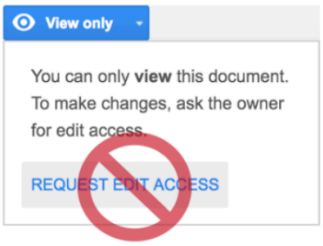
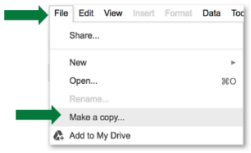
Strike Graph

Personnel Security Policy Template



How to use this template:

This is a view-only file and cannot be edited. **Create your own copy** of this template to edit. In the menu, click **File > Make a copy...**



Strike Graph

Strike Graph Notes:

Our Personnel Security policy template helps you define how people are screened, granted access, moved, and offboarded in a CMMC-aligned way. It covers role risk designations, background checks, transfers, terminations, and third-party personnel. Evidence typically comes from HR records and access logs, while common pitfalls include vague timelines, misaligned HR processes, and undocumented access changes.

Policy #:	Title:	Effective Date:
x.xxx	Personnel Security Policy	MM/DD/YY

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Personnel Security (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800 -100; Electronic Code of Federal Regulations (CFR): 5 CFR 731.106; Federal Information Processing Standards (FIPS) 199 and 201; Intelligence Community Directive (ICD) 704 Personnel Security Standards

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. POSITION RISK DESIGNATION

Strike Graph Notes:
Explain that this is how you label each role as low/medium/high risk, tie it to your HR job catalog, and define who owns those designations. Gather HR job descriptions, existing background-check tiers, and regulatory requirements; avoid generic “all roles are the same” risk labels that auditors will challenge.

Information Technology (IT) shall:

a. Assign a risk designation to all positions.

b. Establish screening criteria for individuals filling those positions.

c. Review and update position risk designations [entity defined frequency].

2. PERSONNEL SCREENING

Strike Graph Notes:
This part is simple and tells you exactly where to plug in your rescreening rules in brackets. Tailor it by mapping risk designations to specific checks (e.g., basic check vs. enhanced, frequency of rescreening for high-risk roles) and aligning to local labor law. Gather your HR background-check policy, vendor contracts, and any union/legal constraints.

IT and department system and application owners shall:

a. Screen individuals prior to authorizing access to the information systems.

b. Rescreen individuals according to [entity defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

c. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

3. PERSONNEL TERMINATION

Strike Graph Notes:
The template is simple and tells you exactly where to plug in your rescreening rules in brackets. Tailor it by mapping risk designations to specific checks (e.g., basic check vs. enhanced, frequency of rescreening for high-risk roles) and aligning to local labor law. Gather your HR background-check policy, vendor contracts, and any union/legal constraints. Pitfalls include promising rescreening you don't actually do, or using vague "periodic" language with no defined timeframe.

Departments shall, upon termination of individual employment:

a. Disable information system access within [entity defined time period].

b. Terminate/revoke any authenticators/credentials associated with the individual.

c. Conduct exit interviews that include a discussion of [entity defined information security topics].

d. Retrieve all security-related information system-related property.

e. Retain access to information and information systems formerly controlled by terminated individual.

f. Notify [entity defined personnel or roles] within [entity defined time period].

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

The entity shall:

g. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.

h. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).

i. Employ automated mechanisms to notify [entity defined personnel or roles] upon termination of an individual.

4. PERSONNEL TRANSFER

Strike Graph Notes:
In this section clarify that the goal is to prevent access "bloat" when people change roles. Use the brackets to define required actions (access review, removal of old rights, assignment of new rights) and the time window after transfer is recorded. Align this with HR system updates and line-manager approvals so changes aren't missed. Gather current "mover" workflows, org charts, and access review procedures. A common gap is letting staff keep privileged or legacy access months after moving teams.

Departments shall:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.

b. Initiate [entity defined transfer or reassignment actions] within [entity defined time period following the formal transfer action].

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

d. Notify [entity defined personnel] within [entity defined time period] of transfer.

e. This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

5. ACCESS AGREEMENTS

Strike Graph Notes:
This is where you formalize NDAs, acceptable use, and rules of behavior, with the "[entity defined frequency]" brackets guiding how often people must re-sign. Tailor it by pointing to your real forms or electronic click-throughs and by deciding triggers: new systems, major policy updates, or every X years. Gather current AUPs, onboarding packets, and HR policy handbooks. Pitfalls: outdated wording, no central record of who signed what, or not requiring re-signatures after big changes.

Departments shall:

a. Develop and document access agreements for information systems.

b. Review and update the access agreements [entity defined frequency].

c. Ensure that individuals requiring access to information and information systems:

   i. Sign appropriate access agreements prior to being granted access.

   ii. Re-sign access agreements to maintain access to information systems when access agreements have been updated or [entity defined frequency].

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

6. THIRD-PARTY PERSONNEL SECURITY

Strike Graph Notes:
In this section describe how you build people-related security into contracts and

vendor onboarding. Spell out which third parties are in scope (e.g., MSPs, developers, cloud providers), what background checks or clearances you require, and how they must handle badges, credentials, and terminations. Gather: standard contract clauses, vendor risk procedures, and the list of systems vendors touch. Common pitfalls include vague "vendor will comply with policy" language, no defined notification window for staff changes, and not monitoring that subcontractors follow the same rules.

IT Department shall:

a. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.

b. Require third-party providers to comply with personnel security policies and procedures established by the entity.

c. Require third-party providers to notify [entity defined personnel] of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within [entity defined time period].

d. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

7. PERSONNEL SANCTIONS

Strike Graph Notes:
This section turns policy violations into a predictable outcome, and again uses brackets so you can name who gets notified and how quickly. Explain that this defines your formal disciplinary pathway for security incidents and must align tightly with HR's employee handbook and legal guidance. Gather HR disciplinary procedures, union or country-specific rules, and your incident response plan.

Avoid promising sanctions you can't apply consistently or leaving the process so vague that managers "handle it their own way."

IT and HR shall:

a. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures

b. Notify [entity defined personnel] within [entity defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

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.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY