Security Plan - #64 - 2 Twelve E3 Lab IaaS

PRINTED BY:  HOWERTON, TRAVIS (HOWIEAVP)

Date Printed: 12/29/2020| thowerton@c2labs.com| 8656600643
Co-Founder and Chief Technology Officer (CTO)

System Information

The objective of information security planning is to improve the protection of information resources and assets. Most systems have some level of information sensitivity and require commensurate protections as part of pro-active risk management best practices. These expectations for protections and controls are documented in a security plan.

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The security plan also delineates the security boundary and the responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system. Additional information may be included in the basic plan and the structure and format organized according to the its specific needs.

In order for the plans to adequately reflect the protection of the resources, a senior management official must authorize a system to operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the system security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and any identified issues. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur whenever there is a security significant change to the system.

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Other Identifier: F00000000

Status: Operational

System Type: General Support System

Facility: N/A

Date Submitted: N/A

Approval Date: N/A

Expiration Date: N/A

Confidentiality: Moderate

Integrity: Moderate

Availability: Moderate

Overall Categorization: Moderate

High Value Asset (HVA)?: false

Description:

System Metadata

Version: 0.0

Imported Using OSCAL Version: 1.0-Milestone3

Remarks: This OSCAL-based FedRAMP SSP Template can be used for the FedRAMP Low, Moderate, and High baselines.\n\nGuidance for OSCAL-based FedRAMP Tailored content has not yet been developed.

System Properties

marking: Controlled Unclassified Information

Revision History

Version: 1.0, Date Published: 2019-06-01T00:00:00.00-04:00, OSCAL Version: 1.0-Milestone3, Remarks: Initial publication.

Version: 2.0, Date Published: 2020-06-01T00:00:00.00-04:00, OSCAL Version: 1.0-Milestone3, Remarks: Updated for annual assessment.

Relevant Roles for this SSP

Prepared By(ID: prepared-by) - The organization that prepared this SSP. If developed in-house, this is the CSP itself.

Prepared For(ID: prepared-for) - The organization for which this SSP was prepared. Typically the CSP.

System Security Plan Approval(ID: content-approver) - The individual or individuals accountable for the accuracy of this SSP.

Cloud Service Provider(ID: cloud-service-provider) - no description provided.

Information System Owner(ID: system-owner) - The individual within the CSP who is ultimately accountable for everything related to this system.

Authorizing Official(ID: authorizing-official) - The individual or individuals who must grant this system an authorization to operate.

Authorizing Official's Point of Contact(ID: authorizing-official-poc) - The individual representing the authorizing official.

Information System Management Point of Contact (POC)(ID: system-poc-management) - The highest level manager who responsible for system operation on behalf of the System Owner.

Information System Technical Point of Contact(ID: system-poc-technical) - The individual or individuals leading the technical operation of the system.

General Point of Contact (POC)(ID: system-poc-other) - A general point of contact for the system, designated by the system owner.

System Information System Security Officer (or Equivalent)(ID: information-system-security-officer) - The individual accountable for the security posture of the system on behalf of the system owner.

Privacy Official's Point of Contact(ID: privacy-poc) - The individual responsible for the privacy threshold analysis and if necessary the privacy impact assessment.

Owner of an inventory item within the system.(ID: asset-owner) - no description provided.

Administrative responsibility an inventory item within the system.(ID: asset-administrator) - no description provided.

ICA POC (Local)(ID: isa-poc-local) - The point of contact for an interconnection on behalf of this system.

ICA POC (Remote)(ID: isa-poc-remote) - The point of contact for an interconnection on behalf of this external system to which this system connects.

ICA Signatory (Local)(ID: isa-authorizing-official-local) - Responsible for signing an interconnection security agreement on behalf of this system.

ICA Signatory (Remote)(ID: isa-authorizing-official-remote) - Responsible for signing an interconnection security agreement on behalf of the external system to which this system connects.

Consultant(ID: consultant) - Any consultants involved with developing or maintaining this content.

[SAMPLE]Unix Administrator(ID: admin-unix) - This is a sample role.

[SAMPLE]Client Administrator(ID: admin-client) - This is a sample role.

[SAMPLE]Program Director(ID: program-director) - This is a sample role.

Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO)(ID: fedramp-pmo) - no description provided.

Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB)(ID: fedramp-jab) - no description provided.

OSCAL Profile

Imported: #890170c3-d4fa-4d25-ab96-8e4bf7cc237c

System Properties

authorization-type: fedramp-agency
security-eauth-level: 2
identity-assurance-level: 2
authenticator-assurance-level: 2
federation-assurance-level: 2

System Annotations

cloud-service-model: saas (Remarks: Remarks are required if service model is \"other\". Optional otherwise.)
cloud-deployment-model: government-only-cloud (Remarks: Remarks are required if deployment model is \"hybrid-cloud\" or \"other\". Optional
otherwise.)

System Sensitivity and Privacy

Security Sensitivity Level: low
privacy-sensitive: yes
pta-1: yes(Class: pta)
pta-2: yes(Class: pta)
pta-3: yes(Class: pta)
pta-4: no(Class: pta)
sorn-id: [No SORN ID](Class: pta)

Information Types and System Classification

Type: Information Type Name(GUID: 06ecba4f-db96-4491-a3a2-7febfa227435)
Description: A description of the information.
InfoType ID (From - https://doi.org/10.6028/NIST.SP.800-60v2r1): C.2.4.1
Confidentiality Impact - Base: fips-199-moderate, Selected: fips-199-moderate
Integrity Impact - Base: fips-199-moderate, Selected: fips-199-moderate
Availability Impact - Base: fips-199-moderate, Selected: fips-199-moderate

Back Matter and Related Resources

UUID	Title	Properties	Links
3a5ca2de-0f66-47e6-844d-6ccdf214b767	FedRAMP Applicable Laws and Regulations	conformity: fedramp-citations	https://www.fedramp.gov/assets/resources/templates/SSP-A12-FedRAMP-Laws-and-Regu Template.xlsx
12da89ef-51dd-4404-948d-e9f0e25b961e	FedRAMP Master Acronym and Glossary	conformity: fedramp-acronyms	https://www.fedramp.gov/assets/resources/documents/FedRAMP_Master_Acronym_and_
d45612a9-cf25-4ef6-b2dd-69e38ba2967a	[SAMPLE]Name or Title of Document	type: law publication: Publication Date	https://domain.example/path/to/document.pdf
a8a0cc81-800f-479f-93d3-8b8743d9b98d	[SAMPLE]Privacy-Related Law Citation	type: law type: pii publication: Publication Date	https://domain.example/path/to/document.pdf

545e75c3-537f-48fe-9630-95337916d982	[SAMPLE]Regulation Citation	type: regulation publication: Publication Date	https://domain.example/path/to/document.pdf
9d6cf2b4-8e88-4040-a33c-7bc206553a1a	[SAMPLE]Interconnection Security Agreement Title	publication: Document Date version: Document Version	N/A
31a46c4f-2959-4287-bc1c-67297d7da60b	CSP Logo	conformity: prepared-for-logo conformity: csp-logo	./logo.png
c5866ad8-8ed7-49b4-844a-0276fa9f8f51	Preparer Logo	conformity: prepared-by-logo	./party-1-logo.png
0846b6ef-cfa4-4bb3-8280-717f7e7b04d4	FedRAMP Logo	conformity: fedramp-logo	https://github.com/GSA/fedramp-automation/raw/master/assets/FedRAMP_LOGO.png
2c1747d6-874a-49a2-8488-2fd9735416bf	3PAO Logo	conformity: 3pao-logo	./logo.png
d2eb3c18-6754-4e3a-a933-03d289e3fad5	The primary authorization boundary diagram.	N/A	./diagrams/boundary.png
61081e81-850b-43c1-bf43-1ecbddcb9e7f	The primary network diagram.	N/A	./diagrams/network.png
ac5d7535-f3b8-45d3-bf3b-735c82c64547	The primary data flow diagram.	N/A	./diagrams/dataflow.png

090ab379-2089-4830-b9fd-26d0729e22e9	Policy Title - Policy document	type: policy publication: Document Date version: Document Version	./sample_policy.pdf
ab300133-d749-4abb-b858-1cd6ffd8af9e	Policy Title - Policy document	type: policy publication: Document Date version: Document Version	./sample_policy.pdf
1002a58e-9e11-4aa6-9ab4-2bde52995952	Procedure Title - Procedure document	type: procedure publication: Document Date version: Document Version	./sample_procedure.pdf
4bb1e2e5-261c-4b5c-b22c-e1627c2e8be6	Procedure Title - Procedure document	type: procedure publication: Document Date version: Document Version	./sample_procedure.pdf
90a128ac-c850-48f6-8fff-a55692f80b41	User's Guide - User's Guide	conformity: user-guide type: guide publication: Document Date version: Document Version	./sample_guide.pdf
fab59751-b855-40cb-93c1-492562e20e18	Privacy Impact Assessment	conformity: privacy-impact-assessment publication: Document Date version: Document Version	./pia.docx
489112e1-57f2-4c29-8dd0-95b1442fbf3b	Document Title - Rules of Behavior	conformity: rules-of-behavior type: rob publication: Document Date version: Document Version	https://sample

c7860916-f2f4-43aa-b578-d48cf8e6d381	Document Title - Contingency Plan (CP)	type: plan publication: Document Date version: Document Version	https://sample
ab56cf27-0dae-40d6-89b7-d750137309af	Document Title - Configuration Management (CM) Plan	type: plan publication: Document Date version: Document Version	https://sample
3f771ab5-8016-4571-98d1-f0fb962e15e2	Document Title - Incident Response (IR) Plan	type: plan publication: Document Date version: Document Version	https://sample
49fb4631-1da2-41ca-b0b3-e1b1006d4025	Separation of Duties Matrix - Separation of Duties Matrix	publication: Document Date version: Document Version	https://sample
9f1aae37-7359-411f-86c1-768aaab85e63	FedRAMP High Baseline	N/A	https://raw.githubusercontent.com/usnistgov/OSCAL/v1.0.0-milestone3/content/fedramp.gov/xml/FedRAMP_HIGH-baseline_profile.xml
890170c3-d4fa-4d25-ab96-8e4bf7cc237c	FedRAMP Moderate Baseline	N/A	https://raw.githubusercontent.com/usnistgov/OSCAL/v1.0.0-milestone3/content/fedramp.gov/xml/FedRAMP_MODERATE-baseline_profile.xml
2acaf846-5496-4d36-8565-9a15b48aef2c	FedRAMP Low Baseline	N/A	https://raw.githubusercontent.com/usnistgov/OSCAL/v1.0.0-milestone3/content/fedramp.gov/xml/FedRAMP_LOW-baseline_profile.xml

Environment:

System Properties

users-internal: 0

users-external: 0

users-internal-future: 0

users-external-future: 0

Users

User	Properties	Roles	Privileges
[SAMPLE]Unix System Administrator (GUID: 9cb0fab0-78bd-44ba-bcb8-3e9801cc952f)	sensitivity: high privilege-level: privileged type: internal	admin-unix	Full administrative access (root), including the following functions: - Add/remove users and hardware - install and configure software - OS updates, patches and hotfixes - perform backups

[SAMPLE]Client Administrator (GUID: 16ec71e7-025c-43e4-9d3f-3acb485fac2e)	sensitivity: moderate privilege-level: non-privileged type: external	external	Portal administration, including the following functions: - Add/remove client users - Create, modify and delete client applications
[SAMPLE]Program Director (GUID: ba7708c1-4041-48ab-9b7b-1ddb5e175fe0)	sensitivity: limited privilege-level: no-logical-access type: internal	program-director	Administrative Access Approver, including the following functions: - Approves access requests for administrative accounts. Access Approver, including the following functions: - Approves access requests for administrative accounts.

Components

Title	Type	Description	Properties	Links	Pr
This System (GUID: 60f92bcf-f353-4236-9803-2a5d417555f4)	system	The entire system as depicted in the system authorization boundary	N/A	N/A	N/
Name of Leveraged System (GUID: e82e6e07-0c62-417e-8a19-3744991b4c65)	system	If the leveraged system owner provides a UUID for their system (such as in an OSCAL-based CRM), it should be used as the UUID for this component.	leveraged-authorization-uuid: 5a9c98ab-8e5e-433d-a7bd-515c07cd1497	N/A	N/
[SAMPLE]Module Name (GUID: 95beec7e-6f82-4aaa-8211-969cd7c1f1ab)	validation	[SAMPLE]FIPS 140-2 Validated Module	cert-no: 0000	(Link: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/0000)	N/
[SAMPLE]Product Name (GUID: 05ceb8df-52e7-49db-9719-891723f366bd)	software	FUNCTION: Describe typical component function. COMMENTS: Provide other comments as needed.	asset-type: os scan-type: infrastructure vendor-name: Vendor Name model: Model Number version: Version Number patch-level: Patch Level validation: fips-module-1	N/A	N/
[SAMPLE]Product (GUID: 1541015b-6d19-42cb-a991-624cc082ed4d)	hardware	FUNCTION: Describe typical component function. COMMENTS: Provide other comments as needed.	asset-type: database scan-type: infrastructure scan-type: database vendor-name: Vendor Name model: Model Number version: Version Number	N/A	N/
OS Sample (GUID: 6617f60b-8bac-422d-9939-94f43ddc0f7a)	os	None	asset-type: os scan-type: infrastructure baseline-configuration-name: Baseline Config. Name allows-authenticated-scan: yes	N/A	N/
Database Sample (GUID: 120f1404-7c9f-4856-a247-63bd89d9e769)	software	None	asset-type: database scan-type: database baseline-configuration-name: Baseline Config. Name allows-authenticated-scan: yes	N/A	N/

Appliance Sample (GUID: 8f230d84-2f9b-44a3-acdb-019566ab2554)	software	None	asset-type: appliance scan-type: web login-url: https://admin.offering.com/login baseline-configuration-name: Baseline Config. Name allows-authenticated-scan: no(Remarks: Vendor appliance. No admin-level access.)	N/A		N/
[SAMPLE]Service Name (GUID: d5841417-de4c-4d84-ab3c-39dd1fd32a96)	service	Describe the service Section 10.2, Table 10-1. Ports, Protocols and Services\n\n**SERVICES ARE NOW COMPONENTS WITH type='service'**	used-by: What uses this service? protocol:	N/A		**Na** **ht** Tra TC 80 **Na** **ht** Tra TC 44
[EXAMPLE]Authorized Connection Information System Name (GUID: 2812ef51-61e7-4505-afbb-da5a073a2a5b)	interconnection	Briefly describe the interconnection. Optional notes about this interconnection	service-processor: [SAMPLE]Telco Name ipv4-address: 10.1.1.1 ipv4-address: 10.2.2.2 direction: incoming-outgoing information: Describe the information being transmitted. port: 80 circuit: 1 connection-security: ipsec(Remarks: If \"other\", remarks are required. Optional otherwise.)	(Link: #9d6cf2b4-8e88-4040-a33c-7bc206553a1a, Type: agreement)		N/

System Inventory

ID	Description	Properties	Roles	Component

unique-asset-id (GUID: 98e37f90-fbb5-4177-badb-9b55229cc183)	Flat-File Example (No implemented-component). COMMENTS: Additional information about this item.	ipv4-address: 10.1.1.1 ipv6-address: 0000:0000:0000:0000 virtual: no public: no fqdn: dns.name uri: uniform.resource.identifier netbios-name: netbios-name mac-address: 00:00:00:00:00:00 software-name: software-name version: V 0.0.0 asset-type: os vendor-name: Vendor Name model: Model Number patch-level: Patch-Level serial-number: Serial # asset-tag: Asset Tag vlan-id: VLAN Identifier network-id: Network Identifier scan-type: infrastructure scan-type: database validation: component-id allows-authenticated-scan: no(Remarks: If no, explain why. If yes, omit remarks field.) baseline-configuration-name: Baseline Config. Name physical-location: Physical location of Asset is-scanned: yes(Remarks: If no, explain why. If yes, omit remarks field.) function: Required brief, text-based description.(Remarks: Optional, longer, formatted description.)	asset-owner asset-administrator	N/A
unique-asset-ID (GUID: c916d3c5-229e-4786-bf3f-4d71baa0e7a5)	Component Inventory Example COMMENTS: If needed, provide additional information about this inventory item.	ipv4-address: 10.2.2.2 ipv6-address: 0000:0000:0000:0000 mac-address: 00:00:00:00:00:00 virtual: no public: no fqdn: dns.name uri: uniform.resource.locator netbios-name: netbios-name patch-level: Patch-Level baseline-configuration-name: Baseline Configuration Name physical-location: Physical location of Asset scan-authenticated: no(Remarks: If no, explain why. If yes, omit remark.) scan-latest: yes(Remarks: If no, explain why. If yes, omit remark.)	asset-owner asset-administrator	asset-administrator
unique-asset-id (GUID: 37c00d5a-ccf2-4112-a0ee-8460be8cff40)	None.	ipv4-address: 10.3.3.3 is-scanned: yes	N/A	37c00d5a-ccf2-4112-a0ee-8460be8cff40
unique-asset-id (GUID: fb7a84fb-7e30-4f5b-9997-2ecd4d270bdd)	None.	ipv4-address: 10.4.4.4 is-scanned: yes	N/A	fb7a84fb-7e30-4f5b-9997-2ecd4d270bdd

unique-asset-id (GUID: 779d4e89-bba6-432c-b50d-d699fe534129)	None.	ipv4-address: 10.5.5.5 is-scanned: yes	N/A	779d4e89-bba6-432c-b50d-d699fe534129
unique-asset-id (GUID: 20b207d5-5e77-4501-b02d-5d2a6e88db85)	None.	ipv4-address: 10.6.6.6 is-scanned: no(Remarks: Asset wasn't running at time of scan.)	N/A	20b207d5-5e77-4501-b02d-5d2a6e88db85
unique-asset-id (GUID: 79b4f0d1-91ab-49e8-af28-045c12aa9272)	None.	ipv4-address: 10.7.7.7 is-scanned: yes	N/A	79b4f0d1-91ab-49e8-af28-045c12aa9272
unique-asset-id (GUID: b31b360d-b58b-4c7c-b344-68e17238d858)	None.	ipv4-address: 10.8.8.8 is-scanned: no(Remarks: Asset wasn't running at time of scan.)	N/A	b31b360d-b58b-4c7c-b344-68e17238d858
10.10.10.0 (GUID: 55b55b3d-3bd9-409a-bc87-3b9a2074bacd)	IPv4 Production Subnet.	ipv4-subnet: 10.10.10.0/24 is-scanned: yes	N/A	N/A
10.10.20.0 (GUID: c0dbefa1-c8e8-4ca8-bd73-67cb7b1fa3f6)	IPv4 Management Subnet.	ipv4-subnet: 10.10.20.0/24 is-scanned: yes	N/A	N/A

Laws and Regulations:

Authorization Boundary: A holistic, top-level explanation of the FedRAMP authorization boundary.

Network Architecture: A holistic, top-level explanation of the network architecture.

Data Flow: A holistic, top-level explanation of the system's data flows.

System Owner: Howerton, Travis

Information System Security Officer (ISSO): Howerton, Travis

Authorization Official (AO): Howerton, Travis

Total Users: 0

Total Privileged Users: 0

Users with Multi-Factor Authentication (MFA): 0

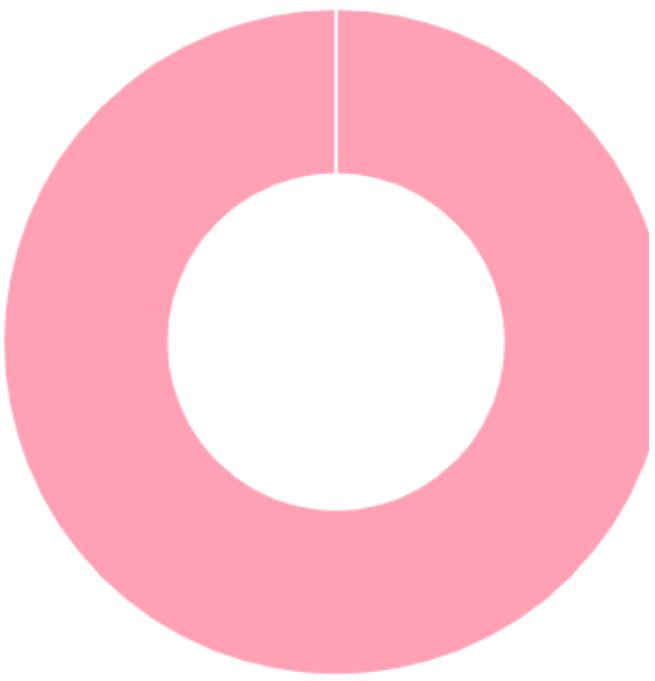
Privileged Users with Multi-Factor Authentication (MFA): 0

Control Implementations

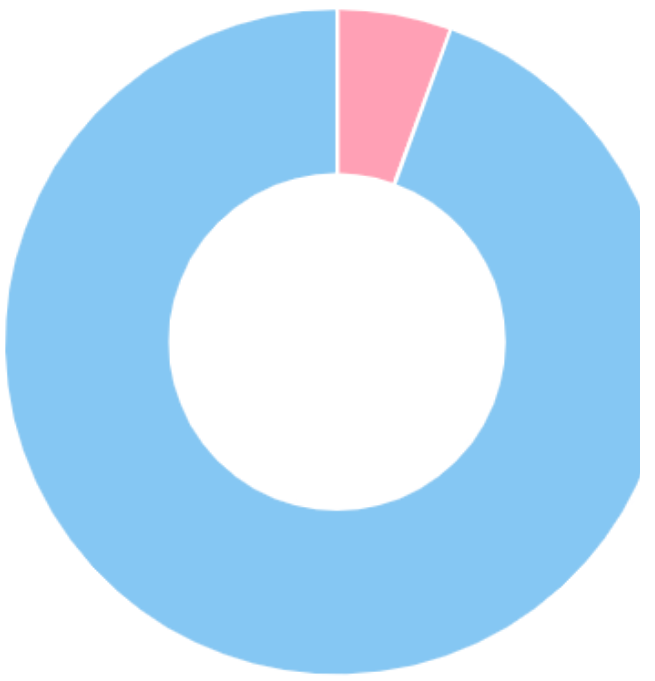
Cyber security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to the information system. Security controls provide the foundation of the security plan by describing the security hardening process of locking down the system. Controls are generally inherited from industry or government cyber security compliance standards (i.e. NIST, HIPAA, PCI, ISO27001, etc.). One or more compliance standards may apply to the information system based on the type of information it is protecting.

The section below captures the identified security controls for this information system. It describes the control to implement, the policy to be applied, a description of how it was implemented, the current status of the control, and the date it was last assessed or tested. Controls should be continuously monitored over the life of the system to ensure that the risk mitigations applied by the control remain effective over the system lifecycle.

By Control Owner



By Status



AC-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and
c. Review and update the current access control:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Access Control

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874.
IA-1
PM-9
PM-24
PS-8
SI-12

Related Controls

IA-1, PM-9, PM-24, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ac-1_stmt.a

UUID: fb4d020a-dc4f-46f5-9c1f-f6242eaf60bc

UUID: fb4d039a-dc4f-46f5-9c1f-f6343eaf69bc

Remarks: The specified component is the system itself.\n\nAny control implementation response that can not be associated with another component is associated with the component representing the system.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	3f5612a4-cd1d-4c47-8cae-75d2eaa332cd	Describe how Part a is satisfied within the system.	N/A

ac-1_stmt.a.1

UUID: 0afdccce-b5ed-4127-ae19-cfbdd17d775e

Remarks: This identifies a policy (attached in resources) that satisfies this control.

Links

(Type: policy)

(Link: #090ab379-2089-4830-b9fd-26d0729e22e9)

ac-1_stmt.a.2

UUID: ffaf5e02-3055-40df-bbeb-3b94e834a43f

Remarks: This identifies a process (attached in resources) that satisfies this control.

Links

(Type: process)

(Link: #att-process-1)

ac-1_stmt.b.1

UUID: b46f97ec-55c1-4249-a9b9-3a228f1e3791

Description: Describe how Part b-1 is satisfied.

ac-1_stmt.b.2

UUID: 59c67969-3d5c-45f1-8e3e-1e642249633f

Description: Describe how Part b-2 is satisfied.

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ac-1_prm_1: [replace with list of personnel or roles]

ac-1_prm_2: [specify frequency]

ac-1_prm_3: [specify frequency]

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

AC-2 - Account Management

Description

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;
d. Specify:
1. Authorized users of the system;
2. Group and role membership; and
3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;
e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];
g. Monitor the use of accounts;
h. Notify account managers and [Assignment: organization-defined personnel or roles] within:
1. [Assignment: organization-defined time period] when accounts are no longer required;
2. [Assignment: organization-defined time period] when users are terminated or transferred; and
3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
1. A valid access authorization;
2. Intended system usage; and
3. [Assignment: organization-defined attributes (as required)];
j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

Discussion

Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.
Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.
Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Family

Access Control

Weight

0

References

Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019.
Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-178.
Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-192.
AC-3
AC-5
AC-6
AC-17
AC-18
AC-20
AC-24
AU-2
AU-12
CM-5
IA-2
IA-4
IA-5
IA-8
MA-3
MA-5
PE-2
PL-4
PS-2
PS-4
PS-5
PS-7
PT-2
PT-3
SC-7
SC-12
SC-13
SC-37

Related Controls

AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ac-2_stmt.a

UUID: 24a85abb-25ad-4686-850c-5c0e8ab69a0c

Description: Do not respond to this statement here. Respond within the `by-component` assembly below.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	8a72663c-28c7-41c2-8739-f1ee2d5761ac	For the portion of the control satisfied by this system or its owning organization, describe **how** the control is met. The component-uuid above points to the \"this system\" component.\n\nAny control response content that does not cleanly fit another system component is placed here. This includes customer responsibility content.\n\nThis can also be used to provide a summary, such as a holistic overview of how multiple components work together.\n\nWhile the \"this system\" component is not expclicity required within every `statement`, it will typically be present.	responsibility: customer (Remarks: General customer responsibility description.)
b7364f67-bf65-4df2-b756-4b9c6b1c4a52	84de735f-ba37-4bb4-b784-79760f986a40	For the portion inherited from an underlying FedRAMP-authorized provider, describe **what** is inherited.	responsibility: customer (Remarks: Component-specific customer responsibility description.)
cae07d12-8566-443a-95de-7596b9cac953	13db02bb-1f33-4f79-8711-ed47c2c3d337	For the portion of the control that must be configured by or provided by the customer, describe the customer responsibility here. This is what will appear in the Customer Responsibility Matrix.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)
implementation-status: partial(Remarks: Describe the portion of the control that is not satisfied.)
implementation-status: not-applicable(Remarks: Describe the justification for marking this control Not Applicable.)
control-origination: sp-system
control-origination: customer-configured(Remarks: Describe any customer-configured requirements for satisfying this control.)

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: Completion Date

Parameter Settings

ac-2_prm_1: [SAMPLE]privileged, non-privileged
ac-2_prm_2: [SAMPLE]all
ac-2_prm_3: [SAMPLE]The Access Control Procedure
ac-2_prm_4: [SAMPLE]annually

Responsible Roles

admin-unix
program-director

Status: Not Applicable

Last Assessment Result:

Date Last Assessed: N/A

AT-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] awareness and training policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
c. Review and update the current awareness and training:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Awareness and Training

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and

Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.

PM-9

PS-8

SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

at-1_stmt.a

UUID: ee5a11fb-9bae-4680-8f8c-575c85d47355

Description: Component-based Approach

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	d3bdee1c-7d84-4ed4-8950-e13256edb7fa	Describe how Part a is satisfied.	N/A

at-1_stmt.a.1

UUID: 2e8ec7ce-c9c6-4f5f-9d50-3a3b9d3acf65

Remarks: This identifies a policy (attached in resources) that satisfies this control.

Links

(Type: policy)

(Link: #090ab379-2089-4830-b9fd-26d0729e22e9)

at-1_stmt.a.2

UUID: e7f9b618-c092-4b8b-b416-0ee477026726

Remarks: This identifies a process (attached in resources) that satisfies this control.

Links

(Type: process)

(Link: #att-process-1)

at-1_stmt.b.1

UUID: 29192f0b-edb1-4820-b951-65ffdc64bb3e

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	5a5e5c3e-1108-47f1-a83f-05e0394219db	Describe how Part b-1 is satisfied.	N/A

at-1_stmt.b.2

UUID: 23a9bfa7-6e3f-4e00-a120-791b26a9157e

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	fcc63699-04ab-4b69-b7b9-a13bee6685b3	Describe how Part b-2 is satisfied.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

at-1_prm_1: [replace with list of personnel or roles]

at-1_prm_2: [specify frequency]

at-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

AU-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] audit and accountability policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
c. Review and update the current audit and accountability:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does

not constitute an organizational policy or procedure.

Family

Audit and Accountability

Weight

0

References

Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

au-1_stmt.a

UUID: 9a2bd937-226e-4aaf-8261-2cf0c2e3aa10

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	30042cb9-ff85-472f-b769-68bd7bb5bbd9	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

au-1_stmt.b.1

UUID: d01f186f-a14f-4e22-b069-84a55e48a112

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	f41962c7-b53b-46f8-a84f-4aba25904bb8	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

au-1_stmt.b.2

UUID: ea153acb-2bd0-41d9-8ebd-ba022d31230a

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	9ad59f0d-17a2-4f3f-af6a-a8529d692195	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

au-1_prm_1: [replace with list of personnel or roles]

au-1_prm_2: [specify frequency]

au-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

CA-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented

within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Assessment, Authorization, and Monitoring

Weight

0

References

[OMB A-130, Appendix II]
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137.
Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ca-1_stmt.a

UUID: e7bd0a7e-5f92-4769-8cd3-76ad2f663a5c

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	e5815f1d-ec94-4d98-8896-ec57e339bd7b	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ca-1_stmt.b.1

UUID: b2c3ec86-b976-4e5a-9dc3-4ac2d570765e

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	ca6b2bd5-3ddf-4167-a942-06e1955e49f8	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ca-1_stmt.b.2

UUID: e9474eb8-36d6-4eab-abeb-f9bd17e66b22

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	507b8b9d-2d40-4748-81c9-c5a13c8f8f05	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ca-1_prm_1: [replace with list of personnel or roles]

ca-1_prm_2: [specify frequency]

ca-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

CM-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] configuration management policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
c. Review and update the current configuration management:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Configuration Management

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8

SA-8

SI-12

Related Controls

PM-9, PS-8, SA-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

cm-1_stmt.a

UUID: 52339583-19b6-4774-9213-50b9f42fe51f

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	2916ebd5-c45a-466e-b8e9-00dd15b0c94d	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

cm-1_stmt.b.1

UUID: f9cc6f3f-c64f-4fae-9a32-f964ebdc8e74

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	678db1d2-a538-4986-ac94-63da312fe3f9	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

cm-1_stmt.b.2

UUID: c548a71f-41d6-4e8c-b400-1764379348c4

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	a871cf91-04c7-4e03-9df6-80b3d5afc9bf	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

cm-1_prm_1: [replace with list of personnel or roles]

cm-1_prm_2: [specify frequency]

cm-1_prm_2: [specify frequency]
cm-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

CP-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] contingency planning policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and
c. Review and update the current contingency planning:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Contingency Planning

Weight

0

References

Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

cp-1_stmt.a

UUID: 8bde1fa5-eb81-4a1b-9e6e-5827e176025a

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	157d7751-938c-441f-9299-02a339d98532	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

cp-1_stmt.b.1

UUID: 2fc9eec1-a49f-4cfa-9f7b-c702a1e21619

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	6358db78-bab1-4139-b512-f65d3e48248b	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

cp-1_stmt.b.2

UUID: db5b3977-bd51-4505-b3e2-1597bbd4d930

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	3de33bbe-1a15-4d10-b35d-56fd85e24571	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

cp-1_prm_1: [replace with list of personnel or roles]

cp-1_prm_2: [specify frequency]

cp-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

IA-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or

controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Identification and Authentication

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
National Institute of Standards and Technology (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 201-2.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020.
Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016.
Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2.
Polk T, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874.
AC-1
PM-9
PS-8
SI-12

Related Controls

AC-1, PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Policy:

Statements

ia-1_stmt.a

UUID: ba92e479-705f-47a4-a763-dfc098ba239d

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	5add335d-7375-49f0-843c-ac994e4d147b	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ia-1_stmt.b.1

UUID: dba8c469-5758-497e-9856-e472a2e08677

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	b04d86a0-b68c-41f0-9c0b-88a8daa457b7	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ia-1_stmt.b.2

UUID: b56e37b1-1f4c-479b-bfa1-a2773c2eebfd

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	c8fde380-9a41-404a-a88b-c20479a21618	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ia-1_prm_1: [replace with list of personnel or roles]

ia-1_prm_2: [specify frequency]

ia-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

IR-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] incident response policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and
c. Review and update the current incident response:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Incident Response

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50.
Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2.
Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ir-1_stmt.a

UUID: 7284efc2-d953-486c-ab8a-3caef6ce06c3

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	7b385445-5e7b-4656-98f1-0f1353aab59e	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ir-1_stmt.b.1

UUID: 75c37e1a-6e8d-4ef0-99f4-c16f7995706c

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	e7ae4685-2e30-4e00-9ada-b00b5eaf5578	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ir-1_stmt.b.2

UUID: 900591ec-2006-4622-bc87-59828d884d4f

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	f443c391-479d-492d-b7e9-55c9c2c107be	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ir-1_prm_1: [replace with list of personnel or roles]

ir-1_prm_2: [specify frequency]

ir-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

MA-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] maintenance policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
c. Review and update the current maintenance:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Maintenance

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.

Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ma-1_stmt.a

UUID: d609e538-3976-418e-a368-58fc75cd03c0

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	93a9b046-63c4-4628-8547-39bc7d8df70c	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ma-1_stmt.b.1

UUID: df1a6dd8-9e18-4408-8783-cb30e0413f22

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	ad14f76a-a3eb-4349-8f6c-54cd99f1c040	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ma-1_stmt.b.2

UUID: f02f759d-7d4c-41f2-b153-f3cc1e157e39

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	32b337f6-eb61-4945-a139-4d2ae7737488	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)
control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ma-1_prm_1: [replace with list of personnel or roles]
ma-1_prm_2: [specify frequency]
ma-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

MP-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] media protection policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and
c. Review and update the current media protection:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Media Protection

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

mp-1_stmt.a

UUID: bab45ad3-65ee-43bc-9c3e-c3e4e2db8001

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	6668f521-4d5c-4317-868f-804878675bf2	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

mp-1_stmt.b.1

UUID: ca35d4a5-ca73-4b3a-aa66-6c712c7a4a49

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	57e65240-5b41-40ee-89b1-f75d8fb259ad	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

mp-1_stmt.b.2

UUID: 0c5c6eda-9644-46f2-a29c-16fe4e248621

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	ea6c7fa7-ccbf-414c-8c6b-9c928e914b35	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)
control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

mp-1_prm_1: [replace with list of personnel or roles]
mp-1_prm_2: [specify frequency]
mp-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

PE-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
c. Review and update the current physical and environmental protection:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security

and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Physical and Environmental Protection

Weight

0

References

Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
AT-3
PM-9
PS-8
SI-12

Related Controls

AT-3, PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

pe-1_stmt.a

UUID: 11fd3e46-4735-4986-91bc-747345fe608a

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	dceb4401-c1fd-41a7-9e07-8d82a8042e61	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

pe-1_stmt.b.1

UUID: a37f91e2-190d-40f7-829c-39776c14c8b4

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	bbd2b372-b57d-4a3a-90c2-2189dd23664b	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

pe-1_stmt.b.2

UUID: f3d57138-916c-4064-b2fc-aa8dd76849f8

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	f4a94538-220f-4f73-9487-73b72b68813e	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

pe-1_prm_1: [replace with list of personnel or roles]

pe-1_prm_2: [specify frequency]

pe-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

PL-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] planning policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and
c. Review and update the current planning:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Planning

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:
Statements

Statements

pl-1_stmt.a

UUID: ec7af577-ff22-46bf-ac0a-cf9d75c72ebb

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	679837fb-601e-4517-abe6-11ff6fc551b4	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

pl-1_stmt.b.1

UUID: 438f3e29-670a-49f2-8b9f-05d951318294

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	ddce2988-ce9b-4f15-a427-6f18e4ba1817	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

pl-1_stmt.b.2

UUID: 96a4d13c-bd2b-4038-96c5-0f923f404bbd

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	18d7c02e-f21b-4cd2-bf33-d27971ced47f	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

pl-1_prm_1: [replace with list of personnel or roles]

pl-1_prm_2: [specify frequency]

pl-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

PS-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] personnel security policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and
c. Review and update the current personnel security:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Personnel Security

Weight

0

References

Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ps-1_stmt.a

UUID: afe1703d-5e59-460b-b048-41b49699c5a1

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	7d6cafb2-b613-4807-ad61-4f0f649bd5ee	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ps-1_stmt.b.1

UUID: 956c93e2-cf8f-482c-aaf7-91ab44c7cbd6

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	f4fbfbc2-1a94-456d-a713-9d547f18a0c7	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ps-1_stmt.b.2

UUID: 6926c688-3fb2-4ab8-9acb-cff0b5acd365

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	2f9c701a-0f3e-4e3d-beae-debb08c406ed	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ps-1_prm_1: [replace with list of personnel or roles]

ps-1_prm_2: [specify frequency]

ps-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

RA-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
c. Review and update the current risk assessment:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

Risk Assessment

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8

SI-12

Related Controls

PM-9, PS-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

ra-1_stmt.a

UUID: 8fe541ea-0920-42d0-8561-4e08f04d796c

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	5894d92b-05bf-4fc4-85dc-f5c37e112bc4	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ra-1_stmt.b.1

UUID: b0e9ed47-fe83-485d-8d79-979833543a83

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	c90ad6ee-5a40-4996-8e6c-d85ff3f7559e	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

ra-1_stmt.b.2

UUID: d9a38f95-ded1-4d1d-afe2-242987222ebd

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	d6f6ac98-4f15-45f2-9ecc-4447e96af44f	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

ra-1_prm_1: [replace with list of personnel or roles]

ra-1_prm_2: [specify frequency]

ra-1_prm_3: [specify frequency]

ra-1_prm_3: [Specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

SA-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and services acquisition policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and
c. Review and update the current system and services acquisition:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

System and Services Acquisition

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018.
PM-9
PS-8
SA-8
SI-12

Related Controls

PM-9, PS-8, SA-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

sa-1_stmt.a

UUID: ae3f64be-2e62-4347-b06a-727bc28e4f9b

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	e5864f16-83f2-4faf-b7be-0810c6e58fc4	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

sa-1_stmt.b.1

UUID: 959519a9-3e12-47bc-8d76-50d9ab0b6544

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	bed8f51a-1773-493c-8167-c83712e03f01	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

sa-1_stmt.b.2

UUID: 9daa3848-9672-469c-9aa0-f363e3339123

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	518d4987-9436-4c1f-9e07-afa6b332f124	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

sa-1_prm_1: [replace with list of personnel or roles]

sa-1_prm_2: [specify frequency]

sa-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

SC-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and communications protection policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and
c. Review and update the current system and communications protection:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how

the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

System and Communications Protection

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SA-8
SI-12

Related Controls

PM-9, PS-8, SA-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

sc-1_stmt.a

UUID: 5e2e8372-c13b-4cf5-90c5-e8833a9fe241

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	88cfadba-043b-483b-8032-73344aa53c96	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

sc-1_stmt.b.1

UUID: 8166980a-86c0-497d-87e4-453adfd0d4bd

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	9abaeb64-56d2-48a1-bd8d-7b55411d31ca	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

sc-1_stmt.b.2

UUID: eeea34ff-18ab-4c35-bf32-c74dbf746e7b

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	ad20ff50-8a7c-4ffc-a918-260960f6fb42	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

sc-1_prm_1: [replace with list of personnel or roles]

sc-1_prm_2: [specify frequency]

sc-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A

SI-1 - Policy and Procedures

Description

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and information integrity policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Family

System and Information Integrity

Weight

0

References

Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1.
Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.
PM-9
PS-8
SA-8
SI-12

Related Controls

PM-9, PS-8, SA-8, SI-12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:

Statements

si-1_stmt.a

UUID: 915b10d2-2275-4d86-951a-eec23f9ee77a

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-	682311e7-e3f7-4d94-acf9-	For the portion of the control satisfied by the service provider,	N/A

2a5d417555f4	131149887fda	describe **how** the control is met.	

si-1_stmt.b.1

UUID: 2a5a6f7f-aeea-4ea4-be1e-859df4bf7521

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	80ee0fe9-7f87-4dfa-887a-ac3bb2131943	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

si-1_stmt.b.2

UUID: c152bbde-57fc-4864-ac51-861bd8bb83b4

Description: Ignore.

Components

Component ID	UUID	Description	Annotations
60f92bcf-f353-4236-9803-2a5d417555f4	78e8f2bb-67d7-49d3-a993-ce4bedcfbc47	For the portion of the control satisfied by the service provider, describe **how** the control is met.	N/A

Annotations

implementation-status: planned(Remarks: Describe the plan to complete the implementation.)

control-origination: sp-system

Control Owner: Howerton, Travis

Implementation:

Properties

planned-completion-date: 2020-11-27Z

Parameter Settings

si-1_prm_1: [replace with list of personnel or roles]

si-1_prm_2: [specify frequency]

si-1_prm_3: [specify frequency]

Responsible Roles

program-director

Status: Not Implemented

Last Assessment Result:

Date Last Assessed: N/A