5.17 Planning (PL) Policy

PURPOSE

To develop plans that describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to assess the effectiveness of the control.

POLICY

01. SYSTEM SECURITY AND PRIVACY PLANS

1. Develop security and privacy plans for the system that:
2. Are consistent with the organization’s enterprise architecture.
3. Explicitly define the constituent system components.
4. Describe the operational context of the system in terms of mission and business processes.
5. Identify the individuals that fulfill system roles and responsibilities.
6. Identify the information types processed, stored, and transmitted by the system.
7. Provide security categorization of the system, including supporting rationale.
8. Describe any specific threats to the system that are of concern to the organization.
9. Provide the results of a privacy risk assessment for systems processing personally identifiable information.
10. Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
11. Provide an overview of the security and privacy requirements for the system.
12. Identify any relevant control baselines or overlays, if applicable.
13. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions.
14. Include risk determinations for security and privacy architecture and design decisions.
15. Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security, and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities; and are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
16. Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities.
17. Review the system security and privacy plans at least annually or when required due to system changes or modifications.
18. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.
19. Protect the plans from unauthorized disclosure and modifications.

02. RULES OF BEHAVIOR

1. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
2. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the systems.
3. Review and update the rules of behavior at least annually.
4. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.
5. Include in the rules of behavior, restrictions on use of social media, social networking sites, and external sites/applications, posting organizational information on public websites, and use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

03. SECURITY AND PRIVACY ARCHITECTURES

1. Develop security and privacy architectures for the system that describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.
3. Describe how the architectures are integrated into and support the enterprise architecture.
4. Describe any assumptions about, and dependencies on, external systems and services.
5. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture.
6. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

04. CENTRAL MANAGEMENT

1. The CJISSECPOL is centrally managed by the FBI CJIS ISO.

05. BASELINE SELECTION

1. Select a control baseline for the system.
2. Tailor the selected control baseline by applying specified tailoring actions.

PROCEDURES

The agency must develop the procedures to ensure compliance with these requirements.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – PL-10, RA-2, RA-3, RA-9, SA-8.