Revision & Sign-off

Change Record

Date	Author

Introduction

This guideline is classified as Public and was developed for internal use. The purpose of the guideline is to complement the USG IT Handbook by providing regulatory requirements concerning cybersecurity awareness and training.

The examples provided may or may not apply to your organization and need to be assessed for applicability. For example, New York State's requirements may have no bearing on your organization unless your organization is doing business in or with New York. Whereas, other regulations like GLBA will affect all USG organizations. These requirements were added because of past precedent. Like breach notification, it took only one state to pass into law breach requirements for notification, and currently all states have breach notification legislation. The same trend is happening at the state level concerning data privacy. Raising awareness as to what one state has formalized into law, may predict what the future of awareness training legislation may look like in the near future.

Board Policy 10.4.2 Institutional and Organizational Level Responsibilities states, "Cybersecurity implementation must include a user awareness, tras(o)-6.6 (n)2.2.9 (a (a)(hS6 (n)-0.7.1 (a)- -0.0)10.6 (m)-CJ

Principle 4.1.4 of PIPEDA, Canada's broadly applicable privacy law, requires training about the

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided.

45 CFR § 164.308(a)(5) Administrative safeguards.

(a)(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

Gramm-Leach-Bliley Act (GLBA)

Training under GLBA is required via the

(e) No contractor employee shall be permitted to have or retain access to a system of records, create, collect, use, process, store, maintain, disseminate, disclose, or dispose, or otherwise handle personally identifiable information, or design, develop, maintain, or operate a system of records, unless the employee has completed privacy training that, at a minimum, addresses the elements in paragraph (b) of this section.

EU-US Privacy Shield Framework

Proper training is necessary for an organization to comply with the Department of Commerce's Privacy Shield Framework. In its 7th Supplemental Principle (a series of principles that follows the primary 7 principles), called "Verification," Privacy Shield requires verification via self-assessment. One area to be attested is the organization must have published privacy policy regarding personal information" that "conforms to the Privacy

Georgia Cybersecurity Board

The Cybersecurity Board, reconstituted by Executive Order on August 13, 2019, is tasked with identifying risks, promoting best practices, and assessing compliance with training.

Section 500.14 Training and Monitoring

As part of its cybersecurity program, each Covered Entity shall: …

> (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Texas Health Privacy Law

Section 181.101 of the Health and Safety Code, as amended by HB 1609, requires that training covers both the state's law and HIPAA. This law is one of the few state health laws that mandates training about the state's own health privacy law. Penalties and sanctions for violating the Texas law are equivalent to HIPAA's.

Section 181.101. Training Required

> (a) Each covered entity shall provide training to employees of the covered entity regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out their duties for the covered entity.
>
> (b) An employee of a covered entity must complete training described by Subsection (a) not later than the 180th day after the date the employee is hired by the covered entity.
>
> (c) If the duties of an employee of a covered entity are affected by a material change in state or federal law concerning protected health information, the employee shall receive training described by Subsection (a) within a reasonable period, not to exceed one year, after the material change becomes effective.
>
> (d) A covered entity shall require an employee of the entity who is trained as described by Subsection (a) to sign, electronically or in writing, a statement verifying the employee's completion of training. The covered entity shall maintain the signed statement for six years.

Standards and Policy

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is a standard developed by the credit card industry's PCI council. It has a number of requirements regarding privacy training.

- PCI-DSS 12.6 – Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
- PCI-DSS 12.6.1 – Educate personnel upon hire and at least annually.
- PCI-DSS 12.6.1.a – Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).
- PCI-DSS 12.6.1.b – Verify that personnel attend awareness training upon hire and at least annually.
- PCI-DSS 12.6.2 – Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.

- PCI DSS 12.9.4 – Verify through observation and review of policies that staff with responsibilities for security breach response are periodically trained.

ISO/IEC 27002

The International Standards Organization (ISO)'s Information Security standard ISO/IEC 27002:2005 is one of the most frequently followed standards by organizations throughout the world. The standard provides guidance on information security management in organizations, and it contains a requirement that all employees receive data security awareness training.

Section 8.2.2 Information Security Awareness, Education, and Training

> All employees of the organization and, where relevant, contractors and third-party users, should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

NIST Special Publication 800-53 (Revision 4)

NIST SP 800-53 is one of the most relied-upon cybersecurity standards. Many federal agencies and state and local governments look to NIST to guide their rulemaking and enforcement. NIST SP 800-53 has extensive cybersecurity awareness training requirements as well as privacy awareness training requirements.

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:

> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
>
> 1. A security awarenese5d -8.7 (a)-5.2.9 (n)-0.8 (e)rs hnay dd -8.7 (a)-5.2.9 (e)-2 (t)-0.5 (y

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. [Assignment: organization-defined frequency] thereafter.

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for [Assignment: organization-defined time period].

AR-5 PRIVACY AWARENESS AND TRAINING

Control: The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and

USG Board of Regents Policy Manual

Section 10.4.2 of the USG Board of Regents Policy Manual addresses Institutional Responsibilities concerning user awareness training and is part of a larger USG cybersecurity policy.

Cybersecurity implementation must include a user awareness, training, and education plan, which is

The Chancellor, organization president or chief executive is responsible for ensuring that appropriate and auditable cybersecurity controls are in place to include awareness, training and education.

5.9.2 Discusses learning objectives and training requirements ….

Awareness training shall be conducted annually, attendance shall be mandatory, completion shall be documented and shall provide practical and simple guidance pertaining to user roles and responsibilities.

Closing Comments

As with all of our documents, they are dynamic and considered works in progress. If you discover an error or have an additional standard or regulation that the community would benefit from mapping, please submit your comment to cybersecurity@usg.edu for correction or consideration.