P2113 - HITRUST - Education, Training, and Awareness Policy

Contents

Purpose:

The purpose of the Education, Training, and Awareness policy is to provide and establish Executive level explicit direction for all individuals and entities to follow the implemented awareness program for providing ongoing security education and training to employees and stakeholders. This policy aims to validate that individuals are knowledgeable about their roles and responsibilities regarding information security, understand potential threats, and adhere to best practices in alignment with HITRUST CSF requirements.

The Organization is responsible for overseeing the development, implementation, and maintenance of the Information Security Program and associated components.

Scope:

This policy applies to all implemented information systems and supporting infrastructure used to support and protect sensitive data (PHI). This applies to systems whether managed centrally or in a distributed fashion, and to all individuals and entities who intend to access information systems and data. Within this document, the phrase "information systems and data" includes all technology resources and systems, transactions, applications, platforms, networks, databases, and other information systems within Integrity's technological environment.

Statement:

Security Awareness Training

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, prior to accessing any system's information.

Reference: 13998.02e1Organizational.2

Dedicated phishing awareness training is developed as part of the organization's onboarding program, is documented and tracked, and includes the recognition and reporting of potential phishing attempts.

Reference: 13.02e1Organizational.6

The organization provides role-based security-related training , especially for personnel with significant security responsibilities (e.g., system administrators), prior to accessing the organization's information resources, when required by system or environment changes, when entering into a new position that requires additional role-specific training, and no less than annually thereafter.

Reference: 1304.02e1Organizational.7

Acceptable Use

The organization establishes and makes readily available to all information system users a set of rules that describe their responsibilities and expected behavior with regard to information and information system usage.

Acceptable use addresses rules for electronic mail and Internet usages and guidelines for the use of mobile devices, especially for the use outside the premises of the organization.

The organization includes in the rules of behavior containing explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.

Reference: 1307.07c1Organizational.124

Malicious Code Protections

The organization prohibits users from installing unauthorized software, including data and software from external networks, and disables any auto-run features which allow file execution without user authorization (such as when files are downloaded from the Internet or when removable media is inserted).

Users are made aware and trained on requirements relating to prohibition of installing unauthorized software, including data and software from external networks.

Reference: 1308.09j1Organizational.5

Disciplinary Action

All employees and contractors are informed in writing that violations of the security policies will result in sanctions or disciplinary action.

Reference: 1306.06e1Organizational.5

This Education, Training, and Awareness Policy is supported by the following procedures:

- *13 – HITRUST – Education, Training, and Awareness Procedure*

The Organization - Integrity, LLC and applicable Business Units.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Related Procedure References:

Related Regulatory Information:

P2113 - HITRUST - Education, Training, and Awareness Policy		
Document Author	**Name:** **Title:** **Email:**	Sumit Dhawan Manager Cybersecurity Compliance Sumit.Dhawan@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matt Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 2/24/2026
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan McQueen Assistant General Counsel Duncan.McQueen@integrity.com 3/16/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 3/30/2026

Last Published Date: 3/30/2026

Document Version Number 2.0