

ENTERPRISE INFORMATION SECURITY POLICY

Status: **Active**
 Effective Date: January 5, 2013
 Revised Date: January 5, 2013
 Approved By: Mark VanOrden, CIO
 Authority: UCA 63F-1-103; Utah Administrative Code R895-7 *Acceptable Use of Information Technology Resources*; Utah Administrative Code R477-11 *Discipline*

2.1 Purpose

This policy provides the foundation for the State of Utah, Department of Technology Services enterprise security policy. The scope of the enterprise security policy is based on the 18 security framework domains defined in the State of Utah security control framework as listed below:

State of Utah - Security Framework Domains	
2.3.1	Security Planning
2.3.2	Program Management
2.3.3	Risk Assessment
2.3.4	Security Assessment and Authorization
2.3.5	System and Services Acquisition
2.3.6	Awareness and Training
2.3.7	Configuration Management
2.3.8	Contingency Planning
2.3.9	Incident Response
2.3.10	Maintenance
2.3.11	Media Protection
2.3.12	Personnel Security
2.3.13	Physical and Environmental Protection

2.3.14	System and Information Integrity
2.3.15	Access Control
2.3.16	Audit and Accountability
2.3.17	Identification and Authentication
2.3.18	System and Communication Protection

The Security Framework includes requirements from the following sources : NIST (National Institute for Standards and Technologies, HITECH (Health Information Technology for Economic and Clinical Health), HIPAA (Health Insurance Portability and Accountability Act), PCI (Payment Card Industry), NACHA (The Electronic Payments Association), FERPA (Family Educational Rights and Privacy Act), HITRUST (Health Information Trust Alliance) and Agency Policies. See **Section 2.2** for a description of each of these standards and regulations.

2.1.1 Background

This policy was developed in response to a comprehensive external audit involving all executive branch agencies and the enterprise network. The audit revealed security deficiencies not properly addressed in previous policy and standards documents. Due to the scope and complexity of implementing the policy changes presented in this document, a time provision has been granted under which executive branch agencies and the Department of Technology Services may not be fully compliant in all aspects between the date of approval and the date compliance can realistically be met.

State agencies and the Department of Technology Services are expected to achieve full policy compliance with this document on or before October 31, 2014. The Enterprise Information Security Office will coordinate compliance efforts and maintain a list of compliance deficiencies during the transition period indicated above.

The Enterprise Information Security Policy will develop and establish essential and proper controls to minimize security risk; to meet due diligence requirements pursuant to applicable state and federal regulations; to enforce contractual obligations; and to protect the State's electronic information and information technology assets.

2.1.2 Scope

This policy applies to all agencies and administrative subunits of state government as defined by UCA §63F-1-102(7), et seq.

2.1.3 Exceptions



The Chief Information Officer, or authorized designee, may acknowledge that under rare circumstances, some associates may need to employ systems that are not compliant with these policy objectives. The Chief Information Officer, or authorized designee, must approve in writing all such instances.

In such instances, a security justification for non-compliance must be established and the request for exemption must be approved in advance through a risk acceptance process. This risk acceptance process requires approval by the Chief Information Officer.

[Risk Acceptance Procedure and Exemption Request Document](#)

2.2 Definitions

Agency Policies

Departments and agencies under the State of Utah have the authority to establish internal policies related to information security objectives specific to the department or agency. Agency policies must be compatible with enterprise security policy, as well as federal and state statutory regulations.

Availability

The availability of system and data access for approved users and business processes is one of the primary objectives of the information security triad; including confidentiality, integrity, and availability.

Confidentiality

The confidentiality of data and protected information is one of the primary objectives of the information security triad; including confidentiality, integrity, and availability.

Encryption

Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state.

FERPA

Family Educational Rights and Privacy Act

HIPAA

Health Insurance Portability and Accountability Act

HITECH

Health Information Technology for Economic and Clinical Health

HITRUST

Health Information Trust Alliance



Information Asset

All hardware, software, processes, and data used in the State of Utah operations.

Information System Resource

All network devices (routers, switches, firewalls, etc.), operating systems, database management systems, or applications used to manage or control access to State of Utah electronic information.

Integrity

The integrity of data and protected information is one of the primary objectives of the information security triad; including confidentiality, integrity, and availability.

NACHA

The Electronic Payments Association

NIST

National Institute for Standards and Technologies

PCI

Payment Card Industry

Public Networks

Networks that are shared by multiple unrelated users and where physical access to the infrastructure is not controlled by the State. Typically, these networks are considered untrusted. The Internet is the largest public network.

Risk Assessment

A process by which risks are identified and the impact of those risks determined. Additionally, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.

Secure-Coding Methodology

Programmatic efforts implemented to identify and minimize vulnerabilities related to software development and data processing.

2.3 Policy

2.3.1 Security Planning

Summary: The objective of system security planning is to improve the protection of information system resources. All State of Utah information systems have some level of sensitivity and require protection. The protection of an information system will be documented in a system security plan.

Purpose: The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.

Policy Objectives: The Department of Technology Services will document all information systems annually and coordinate with agency IT Directors to develop and implement a Security Plan for each system consistent with National Institute of Standards and Technology, Special Publication 800-18 Revision 1 and Special Publication 800-53 Rev3 PL-2 (Appendix F, Page F-85).

Security Control Standards:

[NIST SP 800-53 Rev3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST SP 800-18: Guide for Developing Security Plans for Information Systems](#)

2.3.2 Security Program Management

Summary: The selection and implementation of appropriate security controls for an information system or a system-of-systems are important tasks that can have major implications on the operations and assets of a department or agency as well as the welfare of individuals and the general public. Security controls are the management, operational, and technical safeguards or countermeasures employed within enterprise information systems to protect the confidentiality, integrity, and availability of the system and its information.

Purpose: The purpose of Security Program Management is to appropriately address the following questions:

- What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have selected security controls been implemented or is there a realistic plan for their implementation?
- Are the selected security controls, as implemented, are effective in their application?

Policy Objectives: The Department of Technology Services will identify and monitor on an ongoing basis, risks arising from the use of information and information systems, and report on the effectiveness of existing security controls to agency IT Directors and senior management in the Department of Technology Services, consistent with National Institute of Standards and



Technology, Special Publication 800-53 Rev3 (Appendix G) and Special Publication 800-122.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#)

2.3.3 Risk Assessment

Summary: An effective risk assessment process is an important component of a successful enterprise security program. The principal goal of an enterprise risk assessment process should be to protect departments and agencies and their ability to perform their mission, not just their information assets. Therefore, the risk assessment process should not be treated primarily as a technical function carried out by the Department of Technology Services who operate and manage the information systems, but as an essential management function of the department or agency itself.

Purpose: The purpose of performing a risk assessment is to enable the department or agency to accomplish its mission;

- by better securing information systems that store, process, or transmit department or agency information;
- by enabling management to make well-informed risk management decisions;
- to justify the expenditures related to information security;
- and by assisting management in authorizing (or accrediting) the information systems on the basis of the supporting documentation resulting from the performance of a risk assessment.

Policy Objectives: State of Utah, Departments and Agencies must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of enterprise information systems and the associated processing, storage, or transmission of organizational information, consistent with National Institute of Standards and Technology, Special Publications 800-30, 800-30 Revision 1, 800-39, 800-53A Rev1 RA1-5 (Appendix F, Page F-92), and State of Utah Enterprise Standard 5000-0300-S1, Security Vulnerability Assessments Standard

Security Control Standards:

[NIST SP 800-53A Rev1: Guide for Assessing the Security Controls in Information Systems and Organizations](#)

[DTS 5000-0300-S1: Security Vulnerability Assessments Standard](#)

Additional Information

[NIST SP 800-30: Risk Management Guide for Information Technology Systems](#)

[NIST SP 800-30 R1: Guide for Conducting Risk Assessments](#)

[NIST SP 800-39: Managing Information Security Risk](#)

2.3.4 Security Assessment and Authorization

Summary: In today's environment where many, if not all, of an organization's mission-critical functions are dependent upon information technology, the ability to manage this technology and to assure confidentiality, integrity, and availability of information is now mission-critical. Ongoing monitoring is a critical part of the Security Assessment and Authorization process. Timely, relevant, and accurate information is vital, particularly when resources are limited and agencies must prioritize their efforts.

Purpose: The purpose of information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of security control effectiveness, vulnerabilities in information systems, and threats to information systems and assets, and to support risk mitigation efforts and enterprise risk management decisions.

Policy Objectives: State of Utah, Departments and Agencies must: periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; authorize the operation of organizational information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls, consistent with National Institute of Standards and Technology, Special Publication 800-53 Rev3 CA1-7 (Appendix F, Page F-32)

The Department of Technology Services, Enterprise Information Security Office, will continuously monitor information security vulnerabilities and threats, and report identified changes to agency IT Directors and senior management in the Department of Technology Services, consistent with National Institute of Standards and Technology, Special Publication 800-137.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST 800-137: Information Security Continuous Monitoring \(ISCM\) for Information Systems and Organizations](#)

2.3.5 System and Services Acquisition

Summary: To be most effective, information security must be integrated into the Solution Development Life Cycle (SDLC) from system inception to implementation and ongoing support. Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:

- Early identification and mitigation of security vulnerabilities and misconfiguration, resulting in lower cost of security control implementation and vulnerability mitigation;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.

The consideration of security in the System Development Life Cycle is essential to implementing and integrating a comprehensive strategy for managing risk for all information technology assets in an organization.

Purpose: Adequate security controls must be integrated into processes used for systems and services acquisition, including internal development, purchasing, and outsourcing to ensure that information assets used by the State are protected.

Policy Objectives: All software application and system development or the acquisition of applications and systems, including externally provided cloud based services, by the State of Utah will employ a Solution Development Life-Cycle (SDLC) methodology approved by the Department of Technology Services that incorporates security planning and review during each phase of development or acquisition and adheres to a secure-coding methodology. This approach requires that project and development teams, in collaboration with Agency IT Directors and the Enterprise Information Security Office

assess risks to the development and implementation or acquisition of information systems and assets while incorporating controls into the process to mitigate such risks. A Solutions Development Life-Cycle methodology will be developed and maintained by the Department of Technology Services, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 SA1-14 (Appendix F, Page F-96) and Department of Technology Services Policy 3000-0001.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

[DTS Policy 3000-0001: Acquisition of Goods and Services](#)

2.3.6 Security Awareness and Training

Summary: A strong information security program cannot be put in place without significant attention given to training employees and system users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure information resources. In addition, those in the Department of Technology Services who manage infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because the security of information systems and assets is as much a human issue as it is a technology issue.

Purpose: Everyone has a role to play in the success of a security awareness and training program but department and agency executives, agency IT Directors, and program managers have key responsibilities to ensure that effective training programs are established enterprise wide. The scope and content of the program must be tied to existing security policy directives.

Policy Objectives: All new State of Utah employees and all contractors shall undergo Information system security awareness training before being granted access to information systems and assets. Current State of Utah employees are required to undergo Information system security awareness training annually in order to maintain access to information assets. The Enterprise Information Security Office will collaborate with agency IT Directors to develop and implement security awareness and training programs. The Enterprise Information Security Office will maintain records of training attendance and completion for all employees and contractors consistent with National Institute of Standards and Technology, Special Publications 800-50, and 800-53 Rev3 AT1-5 (Appendix F, Page F-21)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST 800-50: Building an Information Technology Security Awareness and Training Program](#)

2.3.7 Configuration Management

Summary: An information system is composed of many components that can be interconnected in a multitude of arrangements to meet a variety of business, mission, and information security needs. How these information system components are networked, configured, and managed is critical in providing adequate information security and supporting an organization's risk management process.

Purpose: Implementing new information systems and changing existing systems results in some adjustment to the system configuration. To ensure that the required adjustments to system configurations do not adversely affect the security of the information system or the users from operation of the information system, a well-defined configuration management process that integrates information security is required.

Policy Objectives: The Department of Technology Services must: establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and establish and enforce security configuration settings for information technology products employed in enterprise and organizational information systems, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev3 CM1-8 (Appendix F, Page F-38), and 800-128.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST 800-128: Guide for Security-Focused Configuration Management of Information Systems](#)

2.3.8 Contingency Planning

Summary: Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery

of information system functions using alternate equipment, or performance of information system functions using manual methods.

Purpose: Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.

Policy Objectives: State of Utah, Departments and Agencies should establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations, consistent with National Institute of Standards and Technology, Special Publication 800-34 Revision 1, and 800-53 Rev3 CP1-10 (Appendix F, Page F-47).

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST 800-34: Contingency Planning Guide for Information Systems](#)

2.3.9 Incident Response

Summary: A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides illegal copies of software to others through peer-to-peer file sharing services.

- An unencrypted laptop computer or information storage device is lost or stolen.
- An attacker attempts to compromise authentication to an information asset using brute force.
- Authorized access to network resources is blocked with a with a Denial of Service attack.

Purpose: Rapid and effective incident response is required because attacks frequently compromise personal and business data. It is critically important to respond quickly and efficiently when security breaches occur. An incident response capability should support incidents systematically so that appropriate and consistent actions are taken.

Policy Objectives: The Department of Technology Services must: establish an operational incident handling capability for enterprise information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate organizational officials and/or authorities, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev3 IR1-8 (Appendix F, Page F-61), 800-61 Rev2, and the Department of Technology Services, Cyber Security Incident Response Plan.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

[State of Utah, Cyber Security Incident Response Plan](#)

Additional Information:

[NIST SP 800-61 Rev2: Computer Security Incident Handling Guide](#)

2.3.10 Maintenance

Summary: Information systems and equipment require service and /or frequent updates in order to operate at their highest capability, remain secure, and to work in the most efficient manner.

Purpose: Periodic and timely maintenance on information systems, including effective patch management processes is a requirement of a comprehensive security program.

Policy Objectives: State of Utah, Departments and Agencies with system maintenance responsibilities must perform periodic and timely maintenance on information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system

maintenance, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 PS1-8 (Appendix F, Page F-88)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.3.11 Media Protection

Summary: Information systems capture, process, and store information using a wide variety of media. This information is located not only on the intended storage media but also on devices used to create, process, or transmit this information. This media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. Efficient and effective management of information created, processed, and stored by an information system throughout its life (from inception through disposal) is a primary concern of a media protection strategy.

Purpose: The State of Utah is required by federal and state regulatory statute to provide a reasonable assurance, in proportion to the confidentiality of the data, that all digital and paper media containing information assets must be protected at all times from unauthorized access.

Policy Objectives: State of Utah, Departments and Agencies must: protect information system media, both paper and digital; limit access to information on information system media to authorized users; and sanitize or destroy information system media before disposal or release for reuse, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev3 MP1-6 (Appendix F, Page F-71), 800-88.

Employees should only use State-owned encrypted media when downloading State data containing PI, PHI, FTI, or CJIS, or any other sensitive data to a removable media device such as, but not limited to, USB drives, tapes, CDs, and DVDs.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

Additional Information:

[NIST SP 800-88: Guidelines for Media Sanitization](#)

2.3.12 Personnel Security

Summary: In response to increasing threats, organizations need to implement or update a personnel security program to prevent unauthorized access to information systems and assets. Organizations should develop

specific trustworthiness and capability criteria for personnel security and information system integrity. The personnel security program should consider an individual background, qualifications, and operational restrictions prior to granting an individual access to protected information and systems. The overall objective is to ensure that individuals granted access are trustworthy, capable, and operationally safe. Also, the organization, including the employees and the environment in which they function, should operate securely so that they do not constitute an unacceptable security risk that could impact other personnel or the public.

Purpose: Effective information security requires that individuals granted access to systems and data be vetted to ensure that information security objectives can be maintained.

Policy Objectives: State of Utah, Departments and Agencies must ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions. In addition, departments and agencies must ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers and employ formal sanctions for personnel failing to comply with organizational security policies and procedures, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 PS1-8 (Appendix F, Page F-88)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.3.13 Physical and Environmental Protection

Summary: In order to minimize disruption, damage, or loss of information and technology resources utilized by an organization, requirements for physical and environmental protection of information assets are mandatory. For the purposes of this policy, 'facilities' is defined to include all areas that contain information assets, including general workspace, but special focus should be placed on concentrations of assets, such as data centers, server rooms, network/data transmission hubs (i.e. telephone/data/wiring closets), concentrated cable runs, and technology or records staging/storage areas.

Purpose: The State of Utah is required to use reasonable means to protect its information systems from threats posed by individuals or groups with malicious intent, environmental hazards, and other activities or events that pose potential risks to information systems and assets.

Policy Objectives: State of Utah, Departments and Agencies must limit physical access to information systems, equipment, and the respective operating environments to authorized individuals and protect the physical

infrastructure for information systems, including the protection of information systems against environmental hazards and providing appropriate environmental controls in facilities containing information systems, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 PE1-19 (Appendix F, Page F-76), and Department of Technology Services Standard 5000-0500-S1.

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

[DTS 5000-0500-S1: Physical and Environmental Protection Standards](#)

2.3.14 System and Information Integrity

Summary: The two key components of system integrity are software authenticity and the assurance of user identity. Organizations should routinely evaluate how to integrate the following best practices into their current environments to achieve these objectives:

- Enable logging for all centralized authentication services and collect the IP address of the system accessing the service, the username, the resource accessed, and whether the attempt was successful or not.
- Limit the number of authentication attempts and lockout the user if the limit is reached. Security professionals should conduct a manual review before unlocking the account and prohibit automatic unlocks after a specified time period.
- Conduct near real-time log review for failed attempts per user and per unit of time independent of successful logins; abnormal successful logins; and lockouts. Correlate this data to identify anomalous activity.
- Limit remote access.
- Restrict access by IP address wherever possible.
- Limit concurrent logins to one per user.
- Maximize complexity of passwords, passphrases, and personal identification numbers (PINs) whenever possible.
- Enable defenses against key logging such as forced frequent credential changing and updated anti-virus (AV) signatures.
- Validate software.

Purpose: The State of Utah is required to use reasonable means to protect its information systems from threats posed by viruses, spam, hackers, malware, and other malicious activities by installing, maintaining, and monitoring appropriate technical features to protect its systems.

Policy Objectives: State of Utah, Departments and Agencies must identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 SI1-13 (Appendix F, Page F-124)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.3.15 Access Control

Summary: Access control, in one form or another, is considered by most organizations to be the cornerstone of their security programs. The various features of physical, technical, and administrative access control mechanisms work together to construct the security architecture so important in the protection of an organization’s critical and sensitive information assets.

Purpose: The administration of user access to electronic information is required to apply the principles of least privilege and “need to know”, and must be administered to ensure that the appropriate level of access control is applied to protect the information asset in each application or system.

Policy Objectives: State of Utah, Departments and Agencies must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 AC1-22 (Appendix F, Page F-3)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.3.16 Audit and Accountability

Summary: The ability to audit events and activities on a network provides information necessary to determine if an information system or asset has been compromised. Audit and accountability capabilities also help an organization mitigate issues as they are developing.

Purpose: A chronological record of activities involving system events and user activity is required which will enable the reconstruction, review, and examination of the sequence of activities concerning each event.

Policy Objectives: State of Utah, Departments and Agencies must create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 AU1-14 (Appendix F, Page F-24)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.3.17 Identification and Authentication

Summary: A foundational aspect of information security is knowing who has been granted access to systems and assets. The identification and authentication of users and processes allows an organization to restrict access to only authorized users and processes.

Purpose: The protection of information systems and assets from unauthorized modification, disclosure or destruction to ensure that it is accurate, remains confidential, and is available when needed is a requirement of federal and state regulatory statute.

Policy Objectives: State of Utah, Departments and Agencies must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to enterprise information systems, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 IA1-8 (Appendix F, Page F-54)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.3.18 System and Communication Protection

Summary: The protection of information assets at rest and in transit is fundamental to an organization's security program. System and communication protection includes analog based systems as well as digital networks.



Purpose: The State of Utah is required to use reasonable means, commensurate with risk, to protect the confidentiality, availability and integrity of information assets in storage and during transmission.

Policy Objectives: The Department of Technology Services must: monitor, control, and protect analog and digital communications (i.e., information transmitted or received by organizational information systems) at the external boundaries of the enterprise network and at designated internal boundaries of information systems; and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational and enterprise information systems, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev 3 SC1-34 (Appendix F, Page F-106)

Security Control Standards:

[NIST SP 800-53 R3: Recommended Security Controls for Information Systems and Organizations](#)

2.4 Policy Compliance

State of Utah, Departments and Agencies, employees, and contractors are expected to comply with this enterprise security policy. Additional policies and standards developed and implemented by State Departments and Agencies may include additional objectives or detail, but they must be compatible with the security objectives described in this policy document.

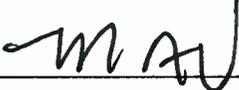
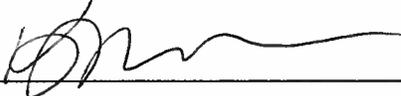
2.5 Enforcement

Violation of this policy by personnel employed by the Department of Technology Services may be the basis for discipline including but not limited to termination. Individuals working in any State of Utah Department or Agency found to have violated this policy may also be subject to legal penalties as may be prescribed by state and/or federal statute, rule, and/or regulation.



Document History

Originator: Boyd Webb, Chief Information Security Officer
Next Review: January 05, 2014
Reviewed Date: January 05, 2013
Reviewed By: Boyd Webb, Chief Information Security Officer

DTS Representative			
Signature:		Date:	1-7-13
Name (Printed):	Mark VanOrden	Title (Printed):	CIO/ DTS Executive Director
Signature:		Date:	1-7-13
Name (Printed):	Kenneth Petersen	Title (Printed):	DTS Chief Operations Officer