POL-AC-01 — Access Control Policy v2.0

Document ID: POL-AC-01 **Title:** Access Control Policy **Version:** 2.0 **Effective Date:** 2025-11-11 **Classification:** Internal Use / Client Facing **Owner:** Information Security Officer (ISO) **Approved By:** [Executive Sponsor / Client Representative] **Review Cycle:** Annually or upon major change **Related Policies:** POL-IS-00 (Information Security Program Charter), POL-IA-05 (Identification & Authentication), POL-SC-13 (System Communications & Data Protection), POL-PS-09 (Personnel Security), POL-AU-03 (Audit & Logging)

---

1. Purpose

This policy defines the principles and responsibilities governing logical and physical access to information systems to ensure that only authorized individuals and processes can access organizational or Controlled Unclassified Information (CUI).

It enforces the principle of **least privilege** and supports compliance with NIST SP 800-171 Rev 2 and CMMC Level 2 access control requirements.

---

2. Scope

This policy applies to: - All users, devices, and systems accessing organizational or client networks (on-premises, cloud-based, or remote) - All employees, contractors, consultants, vendors, and managed service providers granted access to information assets - All systems storing, processing, or transmitting CUI - Physical access to facilities where CUI is accessed or stored

---

3. Policy Statement

Access shall be: - **Authorized** based on legitimate business need - **Authenticated** using approved identification methods (see POL-IA-05) - **Monitored** through audit logging and periodic reviews

Unauthorized access or use of systems or data is strictly prohibited.

---

4. Access Control Principles

4.1 Least Privilege

Users receive **only** the access necessary to perform their assigned duties. Excessive privileges are prohibited.

Implementation: - Default user accounts have minimal permissions - Elevated privileges granted only when justified and approved - Administrative access separated from standard user access - Temporary elevated access revoked immediately after use

---

4.2 Need-to-Know

Access to sensitive or client-specific data (especially CUI) is limited to those with a documented business justification.

Implementation: - CUI access requires documented approval - Data classification drives access decisions (see POL-SC-13) - Compartmentalization of sensitive projects

---

4.3 Segregation (Separation) of Duties

No individual shall have conflicting responsibilities that could enable abuse of privileges (e.g., person who approves changes should not be the sole person implementing changes).

Implementation: - Change management approval separate from implementation (see POL-CM-04) - Financial system controls separate authorization from execution - Security control implementation reviewed by independent party

---

4.4 Periodic Access Reviews

Periodic reviews validate appropriateness of user rights and identify excessive or stale privileges.

Frequency: Quarterly minimum (monthly recommended for privileged accounts)

Required Artifact: REF-AC-01 — Quarterly Access Review Log

4.5 Session Management

Systems enforce automatic session controls to prevent unauthorized access to unattended workstations.

Requirements: - **Screen lock:** Automatically after **15 minutes** of inactivity maximum (10 minutes recommended for CUI systems) - **Session termination:** Automatic logoff after **30 minutes** of inactivity for remote sessions - Users must manually lock screens when leaving workstations unattended

---

5. Account Management

5.1 Unique User Accounts

All user accounts must be **uniquely identifiable** and traceable to an individual.

Shared or generic accounts are prohibited unless: - Approved in writing by ISO or Executive Sponsor - Documented business or technical justification exists - Logged in **REF-AC-02** — Privileged Account Register - Subject to enhanced monitoring

Examples of prohibited shared accounts: “admin”, “support”, “helpdesk” used by multiple people

---

5.2 Account Provisioning

New accounts require: 1. Documented access request (**REF-AC-03** — Access Request Form) 2. Approval by: - Manager or supervisor (standard access) - ISO or system owner (privileged or CUI access) - Executive Sponsor (administrative or high-risk access) 3. Verification of onboarding requirements (background check, security training complete)

Provisioning timeline: Within **5 business days** of approval

Required Artifact: REF-AC-03 — Access Request Forms

5.3 Privileged Account Management

Administrative privileges require explicit written approval and enhanced controls.

Privileged accounts include: - Domain administrators - Local administrator accounts - Database administrators (DBA) - Cloud platform administrators (Azure Global Admin, AWS Root) - Security tool administrators (firewall, SIEM, EDR)

Privileged Account Requirements: - Documented in **REF-AC-02** — Privileged Account Register - Separate from standard user accounts (e.g., “john.doe” for email, “john.doe-admin” for admin tasks) - **Multi-Factor Authentication (MFA) mandatory** - Enhanced monitoring and audit logging - Quarterly access reviews (monthly recommended) - Session recording for high-risk administrative actions (optional but recommended)

Required Artifact: REF-AC-02 — Privileged Account Register

5.4 Account Deprovisioning and Termination

Accounts must be **promptly disabled or removed** when no longer required.

Scenario	Action	Timeline

Employee termination	Disable all access immediately	Within **24 hours** of termination notification
Contractor end of engagement	Disable all access	Within **24 hours** of contract end or last day
Role change (no longer needs access)	Remove unnecessary permissions	Within **5 business days** of role change
Extended leave (>30 days)	Disable account (retain for return)	Before leave begins
Account inactive >90 days	Flag for review and potential disablement	Quarterly access review

Termination Checklist Integration: - HR coordinates with IT/MSP for immediate access revocation - Access termination logged in **REF-AC-04** — Account Termination Log - Badge/key return verified before final paycheck

Required Artifact: REF-AC-04 — Account Termination Log

5.5 Default and System Accounts

Default passwords on new systems must be changed before deployment to production.

System and service accounts: - Use strong passwords (20+ characters) or certificate-based authentication - Documented in **REF-AC-02** — Privileged Account Register - Not used for interactive login by individuals - Password changes after any personnel with knowledge departs

---

6. Remote and Third-Party Access

6.1 Remote Access Requirements

Remote access to organizational systems or CUI requires: - **Approved VPN or Zero-Trust Network Access (ZTNA)** solution - **Multi-Factor Authentication (MFA)** for all remote connections - **Encryption** of all data in transit (TLS 1.2+ or IPSec) - **Session logging** of connection times, user, source IP, and duration

Split tunneling prohibition: See POL-SC-13 for VPN split tunneling restrictions

Required Artifact: REF-SC-04 — Remote Access Authorization Log

---

6.2 Third-Party and Vendor Access

Vendors and contractors are provided **restricted access** through defined onboarding procedures.

Third-Party Access Requirements: - Time-bound access (definedexpiration date) - Least privilege (access only to systems necessary for contracted work) - Separate accounts from employees (identifiable as contractor/vendor) - MFA required - Enhanced logging and monitoring - NDA and security requirements in vendor contract

Access reviews for vendors: Quarterly minimum

Required Artifact: REF-TP-03 — Third-Party Access Register (see POL-TP-16)

---

7. Access Reviews and Logging

7.1 Quarterly Access Reviews

Frequency: Quarterly minimum (monthly for privileged accounts)

Review Process: 1. IT/MSP exports current user list with permissions 2. Managers/supervisors validate direct reports' access is appropriate 3. ISO reviews privileged accounts 4. Identify and document excessive privileges, stale accounts, or anomalies 5. Remediate findings within **30 days** 6. Document review in **REF-AC-01** — Quarterly Access Review Log with signatures

Required Artifact: REF-AC-01 — Quarterly Access Review Log

7.2 Access Logging

Access logs shall capture: - Successful and failed authentication attempts - Privilege escalations or elevation - Account creations, modifications, deletions - Access to CUI data or systems - Session logons and logoffs - Changes to access control configurations (group memberships, permissions)

Log retention: Minimum **1 year** (3 years recommended)

Log review: See POL-AU-03 Audit & Logging Policy

---

8. Roles & Responsibilities

Role	Responsibility
Executive Sponsor	Approves high-risk access requests. Reviews quarterly access metrics. Ensures budget for access control tools (MFA, IAM platforms).

Information Security Officer (ISO)	Approves privileged and CUI access requests. Oversees quarterly access reviews. Maintains Privileged Account Register (REF-AC-02). Enforces least privilege principle.
Compliance Specialist (CS)	Maintains access control documentation (REF-AC-01 through REF-AC-04). Ensures evidence is audit-ready. Tracks access review completion.
IT Owner / MSP	Provisions and deprovisions accounts. Implements technical access controls (MFA, session timeouts, group policies). Generates quarterly access reports. Logs access events.
Human Resources (HR)	Notifies IT immediately of terminations, role changes, and extended leave. Coordinates with IT on access termination checklist. Verifies security training completion before access granted.
Managers / Supervisors	Approve access requests for direct reports. Participate in quarterly access reviews (validate team members' access). Report role changes or departures immediately.
All Users	Use only authorized access. Do not share credentials. Lock screens when leaving workstations. Report suspicious account activity.

---

9. Enforcement

Non-compliance may result in: - **Immediate:** Access revocation during investigation - **First offense (minor):** Written warning and re-training - **Repeat or serious violations:** Termination of employment or contract - **Unauthorized CUI access:** Criminal penalties under 18 USC 1030 (Computer Fraud and Abuse Act)

All violations are subject to incident reporting under **POL-IR-06** Incident Response Plan and logged in **REF-IR-02** Incident Register.

---

10. Keystone Insights: Access Control

From the Perspective of an NSA Technical Director and Mission-Critical System Owner

What C3PAOs Actually Check

- **Access review logs with signatures** - They want to see quarterly reviews with dated evidence. "We review access" means nothing without signed documentation showing WHO reviewed WHAT and WHEN. No signatures = no evidence = finding.
- **Privileged account register** - They will ask for a complete list of all admin accounts with business justification for each. "IT needs admin" is not sufficient justification. You need specific role-based justifications (e.g., "Server administrator - manages CUI application servers - approved by ISO on [date]").

- **Session timeout configuration** - They will test this live during the assessment. They'll log in, walk away, and time how long it takes for the screen lock to engage. 15 minutes for CUI systems is the maximum. Anything longer = finding.

Common Contractor Mistakes

- **Shared credentials** - "We're a small team of 5, so we share the admin password" is a critical violation. Every human gets their own account. Service accounts (for applications, not people) are separate and documented.
- **Stale accounts** - Terminated employee accounts still active 6 months later = automatic finding. Access termination within 24 hours of departure is non-negotiable. Integrate access management with HR processes so terminations trigger immediate IT action.
- **Over-privileged users** - Everyone having domain admin "because it's easier" = assessment failure. Least privilege is not a suggestion—it's a requirement. 80%+ of users should have standard (non-privileged) accounts.

Time-Saving Shortcuts

- **Group-based access control** - Assign permissions to Active Directory groups or IAM roles, not individual users. Makes quarterly reviews 10x faster. Instead of reviewing 50 individual permissions, you review 5 group memberships.
- **Automated alerting** - Configure privileged account usage alerts in your SIEM or log management tool. Real-time alerts when admin accounts are used catch anomalies before audits and demonstrate proactive monitoring.

The Non-Negotiables

- **Multi-factor authentication on privileged accounts** - This is pass/fail for CMMC Level 2. No MFA on admin accounts = you don't pass. Period. Cloud providers (Azure, AWS, GCP) all support MFA natively. Enable it.
- **Access termination within 24 hours** - When someone leaves or changes roles, their access changes immediately. Document the process (HR notifies IT, IT disables accounts, HR verifies before final pay) and execute it consistently. C3PAOs will sample recent terminations and check access logs.

Real-World Application

On TS/SCI systems, we maintained privileged access registers that could be audited in under 10 minutes because we automated the data collection. Every quarterly review was 90% pre-populated from AD queries—group memberships, last login dates, password age. The 10% human review was for justification validation ("Does this person still need domain admin access? Yes/No").

We enforced separation of duties religiously: developers couldn't deploy to production, system admins couldn't approve their own changes, and security team validated controls they didn't implement. When auditors arrived, we handed them dated access review logs with signatures—no scrambling, no excuses.

That's the standard you should aim for—because C3PAOs move fast during assessments. If you can't produce a privileged account register in under 5 minutes, or your last access review was 8 months ago, you're demonstrating a reactive (not proactive) security posture. CMMC rewards proactive discipline.

Appendix A — NIST SP 800-171 Control Mapping

NIST SP 800-171 Control	Control Name	Policy Section
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices	§5
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute	§4.1, §5
3.1.3	Control the flow of CUI in accordance with approved authorizations	§4.2
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity	§4.3
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts	§4.1, §5.3
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions	§5.3
3.1.7	Prevent non-privileged users from executing privileged functions	§5.3
3.1.8	Limit unsuccessful logon attempts	§7.2
3.1.9	Provide privacy and security notices consistent with applicable CUI rules	§3 (policy statement)
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity	§4.5
3.1.11	Terminate (automatically) a user session after a defined condition	§4.5
3.1.12	Monitor and control remote access sessions	§6.1
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions	§6.1
3.1.14	Route remote access via managed access	§6.1

	control points	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information	§6.1
3.1.16	Authorize wireless access prior to allowing such connections	§6 (general remote access controls)
3.1.17	Protect wireless access using authentication and encryption	§6.1
3.1.18	Control connection of mobile devices	§6 (remote access; see also POL-AU-17 BYOD)
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms	See POL-SC-13
3.1.20	Verify and control/limit connections to and use of external information systems	§6.2 (third-party access)
3.1.21	Limit use of organizational portable storage devices on external information systems	See POL-MP-08 Media Protection
3.1.22	Control CUI posted or processed on publicly accessible information systems	§4.2 (need-to-know, CUI compartmentalization)

Appendix B — Evaluation Criteria (Evidence Collection)

Evaluation Area	Evidence Required	Evaluation Method
User authorization	REF-AC-03 Access Request Forms	Review of approvals and ticket records; sample 5-10 recent requests
Privileged account management	REF-AC-02 Privileged Account Register	Verify all admin accounts documented with justifications
Privilege review	REF-AC-01 Quarterly Access Review Logs	Cross-check with user directory; verify reviews within past 90 days
MFA implementation	System configuration export (Azure AD, Active Directory, VPN)	Verify MFA enabled for all privileged accounts; test live during assessment
Account deactivation	REF-AC-04 Account Termination Log cross-referenced with HR termination records	Sample 5-10 recent terminations; verify access disabled within 24 hours
Session timeout	Live testing	Assessor will log in and wait to verify screen lock engages ≤15 minutes
Remote access	REF-SC-04 Remote Access	Verify MFA, encryption, and

controls	Authorization Log	logging for remote sessions

Appendix C — Supporting Reference Registers

Ref ID	Name	Purpose
REF-AC-01	Quarterly Access Review Log	Documents periodic access reviews with signatures and findings
REF-AC-02	Privileged Account Register	Tracks all administrative accounts with justifications
REF-AC-03	Access Request Forms	Standardized form for requesting new access or permission changes
REF-AC-04	Account Termination Log	Tracks timely deprovisioning of terminated/departing personnel

Appendix D — Related References

- NIST SP 800-171 Rev 2 Family 3.1 (Access Control)
- NIST SP 800-53 Rev 5 AC Control Family (additional guidance)
- CMMC Level 2 Practices AC.L2-3.1.x
- DFARS 252.204-7012
- POL-IS-00 Information Security Program Charter
- POL-IA-05 Identification & Authentication Policy
- POL-SC-13 System Communications & Data Protection Policy
- POL-PS-09 Personnel Security Policy
- POL-AU-03 Audit & Logging Policy

Appendix E — Revision History

Version	Date	Author	Changes
2.0	2025-11-11	Austin McGuire	Renamed from POL-AC-02 to POL-AC-01. Updated all policy cross-references to new codes. Enhanced privileged account management, account termination procedures, and remote access requirements. Added detailed session management controls. Added Keystone Insights section. Aligned to NIST SP 800-171 Rev 2 and CMMC Level 2.
1.0	2025-11-11	Austin McGuire	Initial version

END OF DOCUMENT