Access Control Policy

Organization: AegisCISO
Document ID: POL-ACC-001
Version: 1.0
Effective Date: January 2026
Classification: Internal
Owner: Chief Information Security Officer (CISO)

1. Purpose

This policy establishes requirements for controlling access to AegisCISO information systems and data to ensure that only authorized users can access resources appropriate to their roles.

2. Scope

This policy applies to:

- All information systems and applications
- All users including employees, contractors, and third parties
- All access methods (local, remote, API)
- All data and information assets

3. Access Control Principles

3.1 Principle of Least Privilege

POL-ACC-001-01: Access shall be limited to the minimum necessary.

Requirements:

- Users receive only access required for job functions
- Elevated privileges granted only when justified
- Access removed when no longer required
- Default deny for all access requests

3.2 Segregation of Duties

POL-ACC-001-02: Critical functions shall require multiple individuals.

Requirements:

- No single person controls entire transaction
- Development and production access separated
- Request and approval functions separated
- Audit and operational functions separated

3.3 Need-to-Know Basis

POL-ACC-001-03: Access to sensitive data requires business justification.

Requirements:
- Data access linked to specific business need
- Access removed when project/task complete
- Sensitive data access logged
- Regular justification review

4. User Access Management

4.1 User Registration

POL-ACC-001-04: Formal user registration process shall be followed.

Requirements:
- Unique user ID assigned to each person
- Shared accounts prohibited (except documented exceptions)
- User ID linked to identity verification
- Account creation logged

4.2 Access Request and Approval

POL-ACC-001-05: Access requests shall follow formal approval process.

Access Type	Approver	Additional Requirements
Standard system access	Direct manager	Business justification
Sensitive data access	Data owner + manager	Enhanced justification
Privileged access	Manager + Security	Background check verified
Production access	Change manager	Change ticket reference
Third-party access	Vendor manager + Security	Contract verification

4.3 Access Provisioning

POL-ACC-001-06: Access shall be provisioned based on role definitions.

Requirements:
- Role-Based Access Control (RBAC) implemented
- Standard role definitions maintained
- Role assignments documented
- Provisioning within 24 hours of approval
- Automated provisioning where possible

4.4 Access Review

POL-ACC-001-07: User access shall be reviewed regularly.

Access Type	Review Frequency	Reviewer
All user access	Quarterly	Manager
Privileged access	Monthly	Security + Manager

Third-party access	Monthly	Vendor manager
Service accounts	Quarterly	System owner
Dormant accounts	Monthly	IT Security

4.5 Access Modification

POL-ACC-001-08: Access changes shall be managed.

Requirements:

- Role change triggers access review within 5 days
- Transfer between departments requires full review
- Promotion to privileged role requires enhanced verification
- Temporary access has defined expiration

4.6 Access Termination

POL-ACC-001-09: Access shall be removed promptly upon termination.

Termination Type	Access Removal
Voluntary resignation	Last day of employment
Involuntary termination	Before notification (when possible)
Contractor end	Contract end date
Transfer to new role	Upon role change

5. Authentication Requirements

5.1 Password Policy

POL-ACC-001-10: Password requirements for standard accounts.

Requirement	Standard Users	Privileged Users
Minimum length	12 characters	16 characters
Complexity	Upper, lower, number, special	Upper, lower, number, special
History	12 passwords	24 passwords
Maximum age	90 days	60 days
Minimum age	1 day	1 day
Lockout threshold	5 attempts	3 attempts
Lockout duration	30 minutes	Manual unlock

5.2 Multi-Factor Authentication

POL-ACC-001-11: MFA requirements.

MFA Required For:

- All remote access (VPN, cloud)
- All privileged accounts

- All access to sensitive data
- All administrative interfaces
- All external-facing systems

Approved MFA Methods:

- Hardware security keys (FIDO2/WebAuthn) - Preferred
- Authenticator applications (TOTP)
- Push notifications from approved apps
- SMS/Voice (limited use, for recovery only)

5.3 Single Sign-On

POL-ACC-001-12: SSO implementation requirements.

Requirements:

- Enterprise SSO for all compatible applications
- Federation with approved identity providers only
- Session timeout configured
- Re-authentication for sensitive operations

5.4 Service Account Authentication

POL-ACC-001-13: Service account requirements.

Requirements:

- Unique service account per application/service
- Strong passwords or certificates
- No interactive logon permitted
- Password vault storage mandatory
- Regular credential rotation

6. Authorization Requirements

6.1 Role-Based Access Control

POL-ACC-001-14: RBAC shall be implemented.

Requirements:

- Standard roles defined for each system
- Role definitions documented and approved
- Role assignment based on job function
- Conflicting roles identified and controlled

6.2 Attribute-Based Access Control

POL-ACC-001-15: ABAC for fine-grained access control.

Attributes considered:

- User role and department
- Data classification

- Time of access
- Location/network
- Device compliance

6.3 Access to Sensitive Data

POL-ACC-001-16: Enhanced controls for sensitive data.

Data Classification	Access Requirements
Public	Standard authentication
Internal	Authentication + authorization
Confidential	MFA + need-to-know + logging
Restricted	MFA + approval + enhanced logging + DLP

7. Privileged Access Management

7.1 Privileged Account Inventory

POL-ACC-001-17: Privileged accounts shall be inventoried.

Requirements:

- All privileged accounts documented
- Account owners identified
- Purpose and justification documented
- Regular inventory review

7.2 Privileged Access Controls

POL-ACC-001-18: Enhanced controls for privileged access.

Requirements:

- Just-in-time (JIT) access preferred
- Privileged Access Workstations (PAW) for administration
- Session recording for sensitive systems
- Approval workflow for elevated access
- Time-limited privilege escalation

7.3 Privileged Account Monitoring

POL-ACC-001-19: Privileged account activity shall be monitored.

Requirements:

- All privileged sessions logged
- Real-time alerting on anomalies
- Regular log review
- Deviation investigation

8. Remote Access

8.1 Remote Access Requirements

POL-ACC-001-20: Remote access controls.

Requirements:

- VPN mandatory for corporate network access
- MFA required for all remote access
- Device compliance check before access
- Split tunneling prohibited
- Session timeout configured

8.2 Third-Party Remote Access

POL-ACC-001-21: Third-party remote access controls.

Requirements:

- Dedicated access credentials
- Time-limited access
- Session monitoring
- Approval for each session
- Activity logging

9. Physical Access

9.1 Facility Access

POL-ACC-001-22: Physical access controls.

Requirements:

- Badge-based access control
- Visitor registration and escort
- Access logging maintained
- Regular badge audit
- Immediate deactivation upon termination

9.2 Data Center Access

POL-ACC-001-23: Data center access controls.

Requirements:

- Limited to authorized personnel only
- MFA for data center entry
- Visitor escort required
- Access logging with video
- Regular access review

10. Audit and Monitoring

10.1 Access Logging

POL-ACC-001-24: Access events shall be logged.

Events to log:

- Successful and failed authentication
- Authorization decisions
- Privilege escalation
- Access to sensitive data
- Administrative actions
- Account changes

10.2 Access Monitoring

POL-ACC-001-25: Access patterns shall be monitored.

Requirements:

- Automated anomaly detection
- Failed login alerting
- Off-hours access alerting
- Geographic anomaly detection
- Behavior analytics

11. Compliance

11.1 Regulatory Requirements

This policy supports compliance with:

- NCA Essential Cybersecurity Controls (ECC-1: 2-7)
- ISO/IEC 27001:2022 - A.9 Access Control
- GDPR (access control requirements)
- PCI DSS - Requirement 7, 8

11.2 Access Compliance Reporting

Requirements:

- Monthly access review completion reports
- Quarterly privileged access reports
- Annual access control assessment
- Audit finding remediation tracking

12. Exceptions

Exception requirements:

- Business justification
- Risk assessment
- Compensating controls

- Time-limited approval
- CISO approval
- Regular review

13. Roles and Responsibilities

CISO

- Policy ownership
- Exception approval

IT Security

- Access control implementation
- Monitoring and alerting
- Access reviews coordination

System Owners

- Role definitions
- Data classification
- Access approvals

Managers

- Access request approval
- Access review certification
- Termination notification

Users

- Credential protection
- Policy compliance
- Incident reporting

14. Enforcement

Violations may result in:

- Access revocation
- Disciplinary action
- Investigation
- Termination

15. Review

Annual review for:

- Regulatory changes
- Technology updates
- Incident lessons learned

- Industry best practices

16. References

- NCA Essential Cybersecurity Controls
- ISO/IEC 27001:2022
- NIST SP 800-53 (Access Control)
- CIS Controls

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release