POLICY MANUAL

OPERATING POLICIES AND PROCEDURES

Number 558
Subject: Protecting Private Sensitive Information and Critical Institutional Data
Effective Date: March 31, 2010

558.1 PURPOSE

The intention of this policy is to protect Utah State University's Private Sensitive Information (PSI) and Critical Institutional Data (CID) while stored on or transmitted by institutional information technology resources, and to recognize the applicable issues of the Utah State Board of Regents Policy R345, Information Technology Resource Security.

558.2 POLICY

- Utah State University (USU) and its colleges, departments, and divisions, must take measures to protect Private Sensitive Information (PSI) and Critical Institutional Data (CID) that are stored, processed or transmitted using institutional resources.
- All computers and other IT Resources that are used to display, process, store or transmit PSI or CID must be maintained by support technicians who have ongoing HR job responsibilities for those resources, in compliance with the Computer Management Policy 551 to reduce the likelihood of vulnerability. These technical support personnel may be employed in departments or in the Office of Information Technology (OIT).
- USU requires all employees, contractors, consultants, vendors and students:
    - to follow best practice protection of the USU IT Resources they use to store, process or transmit information. Protection from both electronic and physical compromise or loss is required. Some uses of equipment may be prohibited because of the exposure risks they introduce to PSI being processed on the same equipment (e.g. web browsing, free program installations, downloading, instant messaging, remote logins, which may

introduce unexpected or hidden malware.) See also Computer Management Policy 551.
    - to report to the OIT ServiceDesk or the OIT Security Team, all evidence or suspicion of network intrusion attempts, information security breaches, and other security related incidents perpetrated against University data and information resources. See also Network Monitoring & Vulnerability Scanning Policy 555.
- USU requires that the transfer of PSI to end-user equipment be restricted to necessary circumstances. When PSI is transferred it must be protected by encryption or other measures.
- Offsite storage, processing or backup of PSI/CID must use service providers evaluated and approved by the responsible data steward in consultation with OIT. OIT is directed to publish standards that conform to this policy.
- The following roles and responsibilities are established for protecting and preserving the University's PSI and CID:
    - **Data Trustees** are University Administrative Officers (President, Provost, Vice Presidents, etc) who have top-level responsibilities for databases used within their divisions. The responsibilities of Data Trustees include: designating data stewards, establishing office practices that will protect and preserve the PSI and CID collected and/or used in their units, and defining policies and procedures that support and require best practices.
    - **Data Stewards** are management level officials (Controller, Registrar, Directors, Managers, etc) who have direct operational level responsibility for specific databases that may contain PSI and/or CID. Data Stewards are responsible for: coordinating with Data Trustees, classifying specific data as PSI or CID, authorizing specific data users to access databases as needed for their job functions, and enforcing the policies, procedures and office practices that apply to their specific databases
    - **System Administrators** are IT professionals who manage computer systems or software which store, process or transmit information. They are responsible for the data preservation and security features of their computer systems.
    - **Data Users** are Faculty, Advisors and other staff who examine data, including PSI and CID, as part of their duties. Data Users must protect against unauthorized duplication or release of PSI as well as loss or corruption of CID from their user-controlled equipment.
- Upon discovery or notification of a security incident, the OIT Security Team will promptly and systematically investigate and escalate, remediate, or collaborate with other units to resolve the issue.
- The OIT Security Team shall establish procedures for convening an Incident Response Team to respond to security breaches that may expose PSI or destroy CID.
    - Each incident will be documented as part of the incident response, providing a general description of events, approximate timelines, parties involved, resolution of the incident, external notifications required and recommendations for prevention and remediation. To protect

confidentiality and promote identification of perpetrators, any external notification about an incident must be handled by Public Relations & Marketing after approval by the CIO/VP for IT and the Office of Risk Management in consultation with the President's designee.

- If an incident is judged by the Security Team, in consultation with available administrators, to be a critical threat to the confidentiality of data and/or the integrity of Information Resources, OIT is authorized to take immediate action to eliminate the threat in accordance with the Network Monitoring and Vulnerability Scanning Policy (#555). This action may include the interruption of service, denial of access, or removal of systems from the network while the incident is being resolved. Such actions will be reported to the CIO/VP for IT and the affected members of the university community. Business continuity will not take precedence over the actions required to control a critical security incident. Losses due to a security incident must be weighed against losses due to interruption of services to the university community in assessing the criticality of a threat.

- When IT Resource media are being disposed or recommissioned, industry standard procedures for thorough obliteration of PSI from electronic media must be employed by the media owner/user or by USU Resource Recovery.
- USU does not accept liability for PSI that is transmitted through, or stored on, IT Resources by the end user for non-university related purposes.
- Employees whose job duties involve PSI or CID must complete annual training on these policies and subsequent procedures. Training will be provided by OIT in conjunction with the Office of Human Resources training program.

558.3 GRIEVANCE

- **Private Sensitive Information (PSI)** - any information that might result in a loss to its owner if the information was obtained by someone with unknown trustability or malicious intent. PSI includes but is not limited to, the owner's name in combination with any of: Social Security number, birth date, access passcodes, academic record, medical history, and financial matters. PSI is owned by the individual, not by USU. This policy is concerned with private sensitive information only if it is required or requested by USU and stored or transmitted on USU IT Resources.
- **Institutional Data** - any information that is generated or acquired, stored and required for the continued function of USU, including but not limited to: academic records, employment records, financial records, schedules, etc. Institutional Data is owned by USU (except for information that is also PSI).
- **Critical Institutional Data (CID)** - any USU institutional data that cannot be regenerated from readily available sources if corrupted or lost and is necessary for the function of USU. CID may be private or public.
- **IT Resource** - any electronic equipment, infrastructure or software used to transmit, process or store digital data or information. This policy is concerned only with IT Resources owned or leased by USU or privately owned client-side equipment that is directly connected to USU IT infrastructure. IT Resources

include, but are not limited to: servers, network wiring, routers, switches, wireless access points, desktop, laptop, handheld and other portable client equipment and peripherals such as printers, scanners, web cameras, as well as programs and operating systems used on any of that equipment. For the purposes of this policy "IT Resource" does not include the data (PSI, CID or other) that is transmitted, processed or stored on the IT Resource.

- **Critical IT Resource** - any IT Resource which, if it fails to function when needed, would cause an unacceptable disruption to mission critical academic or business services of USU or expose USU to liability. Examples include: the wired network, the telephone system, the enterprise administrative computing system (Banner), etc.
- **Compromise** - loss of exclusive, authorized control of an IT Resource to an unauthorized person or to unauthorized software resulting in exploitation, control and/or use of the IT Resource beyond USU's purpose or intent for that IT Resource.
- **Vulnerability** - the lack of adequate controls to prevent an IT Resource from becoming compromised. A weakness in a system allowing possible or actual unauthorized action.
- **Server** - a computer used to provide services or data to multiple users.
- **Security** - the process of managing risks to prevent or reduce loss.
- **Security Breach** - an identified compromise which exposes PSI to unauthorized access or an IT Resource to unauthorized use.
- **Incident Response Team** - an ad hoc team of specialists convened to investigate the causes of a security breach or other data exposure event, to evaluate the extent and cost of a loss, and to formulate corrective actions to prevent recurrence.
- **Disaster Recovery Plan** - a plan to restore the function of USU IT resources and appropriate access to critical institutional data after a disaster which has damaged or disabled existing systems for those functions and access.
- **Unauthorized Access** - access to a USU IT Resource or to USU data that is outside of the approved uses.
- **Appropriate Use Policy** - a statement of the allowed and proscribed uses of USU IT Resources.