For High-Impact Information Systems

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

AT-1.1 - **Examine** security awareness and training policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with security awareness and training responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents security awareness and training policy and procedures.				
(ii)	The organization disseminates security awareness and training policy and procedures to appropriate elements within the organization.				
(iii)	The responsible parties within the organization periodically review security awareness and training policy and procedures.				
(iv)	The organization updates security awareness and training policy and procedures when organizational review indicates updates are required.				

AT-1.2 - Examine security awareness and training policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with security awareness and training responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment,				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	coordination among organizational entities, and compliance.				
(ii)	The security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.				

AT-2 SECURITY AWARENESS - The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.

AT-2.1 – Examine security awareness and training policy; procedures addressing security awareness training implementation; NIST Special Publication 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan (for organization-defined frequency of refresher security awareness training); other relevant documents or records, **and**

Interview organizational personnel comprising the general information system user community to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes.				
(ii)	The security awareness training is consistent with applicable regulations and NIST Special Publication 800-50.				
(iii)	The security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access.				
(iv)	The organization defines the frequency of refresher security				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	awareness training.				
(v)	The organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.				

AT-3 SECURITY TRAINING - The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.

AT-3.1 - Examine security awareness and training policy; procedures addressing security training implementation; NIST Special Publication 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records**, and**

Interview organizational personnel with significant information system security responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities.				
(ii)	The organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes.				
(iii)	The security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security.				
(iv)	The security training is consistent with applicable regulations and NIST Special Publication 800-50.				
(v)	The organization defines the frequency of refresher security training.				
(vi)	The organization provides refresher security training in accordance with organization-defined frequency, at least annually.				

AT-4 SECURITY TRAINING RECORDS - The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

AT-4.1 - Examine security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization monitors and documents basic security awareness training and specific information system security training.				

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS - The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

AT-5.1 – Examine security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records to determine if the following requirements is met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and share security-related information.				