NIST 800-171

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

30	NIST 800-171 3.3.3 - Event Review
31	NIST 800-171 3.3.4 - Audit Failure Alerting
32	NIST 800-171 3.3.5 - Audit Correlation
33	NIST 800-171 3.3.6 - Reduction & Reporting
34	NIST 800-171 3.3.7 - Authoritative Time Source
35	NIST 800-171 3.3.8 - Audit Protection
36	NIST 800-171 3.3.9 - Audit Management
37	NIST 800-171 3.4.1 - System Baselining
38	NIST 800-171 3.4.2 - Security Configuration Enforcement
39	NIST 800-171 3.4.3 - System Change Management
40	NIST 800-171 3.4.4 - Security Impact Analysis
41	NIST 800-171 3.4.5 - Access Restrictions for Change
42	NIST 800-171 3.4.6 - Least Functionality
43	NIST 800-171 3.4.7 - Nonessential Functionality
44	NIST 800-171 3.4.8 - Application Execution Policy
45	NIST 800-171 3.4.9 - User-Installed Software
46	NIST 800-171 3.5.1 - Identification
47	NIST 800-171 3.5.2 - Authentication
48	NIST 800-171 3.5.3 - Multifactor Authentication
49	NIST 800-171 3.5.4 - Replay-Resistant Authentication
50	NIST 800-171 3.5.5 - Identifier Reuse
51	NIST 800-171 3.5.6 - Identifier Handling
52	NIST 800-171 3.5.7 - Password Complexity
53	NIST 800-171 3.5.8 - Password Reuse
54	NIST 800-171 3.5.9 - Temporary Passwords
55	NIST 800-171 3.5.10 - Cryptographically-Protected Passwords
56	NIST 800-171 3.5.11 - Obscure Feedback
57	NIST 800-171 3.6.1 - Incident Handling
58	NIST 800-171 3.6.2 - Incident Reporting
59	NIST 800-171 3.7.1 - Perform Maintenance
60	NIST 800-171 3.7.2 - System Maintenance Control

61	NIST 800-171 3.7.3 - Equipment Sanitization
62	NIST 800-171 3.7.4 - Media Inspection
63	NIST 800-171 3.7.5 - Nonlocal Maintenance
64	NIST 800-171 3.7.6 - Maintenance Personnel
65	NIST 800-171 3.8.1 - Media Protection
66	NIST 800-171 3.8.2 - Media Access
67	NIST 800-171 3.8.3 - Media Disposal
68	NIST 800-171 3.8.4 - Media Markings
69	NIST 800-171 3.8.5 - Media Accountability
70	NIST 800-171 3.8.7 - Removable Media
71	NIST 800-171 3.8.8 - Shared Media
72	NIST 800-171 3.8.9 - Protect Backups
73	NIST 800-171 3.9.1 - Screen Individuals
74	NIST 800-171 3.9.2 - Personnel Actions
75	NIST 800-171 3.10.1 - Limit Physical Access
76	NIST 800-171 3.10.2 - Monitor Facility
77	NIST 800-171 3.10.3 - Escort Visitors
78	NIST 800-171 3.10.4 - Physical Access Logs
79	NIST 800-171 3.10.5 - Manage Physical Access Devices
80	NIST 800-171 3.10.6 - Alternative Work Sites
81	NIST 800-171 3.11.1 - Risk Assessments
82	NIST 800-171 3.11.2 - Vulnerability Scan
83	NIST 800-171 3.11.3 - Vulnerability Remediation
84	NIST 800-171 3.12.1 - Security Control Assessment
85	NIST 800-171 3.12.2 - Plan of Action
86	NIST 800-171 3.12.3 - Security Control Monitoring
87	NIST 800-171 3.12.4 - System Security Plan
88	NIST 800-171 3.13.2 - Security Engineering
89	NIST 800-171 3.13.3 - Role Separation
90	NIST 800-171 3.13.4 - Shared Resource Control
91	NIST 800-171 3.13.5 - Public-Access System Separation

92	NIST 800-171 3.13.6 - Network Communication by Exception
93	NIST 800-171 3.13.8 - Data in Transit
94	NIST 800-171 3.13.9 - Connections Termination
95	NIST 800-171 3.13.10 - Key Management
96	NIST 800-171 3.13.11 - CUI Encryption
97	NIST 800-171 3.13.12 - Collaborative Device Control
98	NIST 800-171 3.13.13 - Mobile Code
99	NIST 800-171 3.13.14 - Voice over Internet Protocol
100	NIST 800-171 3.13.15 - Communications Authenticity
101	NIST 800-171 3.13.16 - Data at Rest
102	NIST 800-171 3.14.1 - Flaw Remediation
103	NIST 800-171 3.14.2 - Malicious Code Protection
104	NIST 800-171 3.14.3 - Security Alerts & Advisories
105	NIST 800-171 3.14.4 - Update Malicious Code Protection
106	NIST 800-171 3.14.5 - System & File Scanning
107	NIST 800-171 3.14.6 - Monitor Communications for Attacks
108	NIST 800-171 3.14.7 - Identify Unauthorized Use
109	NIST 800-171 3.8.6 - Portable Storage Encryption
110	NIST 800-171 3.13.7 - Split Tunneling
111	NIST 800-171 3.6.3 - Incident Response Testing
112	NIST 800-171 3.1.16 - Wireless Access Authorization
113	NIST 800-171 3.13.1 - Boundary Protection

Purpose

The purpose is to ensure that qualifying defense contractors and subcontractors meet all the requirements defined in DFARS and FAR contractual obligations and associated guidance.

Scope

This policy applies to the workforce members of defense contractors or subcontractors that access, process, or store Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

NIST 800-171 3.1.1 - Limit System Access

NIST 800-171	Other Requirements
3.1.1 Limit System Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Guidance
This requirement focuses on account management for systems and applications. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement AC.L1-3.1.2.

Identify users, processes, and devices that are allowed to use company computers and can log on to the company network. Automated updates and other automatic processes should be associated with the user who initiated (authorized) the process. Limit the devices (e.g., printers) that can be accessed by company computers. Set up your system so that only authorized users, processes, and devices can access the company network.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.11 - Access Termination: Implement procedures for terminating access when the employment of a workforce member ends or as required by other determinations.
- CC7.12 - Limit Access: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.2 - Limit Transactions & Functions

NIST 800-171	Other Requirements
3.1.2 Limit Transactions & Functions	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Guidance
Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.9 - Workforce Authorization & Supervision: Implement procedures for the authorization and/or supervision of workforce members.
- CC7.13 - Limit Functions: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.3 - Control CUI Flow

NIST 800-171	Other Requirements
3.1.3 Control CUI Flow	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Control the flow of CUI in accordance with approved authorizations.

Guidance
Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the internet; blocking outside traffic that claims to be from within the organization; restricting requests to the internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST SP 800-41 provides guidance on firewalls and firewall policy. SP 800-125B provides guidance on security for virtualization technologies.

In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes: prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC1.4 - Data Flow Management: Ensure that a baseline of network operations and expected data flows for users and systems is established and managed.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.4 - Separation of Duties

NIST 800-171	Other Requirements
3.1.4 Separation of Duties	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Guidance
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.4 - Access Permission Management: Manage access permissions, incorporating the principles of least privilege and separation of duties.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.5 - Least Privilege

NIST 800-171	Other Requirements
3.1.5 Least Privilege	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Employ the principle of least privilege, including for specific security functions and privileged accounts.

Guidance
Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.4 - Access Permission Management: Manage access permissions, incorporating the principles of least privilege and separation of duties.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.6 - Non-Privileged Account Use

NIST 800-171	Other Requirements
3.1.6 Non-Privileged Account Use	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Use non-privileged accounts or roles when accessing nonsecurity functions.

Guidance
This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non- privileged account.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.23 - Using Privileged Accounts: Use non-privileged accounts or roles when accessing nonsecurity functions. Use privileged accounts only when performing functions requiring them.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.7 - Privileged Functions

NIST 800-171	Other Requirements
3.1.7 Privileged Functions	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Prevent non-privileged users from executing privileged functions and audit the execution of such functions in audit logs.

Guidance
Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2 (AC.L1-3.1.2).

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.29 - Privileged Functions: Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.8 - Unsuccessful Logon Attempts

NIST 800-171	Other Requirements
3.1.8 Unsuccessful Logon Attempts	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Limit unsuccessful logon attempts.

Guidance
This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.24 - Limit Unsuccessful Logons: Limit unsuccessful logon attempts.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.9 - Privacy & Security Notices

NIST 800-171	Other Requirements
3.1.9 Privacy & Security Notices	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Provide privacy and security notices consistent with applicable CUI rules.

Guidance
This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.21 - Privacy & Security Notices: Provide privacy and security notices consistent with applicable rules.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.10 - Session Lock

NIST 800-171	Other Requirements
3.1.10 Session Lock	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.

Guidance
Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC13.13 - Session Lock: Use session lock with pattern-hiding displays to prevent access/viewing of data after a period of inactivity.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.11 - Session Termination

NIST 800-171	Other Requirements
3.1.11 Session Termination	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Terminate (automatically) a user session after a defined condition.

Guidance
This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.30 - Terminate Sessions: Terminate (automatically) user sessions after a defined condition.
- CC8.26 - Terminate Sessions: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

NIST 800-171 3.1.12 - Control Remote Access

NIST 800-171	Other Requirements
3.1.12 Control Remote Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Monitor and control remote access sessions.

Guidance
Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

NIST SP 800-46, SP 800-77, and SP 800-113 provide guidance on secure remote access and virtual private networks.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.3 - Remote Access Management: Manage remote access to assets.

References
- NIST 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A Self-Assessment Methodology - https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Submitting Self-Assessment Score to SPRS - https://www.sprs.csd.disa.mil/nistsp.htm

Truncated Sample Report