Sample System Security Plan

DRAFT EXCERPT · Apex Precision test scenario

All people, accounts, configurations, review outcomes and implementation statements in this kit are invented for training. No CUI, export-controlled information, real contract data or credentials are included. Do not submit these files to SPRS, an assessor or a contracting officer as evidence of real implementation.

System and boundary

System: Apex Lab Workspace. Fictional staff: 12. Fictional managed workstations: 8. Boundary: one test office, sample identity directory and sample file repository. General corporate email and personal devices are excluded from this exercise. A real organization must validate all actual CUI flows and external services. No real CUI resides in this kit.

Roles and connections

Morgan Taylor: contractor owner. Jamie Reed: IT lead. Riley Chen: consultant reviewer. These are fictional names. A lab directory connects to the sample repository over an assumed encrypted test link. Hardware, locations and supplier suitability remain unverified.

Version and limits

Version 0.1 / 23 October 2026. Baseline: NIST SP 800-171 Rev. 2, 110 requirements. This excerpt illustrates four controls only; it is not an adequate full SSP and does not prove implementation of 3.12.4.

Sample System Security Plan · continued

3.1.1 · Access authorization

NEEDS-REVIEW. Policy requires owner-approved access and a recorded periodic review. lab-user-03 has no approver or review date in the sample register. IT lead must investigate and obtain a documented decision. Do not treat the policy alone as technical evidence.

3.1.8 · Unsuccessful logon attempts

MISSING. The incomplete fictional configuration says failed_logon_limit=not_configured. The example correction uses a locally chosen threshold of 5 and 15-minute lockout. These numbers are sample policy choices, not universal NIST mandates.

3.12.4 · System security plan

AI-DRAFTED. This file contains sample scope and four narratives only. The full real SSP must describe the actual boundary, environment, implementation and connections; a qualified person determines sufficiency. Uploading this excerpt does not satisfy this requirement.

3.3.1 · Audit records

USER-ASSERTED. The example narrative assumes access events are logged. No operational log or functional test is supplied. Real event selection, retention and review must be documented and tested.

Remaining 106 requirements

Not described in this excerpt. The separate 110-control worksheet contains a synthetic scoring benchmark with 108 assumed-implemented controls and two gaps; that assumption must never be copied into an actual assessment.