OKLAHOMA COUNTY

PASSWORD AND ACCESS MANAGEMENT POLICY

Information Technology Operations

Aligned with CJIS Security Policy | NIST SP 800-53 | CIS Controls v8

Document ID:	IT-POL-PAM-001
Version:	1.0
Effective Date:	[Date of BOCC Resolution]
Last Reviewed:	[Date]
Classification:	Internal Use
Document Owner:	Director of MIS
Approved By:	Board of County Commissioners — Resolution No. [____]

CONFIDENTIAL — FOR OFFICIAL USE ONLY

Table of Contents

1. Purpose

This Password and Access Management Policy establishes the requirements for managing user identities, authentication credentials, and access privileges across all Oklahoma County information systems. It defines standards for password strength, multi-factor authentication, account lifecycle management, privileged access control, and access review processes.

This policy is adopted under the authority of the Oklahoma County Information Technology Governance Charter (IT-GOV-CHARTER-001), as approved by the Board of County Commissioners. It is binding on all County Offices, Departments, and agencies as defined in the Governance Charter.

This policy supplements the access control provisions in the Acceptable Use Policy (IT-POL-AUP-001, Section 5) and the Information Security Policy (IT-POL-ISP-001, Section 7) with detailed operational requirements.

> ***Framework Alignment:*** *NIST SP 800-53: IA-1 (Identification and Authentication Policy), AC-1 (Access Control Policy) | NIST SP 800-63B (Digital Identity Guidelines — Authentication) | CIS Controls 5, 6 | CJIS Security Policy 5.5, 5.6*

2. Scope

This policy applies to all user accounts, service accounts, privileged accounts, and authentication mechanisms on all Oklahoma County IT systems, including:

- On-premises Active Directory and all AD-integrated systems
- Azure Active Directory (Entra ID) and all cloud-integrated services
- Microsoft 365, cloud applications, and SaaS platforms
- VPN and remote access systems
- Network infrastructure devices (firewalls, switches, routers, wireless controllers)
- Database accounts and application service accounts
- Telephony, PBX, and voicemail systems
- CJIS systems and applications
- Any system connected to the County core network

This policy applies to all personnel covered by the Acceptable Use Policy, including employees of all County offices, contractors, vendors, and any individual with access to County systems.

> ***Framework Alignment:*** *NIST SP 800-53: IA-1, AC-1 | CIS Controls 5.1, 6.1*

3. Identity and Account Management

3.1 Account Types

Account Type	Definition	Examples	Governance Requirements
Standard User	Individual account for day-to-day work with standard permissions	Domain user, email, Microsoft 365 access	Assigned per onboarding SOP; reviewed annually
Privileged Account	Account with elevated permissions beyond standard user access	Domain admin, server admin, firewall admin, Azure Global Admin	Separate from standard account; MFA required; reviewed quarterly; enhanced logging
Service Account	Non-interactive account used by applications, scripts, or automated processes	SQL service account, backup agent, SIEM collector	Documented owner; reviewed semi-annually; strong password; no interactive login
Shared Account	Account shared by multiple users (strongly discouraged)	Legacy application with single-user licensing	Prohibited by default; exception required per Section 3.4; compensating controls mandatory
Vendor / External	Account for third-party contractors or vendor personnel	Vendor support account, consultant access	Time-limited; MFA required; sponsor required; reviewed monthly; disabled when not actively needed
Emergency / Break-Glass	Highly privileged account used only in emergencies when normal accounts are unavailable	Local admin on domain controllers, emergency Azure admin	Sealed credentials; use triggers alert; all use documented and reviewed

3.2 Account Provisioning

- All account creation requests must be submitted through MIS' ITSM tool with supervisor approval
- Access rights are assigned based on the user's job function using role-based access control (RBAC) where available
- The principle of least privilege is applied to all accounts — users receive only the minimum access necessary to perform their duties
- New accounts are provisioned per the Account Provisioning SOP within 2 business days of approved request
- Privileged access requires additional justification, MIS Operations Manager approval, and is documented in the privileged access register

3.3 Account Deprovisioning

- Accounts for separated employees (termination, resignation, retirement) must be disabled within 24 hours of separation, and within 4 hours for involuntary separations
- Accounts for contractors and vendors must be disabled on the contract end date or within 24 hours of notification, whichever is sooner
- Upon separation, access to email, VPN, cloud services, and all remote access must be revoked immediately
- A deprovisioning checklist is maintained and executed for each separation, covering all systems the user had access to
- Departing employees' data is retained per records retention requirements; mailboxes are converted to shared mailboxes or archived per the applicable SOP

3.4 Shared Accounts

Shared accounts are prohibited by default. Any exception requires a written business justification submitted to the MIS Operations Manager, including the reason a unique account cannot be used, the proposed compensating controls (e.g., physical access logs, secondary authentication), and an expiration date for the exception. Shared accounts may never be used to access CJI systems.

Framework Alignment: *NIST SP 800-53: AC-2 (Account Management), IA-4 (Identifier Management), IA-8 (Identification and Authentication — Non-Organizational Users) | CIS Controls 5.1–5.6*

CJIS CJIS Security Policy 5.5.2: Each user accessing CJI must be uniquely identified and authenticated. Shared or group accounts for CJI access are strictly prohibited.

4. Password Standards

4.1 Password Requirements

All passwords for Oklahoma County systems must meet the following minimum standards:

Requirement	Standard User Accounts	Privileged Accounts	Service Accounts
Minimum Length	14 characters	20 characters	24 characters
Complexity	3 of 4 character types (upper, lower, number, special)	4 of 4 character types	High entropy; randomly generated
Maximum Age	Unlimited days (with MFA enforced); 90 days (without MFA)	90 days	365 days (with alerting on expiration)
Password History	Last 24 passwords	Last 24 passwords	N/A — unique each rotation
Lockout Threshold	5 consecutive failures	3 consecutive failures	N/A — no interactive login
Lockout Duration	30 minutes (auto-unlock) or manual unlock by MIS	Manual unlock by MIS only	N/A
Storage	Hashed (bcrypt, scrypt, or PBKDF2); never stored in plaintext	Same	Stored in approved password vault only

4.2 Password Prohibitions

- Passwords must not contain the user's username, display name, or any part of their full name
- Passwords must not be dictionary words, common phrases, keyboard patterns (qwerty, 123456), or previously breached passwords
- Passwords must not be reused across County systems and personal accounts
- Passwords must never be written down in unsecured locations, stored in unencrypted files, spreadsheets, or browser password managers on shared workstations
- Passwords must never be shared with any person, including supervisors, IT staff, or helpdesk — MIS will never ask for a user's password

4.3 Passphrases

Users are encouraged to use passphrases — a sequence of random words with mixed case and special characters — as an alternative to traditional complex passwords. Passphrases that meet the minimum length and complexity requirements are acceptable. Example: "Correct-Horse-Battery-Staple!7" (note: do not use this specific example).

> ***Framework Alignment:*** *NIST SP 800-63B: Section 5.1 (Memorized Secret Verifiers) | CIS Controls 5.2, 5.3 | CJIS Security Policy 5.6.2.1*

5. Multi-Factor Authentication (MFA)

5.1 MFA Requirements

Multi-factor authentication is required for the following:

System / Access Type	MFA Required	Acceptable Factors
VPN / Remote Access	Yes — all users	Authenticator app, hardware token, or push notification
Microsoft 365 / Cloud Admin	Yes — all admin roles	Authenticator app or FIDO2 security key
Microsoft 365 / Standard User	Yes — all users	Authenticator app, push notification, or phone verification
Privileged Accounts (Domain Admin, etc.)	Yes — always	Authenticator app or FIDO2 security key (SMS not permitted for privileged accounts)
CJI Systems	Yes — all access	Per CJIS advanced authentication requirements
On-Premises Workstation Login	Recommended; required for Restricted data access	Authenticator app, smart card, or Windows Hello for Business
Network Device Administration	Yes — all admin access	Authenticator app or RADIUS with MFA
Vendor / Remote Third-Party Access	Yes — always	Authenticator app or hardware token

5.2 Acceptable MFA Methods

The following MFA methods are approved, in order of preference:

1. FIDO2 security keys (phishing-resistant — preferred for privileged accounts)
2. Authenticator applications (Microsoft Authenticator, Google Authenticator, or approved equivalent)
3. Push notifications via approved authenticator app
4. Hardware OTP tokens
5. Phone call verification (standard accounts only; not permitted for privileged or CJI access)
6. SMS one-time codes (standard accounts only; not permitted for privileged or CJI access due to SIM-swap risk)

SMS-based MFA is being phased out. NIST SP 800-63B deprecates SMS as an authentication factor due to known vulnerabilities. Oklahoma County will transition all remaining SMS-based MFA to authenticator app or hardware token within 12 months of this policy's adoption.

Framework Alignment: *NIST SP 800-63B: Section 5.1.3 (Multi-Factor Authenticators) | CIS Controls 6.3, 6.4, 6.5 | CJIS Security Policy 5.6.2.2 (Advanced Authentication)*

CJIS	CJIS Security Policy 5.6.2.2: Advanced authentication (MFA) is required for all personnel accessing CJI, from any location, on any device. The authentication mechanism must provide two or more of: something you know, something you have, something you are.

6. Privileged Access Management

6.1 Privileged Account Controls

- Privileged accounts must be separate from standard user accounts — administrators must have a standard account for daily work and a separate admin account for elevated tasks
- Privileged accounts must not be used for email, web browsing, or any non-administrative function
- All privileged account usage is logged, monitored, and subject to periodic review
- Privileged access is granted only with MIS Operations Manager approval and documented business justification
- The number of privileged accounts is minimized — access is granted only to personnel who require it for their role

6.2 Privileged Access Register

MIS maintains a Privileged Access Register that documents:

- Each privileged account, its owner, and the systems/roles it grants access to
- The business justification for the privileged access
- The date access was granted and the last review date
- Whether MFA is enforced (mandatory for all privileged accounts)

The register is reviewed quarterly by the MIS Operations Manager and the Senior Security Analyst. Privileged accounts that are no longer justified are disabled immediately.

6.3 Emergency / Break-Glass Accounts

- Break-glass accounts are maintained for emergency access to critical systems when normal authentication is unavailable
- Break-glass credentials are stored in a sealed, tamper-evident envelope in a secure physical location, or in an approved hardware vault
- Use of a break-glass account triggers an immediate alert to the MIS Operations Manager and Senior Security Analyst
- All break-glass account usage must be documented with justification, reviewed by the MIS Operations Manager, and the credentials rotated immediately after use

Framework Alignment: *NIST SP 800-53: AC-6 (Least Privilege), AC-6(1) (Authorized Access to Security Functions), AC-6(5) (Privileged Accounts) | CIS Controls 5.4, 6.6, 6.8*

7. Access Review and Recertification

7.1 Review Schedule

Account Type	Review Frequency	Reviewer	Actions
Privileged Accounts	Quarterly	MIS Operations Manager + Senior Security Analyst	Verify continued need; confirm MFA; validate scope of access
Standard User Accounts	Annually	Department supervisor + MIS	Verify active employment; validate role-appropriate access
Service Accounts	Semi-annually	Account owner (documented) + MIS	Verify active use; validate permissions; rotate credentials if expired
Vendor / External Accounts	Monthly	Vendor sponsor + MIS	Verify active engagement; disable if contract ended or access no longer needed
Emergency / Break-Glass	Quarterly	MIS Operations Manager	Verify sealed credentials; validate alerting; confirm procedure documentation

7.2 Access Review Process

7. MIS generates an access report from Active Directory and Azure AD for the accounts under review
8. The report is distributed to the responsible reviewer(s) with a 10-business-day response deadline
9. Reviewers certify that each account is still required and the access level is appropriate, or request modification/removal
10. MIS implements all requested changes within 5 business days of receiving the reviewer's response
11. Non-responses after the deadline are escalated to the MIS Operations Manager; accounts with unresponsive reviewers may be disabled pending review
12. Review completion is documented and tracked in MIS's ITSM Tool

Framework Alignment: *NIST SP 800-53: AC-2(3) (Disable Inactive Accounts), AC-2(4) (Automated Audit Actions) | CIS Controls 5.1, 5.3*

8. Account Security Controls

8.1 Session Management

- Workstation screen locks activate after a maximum of 15 minutes of inactivity (10 minutes for CJI workstations)
- VPN sessions time out after 30 minutes of inactivity and require re-authentication
- Cloud application sessions enforce re-authentication at least every 24 hours for standard users and every 12 hours for privileged accounts
- Concurrent sessions for privileged accounts are limited to prevent credential sharing

8.2 Account Lockout and Recovery

- Accounts are locked after the threshold defined in Section 4 (5 failures for standard, 3 for privileged)
- Standard accounts auto-unlock after 30 minutes; privileged accounts require manual unlock by MIS
- Password reset requests require identity verification: for in-person requests, government-issued photo ID; for remote requests, verification through a secondary channel (supervisor confirmation, pre-registered security questions, or MFA-protected self-service portal)
- MIS helpdesk staff are trained to recognize social engineering attempts targeting password reset processes

8.3 Inactive Account Management

- Accounts with no login activity for 45 consecutive days are automatically disabled
- Disabled accounts are reviewed monthly; accounts disabled for 90 days with no reactivation request are deleted (after data retention verification)
- Exceptions for extended leave (FMLA, military, sabbatical) must be documented with HR and approved by the MIS Operations Manager

Framework Alignment: *NIST SP 800-53: AC-11 (Device Lock), AC-12 (Session Termination), IA-5 (Authenticator Management) | CIS Controls 5.2, 5.6*

CJIS	CJIS Security Policy 5.5.5 (Session Lock): Systems processing CJI must enforce a session lock after a maximum of 30 minutes of inactivity. Session lock must require re-authentication to resume.

9. Credential Storage and Management

9.1 Password Vault

- MIS maintains an approved enterprise password vault for storing privileged credentials, service account passwords, and emergency access credentials
- All privileged and service account credentials must be stored in the approved vault — storage in spreadsheets, text files, sticky notes, or browser password managers on shared systems is prohibited
- Access to the password vault is restricted to authorized personnel with MFA enforcement
- Vault access is logged and auditable

9.2 User Password Managers

- Individual users are encouraged to use an MIS-approved password manager for their personal County credentials
- Browser-based password managers on shared or kiosk workstations are prohibited
- The use of personal password managers (non-County-approved) is permitted for County credentials provided the manager uses encryption and a strong master password, but MIS cannot provide support for these tools

Framework Alignment: *NIST SP 800-53: IA-5(1) (Password-Based Authentication) | CIS Controls 5.2*

10. CJIS-Specific Access Requirements

In addition to all requirements in this policy, the following apply to all access to CJI systems:

- All personnel must have a completed fingerprint-based background check before CJI access is granted
- Background checks must be renewed at least every five years
- Advanced authentication (MFA) is mandatory for all CJI access, from any location, on any device
- Shared or group accounts for CJI access are strictly prohibited — no exceptions
- CJI session inactivity timeout must not exceed 30 minutes
- CJI access is restricted to personnel with a validated need-to-know, approved by the responsible Criminal Justice Agency
- The LASO must be notified of all CJI access provisioning and deprovisioning
- CJIS Security Awareness Training must be completed within six months of initial access and biennially thereafter

Framework Alignment: *CJIS Security Policy 5.5, 5.6 | NIST SP 800-53: IA-2, IA-5, AC-2, AC-7*

11. Enforcement

Violations of this policy are subject to the enforcement provisions of the Acceptable Use Policy (IT-POL-AUP-001). Credential sharing, unauthorized access, and failure to protect privileged credentials are treated as serious violations. For departmental IT operations, enforcement follows the IT Governance Charter escalation process (Section 9).

CJIS access control violations are reportable to the LASO and may result in immediate suspension of CJI access pending investigation.

12. Policy Administration

This policy is reviewed at least annually by MIS and the IT Council. Amendments follow the IT Governance Charter (Section 8) and require BOCC approval. The MIS Operations Manager may update technical standards (e.g., approved MFA methods, password vault platforms) without BOCC action, provided no substantive policy changes are involved.

13. Related Policies and Documents

Document	ID	Status
IT Governance Charter	IT-GOV-CHARTER-001	Pending
Information Security Policy	IT-POL-ISP-001	Pending

Document	ID	Status
Acceptable Use Policy	IT-POL-AUP-001	Pending
Change Management Policy	IT-POL-CHG-001	Pending
Incident Response Plan	IT-POL-IRP-001	Pending
Account Provisioning SOP	IT-SOP-ACCT-PROV	Planned
Account Deprovisioning SOP	IT-SOP-ACCT-DEPROV	Planned
FBI CJIS Security Policy	External	Current Version
NIST SP 800-63B	External	Current Version
NIST SP 800-53 Rev. 5	External	Current Version
CIS Controls v8	External	Current Version