NIST 800-171: Security Awareness Training Compliance Checklist

Awareness and Training: SP 800-171 Security Family 3.2

Users of a system can be viewed as the weakest link in securing systems. Often users are not aware of how their actions may impact the security of a system. Making system users aware of their security responsibilities and teaching them correct practices helps change their behavior. It also supports individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures or how to use them, users cannot be truly accountable for their actions.

The purpose of information security awareness, training, and education is to enhance security by:

- raising awareness of the need to protect system resources,
- developing skills and knowledge so system users can perform their jobs more securely, and
- building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems.

The company is responsible for making sure that managers and users are aware of the security risks associated with their activities and that employees are trained to carry out their information security-related duties and responsibilities. Examples of awareness and training security requirements include: security awareness training, role-based security training, and security training records.

The following security requirements fall under the Awareness and Training family

3.2.1 Ensure that managers, systems administrators, and users of organization information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organization information systems.

Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities?

Does the training provide a basic understanding of the need for information security, applicable policies, standards, and procedures related to the security of the information system, as well as user actions to maintain security and respond to suspected security incidents?

Does the training also address awareness of the need for operations security?

Is basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter?

Additional Information

Companies determine the appropriate content of security awareness training and security awareness techniques based on the specific company requirements and the information systems to which employees have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior company officials, displaying logon screen messages, and conducting information security awareness events.

3.2.2 Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Do employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities?

Does the training cover physical, personnel, and technical safeguards and countermeasures?

Does the training address required security requirements related to environmental and physical security risks?

Does the training include indications of potentially suspicious email or web communications?

Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on a periodic basis?

Additional Information

Companies determine the appropriate content of security training based on the assigned roles and responsibilities of individuals, and the specific security requirements of companies and the information systems to which personnel have authorized access. In addition, companies provide enterprise architects, information system developers, software developers, acquisition/ procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security requirement assessors, and other personnel having access to system-level software, adequate security- related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the company security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of company information security programs. Role-based security training also applies to contractors providing services to federal agencies.

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Do users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threat, e.g., long-term job dissatisfaction, attempts to gain unauthorized access to information, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies?

Does security training include how to communicate employee and management concerns regarding potential indicators of insider threat?

Are practical exercises included in security awareness training that simulate actual cyberattacks?

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Additional Information

Potential indicators and possible precursors of insider threat can include behaviors such as longterm job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies, procedures, directives, rules, or practice.

Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate company channels in accordance with established company policies and procedures.