Password Policy (Draft)

IAM-005-PO | Version 0.1

Effective Date	**[To be determined upon Board adoption]**
Approved By	**Yellowstone County Board of County Commissioners**
Policy Owner	**Information Technology Department**
Related Documents	
Review Cycle	**Annual**
Classification	**Public**

Version History

Version	Date	Reason/Comments
1.0	11/06/2026	Initial Draft by Will Grimm
1.1	11/17/2026	Revision by Larry Ziler

Important Notice

This is an official governance policy of Yellowstone County, Montana. All County departments, divisions, elected offices, and covered third parties are bound by the requirements set forth herein. Questions regarding interpretation or applicability shall be directed to the Information Technology Department.

Password Policy (Draft)

IAM-005-PO
Version 0.1
Revision Date 11/06/2026

SECTION 1 — PURPOSE

This policy establishes standardized password and authentication requirements for all users, systems, and applications within the organization. It ensures compliance with NIST SP 800-63B Digital Identity Guidelines, FBI CJIS Security Policy, and CJIN requirements, while supporting strong cybersecurity practices.

SECTION 2 — SCOPE

This policy applies to all of the following:

- All Yellowstone County departments, divisions, offices, and elected offices
- All County-owned, County-leased, or County-managed endpoints, servers, and network infrastructure devices
- All on-premises systems and County-managed cloud-connected systems
- Third-party vendors, contractors, and managed service providers (MSPs) who operate systems on behalf of the County or who connect to County networks in any capacity
- All systems subject to Criminal Justice Information Services (CJIS) compliance requirements, including those operated by or in support of the Yellowstone County Sheriff's Office and any other law enforcement or justice function

Scope Exclusion — Personal Devices

This policy does **NOT** apply to personally owned devices unless such devices are used to access County systems or networks under a formally executed Bring Your Own Device (BYOD) agreement. Where a BYOD agreement is in effect, the device owner is responsible for compliance with this policy as a condition of network access.

SECTION 3 — AUTHORITY

This policy is established under the authority of the Yellowstone County Board of County Commissioners pursuant to the County's IT governance framework and applicable Montana statutes governing county information technology management and data security.

The Yellowstone County designated IT Director is hereby authorized to interpret, enforce, and grant formally documented exceptions to this policy in accordance with the exception process described in Section 8.

This policy aligns with and is subordinate to the County's overarching Information Security Policy. In the event of conflict between this policy and the Information Security Policy, the Information Security Policy shall govern. This policy supplements and does not replace any applicable state or federal requirements.

SECTION 4 — DEFINITIONS

For the purposes of this policy, the following terms shall have the meanings set forth below:

Term	Definition
CJIN	The state-managed system containing criminal justice information, subject to security and access controls.
CJIS	Federal standards and requirements governing the protection of Criminal Justice Information (CJI), including authentication and password requirements.
Credential	Information (such as a password, passphrase, token, or certificate) used to verify a user's identity.
Hashing	A one-way cryptographic process used to securely store passwords without revealing the original password.
MFA	An authentication method requiring two or more distinct factors to verify identity, significantly increasing security.

Term	Definition
Passphrase	A longer string of words or characters used as a password. Typically, easier to remember and more secure than short, complex passwords.
Privileged Account	An account with elevated permissions, including administrator or service accounts, that provides access to critical systems or functions.
Service Account	A non-human account used by applications, services, or systems to perform automated functions.
Special Character	Characters that are not letters or numbers. Ex: (!@#$%^&*+-*)

SECTION 5 — POLICY STATEMENT

The goals of this policy are to:

- Protect sensitive and regulated data (including CJIS/CJIN information).
- Ensure consistent password requirements across the environment.
- Reduce compromise risk through modern authentication practices.
- Align organizational authentication controls with state and federal mandates.

SECTION 6 — REQUIREMENTS

The following requirements are mandatory. The terms **SHALL**, **SHALL NOT**, and **MUST** indicate non-discretionary obligations. All covered entities and systems are subject to these requirements unless a formally approved exception is on file.

6.1 Minimum Requirements: Yellowstone County will follow the policy recommendations from NIST and CJIS. Where these policy recommendations differ, the more restrictive of the two policies will be adopted.

All passwords must meet the following standards:

- Minimum password length: 12 characters
- Maximum password length: 64 characters
- Character complexity rules require an Uppercase & Lowercase Letter, Number, and Special Character
- Users may use passphrases and are encouraged to create passwords that are easy to remember, difficult to guess, and compliant with all requirements of this policy
- Passwords must not contain the user's name, username, or organizationally assigned ID.
- Systems shall prevent users from reusing the previous 24 passwords where technically feasible.

6.2 Passwords Screening

All passwords created, updated, or reset must be screened using an approved program or tool to reject:

- Known compromised password lists
- Common dictionary words
- Repetitive or predictable patterns
- Custom wordlist approved by the IT Director

6.3 Password Expiration

To meet organizational and CJIN/CJIS compliance needs:

- Passwords must be changed every 365 days.
- Passwords cannot be changed within 10 days of changing their password.
- Accounts handling CJIS-related data must follow CJIS requirements if stricter controls are mandated in the future.

Passwords may be reset sooner if:

- The account is suspected to be compromised
- Required by audit or compliance review
- Directed by IT Security

6.4 Multi-Factor Authentication (MFA)

MFA is required for:

- Remote access
- VPN connectivity
- Access to CJIS or CJIN data
- Administrative accounts
- Cloud services containing sensitive or confidential data

Approved factors include:

- FIDO2 security keys
- Authentication apps
- One-time passwords (TOTP)
- Certificate-based authentication

SMS-based MFA should be avoided per NIST recommendations.

6.5 Account Lockout

To reduce brute-force attack risk:

- 5 failed attempts triggers lockout
- Lockout duration: 30 minutes
- Manual unlock may be performed by IT staff after verification of identity

6.6 Password Storage and Management

The organization will:

- Use encrypted, salted, and hashed storage for all credentials.
- Prohibit plaintext storage of passwords in any system or document.
- Provide secure reset mechanisms requiring identity verification.

Password managers may be approved for employee use with IT review.

6.7 Administrative and Service Accounts

Administrative and service accounts must follow enhanced controls:

- Must use unique passwords not shared across services
- Must use MFA where technically feasible
- Must not be used for day-to-day productivity tasks
- Shared user accounts are prohibited unless specifically approved by the IT Director and documented as an approved exception.

Privileged accounts must be monitored and audited quarterly.

SECTION 7 — ROLES & RESPONSIBILITIES

The following table defines the responsibilities of each role with respect to this policy. All roles are accountable for compliance within their respective areas of authority.

Role	Responsibilities
Board of County Commissioners	Adopts and approves this policy and material amendments thereto; provides governance oversight of County IT policy; receives compliance status reports as warranted.
IT Director	Interprets and enforces this policy; approves or denies exception requests; reports compliance status to County leadership; ensures adequate resources are allocated for compliance verification; maintains the exception register.

Role	Responsibilities
IT Security / Compliance Staff	Administers and monitors compliance with password and authentication requirements; conducts compliance reviews and audits; maintains documentation and audit records; manages password policy configurations and monitoring tools; coordinates remediation of non-compliance; escalates significant violations to the IT Director.
System Administrators	Configure and maintain systems in accordance with approved password and authentication standards; implement password expiration, account lockout, privileged access controls, and multi-factor authentication where applicable; promptly remediate identified weaknesses or non-compliance.
Department Heads	Ensure employees within their departments understand and comply with this policy; support compliance efforts and training initiatives; promptly report security concerns and suspected account compromises; cooperate with audits and investigations.
Employees and Authorized Users	Create and maintain passwords in accordance with this policy; protect authentication credentials from unauthorized disclosure; utilize multi-factor authentication when required; immediately report suspected credential compromise or unauthorized account activity to the IT Department.
Vendors and Contractors	Comply with applicable password and authentication requirements when accessing County systems, networks, or data; ensure personnel are trained regarding authentication security requirements; provide compliance attestation upon request; promptly report suspected security incidents involving County accounts or systems.

SECTION 8 — COMPLIANCE & ENFORCEMENT

The IT Department is responsible for monitoring compliance with this policy and taking enforcement action as necessary.

Violations of this policy are taken seriously and may result in one or more of the following actions, depending on the nature, severity, and circumstances of the violation:

- Immediate suspension or restriction of an account determined to present a security risk
- Forced password reset or credential revocation

- Temporary or permanent removal of access privileges to County systems, applications, networks, or data
- Escalation of violations to the affected department's leadership and the IT Director
- Disciplinary action against County employees in accordance with Yellowstone County Human Resources policies, up to and including termination of employment
- For vendors and contractors: suspension or revocation of account access, invocation of contract remedies, or termination of services
- Referral to appropriate law enforcement authorities where criminal activity is suspected

The IT Department is authorized to take immediate technical remediation actions necessary to protect County systems and data, including disabling accounts, forcing password changes, requiring additional authentication controls, restricting access privileges, or temporarily suspending access where a security risk has been identified. Such action may be taken without advance notice to the system user or owner where a security risk has been identified. Post-action notification to the affected department shall occur as soon as practicable following remediation.

Enforcement actions shall be documented by the IT Department and retained in accordance with the County's records retention schedule.

SECTION 9 — EXCEPTIONS

Requests for exceptions to this policy MUST be submitted in writing using the County's official IT Policy Exception Request form, available from the IT Department. Exceptions shall not be granted verbally or informally.

Each exception request SHALL include, at a minimum, the following:

- Identification of the specific system(s) for which the exception is requested
- Business or operational justification for the exception

- A risk assessment identifying the risks introduced by enabling IPv6 on the specified system(s)
- Proposed compensating controls to mitigate identified risks during the exception period
- The requested duration of the exception

All exceptions require written approval from the designated IT Director. Exceptions SHALL NOT be granted by any other authority. Approved exceptions SHALL be reviewed at least annually and shall expire automatically unless formally renewed prior to the expiration date. No exception grants indefinite or permanent exemption from password or authentication requirements. An exception register documenting all active and expired exceptions SHALL be maintained by the IT Department and made available for audit upon request.

SECTION 10 — REVIEW & REVISION

This policy SHALL be reviewed annually by the IT Department, commencing one year from the effective date. The review shall assess whether changes in technology, the County's operational environment, regulatory requirements, or emerging cybersecurity guidance necessitate amendments to this policy.

The review SHALL include consideration of applicable requirements and guidance issued by:

- National Institute of Standards and Technology (NIST)
- FBI Criminal Justice Information Services (CJIS) Security Policy
- Criminal Justice Information Network (CJIN) requirements
- State and federal regulatory requirements applicable to County operations

Material changes to this policy — including changes to the scope of covered systems, enforcement provisions, exception criteria, or any requirement that substantively alters the obligations of covered parties — SHALL be submitted to the Board of County Commissioners for review and approval prior to taking effect.

Minor clarifications, editorial corrections, and non-substantive updates may be approved by the IT Director without Board action, provided such changes do not alter the policy's substantive requirements and are documented in the policy version log.

The next scheduled review date is one year from the effective date of this policy as adopted by the Board of County Commissioners. The IT Department is responsible for initiating the review process and presenting any proposed amendments in a timely manner. The IT Department shall maintain a version history log for this policy, recording all revisions, approval dates, and the nature of changes made.

The IT Department shall maintain a version history log for this policy, recording all revisions, approval dates, and the nature of changes made.

SECTION 11 — REFERENCES

The following documents, standards, and resources are referenced by or related to this policy:

1. NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*
2. CJIS Security Policy, Version 6.1
3. Montana Criminal Justice Information Network (CJIN) Security Requirements
4. Yellowstone County Information Security Policy
5. Yellowstone County Acceptable Use Policy
6. Yellowstone County IT Policy Exception Request Form
7. Microsoft Security Baselines and Identity Security Guidance