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: ISO, NetCom, ITAC and the Network Research Forum all have projects in progress architecting and evaluating solutions.</p> <p>Router ACLs are in place and reviewed periodically by ISO.</p>
<p>5. Automate vulnerability assessment and policy compliance.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: Mail Relay probes in place since 2000 and very successful.</p>
<p>6. Ensure that security tools are available to all campus organizations and individuals. Including: Anti-virus, Data Integrity, Patch management.</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: Volume purchase agreements have been made with NAI and TrendMicro for anti-virus software.</p> <p>A campus-wide TripWire license is in effect.</p> <p>Needs assessment for Patch management is underway.</p>

Incident Response

<p>1. Formalize Incident Response Team roles and responsibilities. Publish protocols for handling incidents.</p> <p>Completion:</p> <p>Lead: Dave Huth, ISO Staff</p>	<p>Status: Incident Response Team has been active since 1998 and is successful. Protocols being drafted for publication.</p>
<p>2. Develop an incident tracking and reporting system.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: In progress utilizing NetCom's Remedy help desk system.</p>
<p>3. Coordinate with NetCom the development, accurate population and maintenance of the POC database.</p> <p>Completion:</p> <p>Lead: ISO Staff</p>	<p>Status: In progress.</p>
<p>4. Coordinate the ability to generate lists that target appropriate populations.</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: Not Started.</p>
<p>5. Formalize relationships with legal/enforcement entities</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: Not Started.</p>

Training and Awareness

<p>1. Train campus IT administrators on the proper use of ISO supported security tools.</p> <p>Completion:</p> <p>Lead:</p>	<p>Status: Conceptual phase.</p>
---	----------------------------------

<p>2. Develop and deliver security awareness packages for: IT professionals; University administrators; faculty, staff and students.</p> <p>Completion:</p> <p>Lead:</p>	<p>Status: Conceptual phase. ISO continues to speak at group meetings and post alerts to campus lists.</p>
<p>3. Implement standard reporting mechanisms for security alerts, updates and current campus activity.</p> <p>Completion:</p> <p>Lead:</p>	<p>Status: Conceptual phase.</p>

Services

<p>1. Security auditing and vulnerability assessment.</p> <p>Completion:</p> <p>Lead:</p>	<p>Status: Auditing in progress for ecommerce sites. Documents for self audit being prepared.</p>
<p>2. Security architecture and design.</p> <p>Completion:</p> <p>Lead:</p>	<p>Status: Ongoing consultation service.</p>
<p>3. Risk assessment, security plan and disaster recovery.</p> <p>Completion:</p> <p>Lead:</p>	<p>Status: Documents to support the security policy in progress. Service in conceptual phase.</p>

Identity Management and Middleware

<p>1. Coordinate institutional (meta) directory development supporting core and departmental applications.</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: In progress.</p>
--	-----------------------------

<p>2. Coordinate authentication technologies.</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: In progress.</p>
<p>3. Develop mechanisms for authorization based on directory information.</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: Conceptual phase.</p>
<p>4. Define PKI certificate content and policy. Develop mechanisms to deploy server side certificates. Develop mechanisms to deploy University internal digital certificates.</p> <p>Completion:</p> <p>Lead: Dave Huth</p>	<p>Status: In progress.</p>