05-02. Information Security

Internal Policies and Procedures
of the
Utah State Board of Education

Policy # 05-02

Subject: Information Security

Effective Date: 08/01/2018
Revision Date:

1. Purpose:

1.1. To delineate security requirements, roles, and responsibilities necessary to protect USBE data and information systems from unauthorized access, inappropriate disclosure, or compromise.

1.2. This policy shall be used to assess the risk of conducting business and to assess third-party suppliers who sign a contract to provide services to USBE.

1.3. This policy:

1.3.1. complies with all legal, regulatory, and contractual obligations regarding protection of USBE data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence;

1.3.2. provides the authority to design, implement, and maintain security controls meeting USBE standards concerning the protection of data in motion, at rest, and processed by related information systems;

1.3.3. ensures USBE employees comply with the policy and undergo annual security training;

1.3.4. informs employees that the USBE monitors employee usage of information systems and hosted data without additional notice;

1.3.5. requires that USBE data be stored and manipulated on USBE-provided information systems or contracted systems that are approved for use and comply with this policy; and

1.3.6. implements a security incident reporting mechanism that captures incidents securely. Security incidents include policy violations, potential data breach, fraud, intrusions to information systems, and theft of hardware or data.

2. Policy and Scope:

2.1. All USBE employees, temporary employees, and contractors shall comply with this policy.

2.2. USBE employee's conduct or behavior while using any USBE-managed information system shall comply with USBE security policies.

References:

NIST Cybersecurity Framework (CSF), NIST SP 800-53 Rev. 4, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP-800-161, FIPS 100-42

3. General Policies and Procedures

3.1. In accordance with USBE policy and procedures, this policy is reviewed and adjusted as needed on an annual basis or more frequently.

3.2. All information is classified according to policy established in this and related documents.

3.3. USBE is designated as the steward for all confidential information.

3.4. Only authorized employees and agents are allowed access to confidential information and related systems, and these authorized employees are accountable for following this policy and any related documents.

3.5. Networks, systems, software, and all other IT services that store, transmit, or process confidential information are managed according to this policy and all related documents.

3.6. Information security controls shall comply with this policy and supporting standards, plans, and procedures, unless specifically exempted.

3.7. Data Stewards are designated for all confidential information, maintain a record of all confidential information for which they are responsible, and manage confidential information according to this policy and all other applicable policies, standards and plans.

4. Roles and Responsibilities

The following individuals are responsible for the general information security roles and responsibilities outlined below.

4.1. Information Security Manager

4.1.1. Provides governance for Agency IT systems and information with respect to security compliance with this policy.

4.1.2. Publishes a common operating environment (COE) that defines the infrastructure standards incorporating security policies. Reviews and approves any low risk COE deviations or exceptions.

4.1.3. Provides guidelines for on-and-off network information systems with respect to maintaining an information security plan complying with Agency security policies.

4.1.4. Acts as primary custodian of the information security risk assessment process. Reports identified risk to the USBE risk committee.

4.1.5. Keeps USBE security policy and procedures current for both digital and physical assets.

4.1.6. Oversees security operations including risk management, incident response, vulnerability management, network security monitoring, threat hunting, and penetration testing.

4.1.7. Acts as the incident lead during an active incident and is responsible for submitting a root cause report after the fact to IT management.

4.1.8. Works with Information Technology (IT) managers to develop security practices, standards, and guidelines for the implementation of this policy.

4.1.9. Enforces compliance with USBE security policies by conducting periodic security checks and audits.

4.1.10. Works with the Chief Privacy Officer (CPO) to oversee internal and external reporting requirements (FERPA, CJIS, GRAMA).

4.1.11. Works with the CPO to implement security awareness and training campaigns.

4.2. USBE Supervisors

4.2.1. Comply with Agency security policies by incorporating security practices, standards, and guidelines in various stages of IT development, implementation, operation, and retirement.

4.2.2. Ensure annual security training is completed by USBE employees and non-employees (such as team members and subcontractors).

4.2.3. Follow established incident reporting and escalation procedures.

4.2.4. Periodically update standard operating procedures (SOPs) to ensure compliance with USBE information security policies and procedures.

4.3. USBE Employees

4.3.1. Comply with USBE information security policies and procedures.

4.3.2. Complete the security training at the beginning of employment and every year thereafter.

4.3.3. Follow established incident reporting and escalation procedures.

4.3.4. Take reasonable care to protect Agency provided equipment and access credentials.

4.4. **Contracted third-parties, suppliers, temporary employees, and consultants**

4.4.1. Demonstrate ability to meet and perform per USBE information security policies and procedures.

4.4.2. Provide USBE with required third-party audit reports as part of due care.

5. Compliance and Penalties for Noncompliance

5.1. Compliance with the policy is conducted through executing periodic assessments by Security, internal/external audits, or self-assessments.

5.2. A USBE employee who fails to comply with this policy may be subject to disciplinary action, such as removal or limiting access to the system, termination of employment or contract, or unfavorable remarks in the employee performance review.

5.3. Compliance failures could have legal or regulatory ramifications with regard to federal, state, local, or international law.

Policy Guidance by Functional Area

The following subsections are found in the full USBE Information Security Policy, found here. These subsections provide information security policy guidance for the USBE and are organized according to the following 11 functional areas with relation to preventive, detective, forensic, and audit objectives.

6.0 Systems Administration
7.0 Network Security
8.0 Application Security
9.0 Endpoint, Server, and Device Security
10.0 Identity, Authentication and Access Management
11.0 Data Protection and Cryptography
12.0 Monitoring, Vulnerability, and Patch Management
13.0 High Availability, Disaster Recovery, and Physical Protection
14.0 Cyber Intrusion Response
15.0 Asset Management and Supply Chain
16.0 Policy, Audit, E-Discovery, and Training