STOREY COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER: **400.013**
EFFECTIVE DATE: **04/21/2026**
REVISED:

AUTHORITY: **BOCC**
COUNTY MANAGER: **AO**

SUBJECT: MULTI-FACTOR AUTHENTICATION POLICY

I. Purpose:

The purpose of this policy is to safeguard Storey County's digital infrastructure, sensitive data, and resident information. Passwords alone are no longer sufficient to protect against unauthorized access. It aligns with modern cybersecurity standards (like National Institute of Standards and Technology/Criminal Justice Information Services (NIST/CJIS)) while specifically adhering to your requirements for allowed methods. This policy mandates the use of Multi-Factor Authentication (MFA) to provide an additional layer of security.

II. Scope:

This policy applies to all individuals who access Storey County information systems, including:

1. Full-time, part-time, and seasonal employees.
2. Elected and appointed officials.
3. Contractors, consultants, and third-party vendors.
4. Volunteers and interns.

III. Policy Statement:

Effective immediately, all users are required to use Multi-Factor Authentication to access Storey County networks, email (Microsoft 365), Virtual Private Networks (VPNs), and any internal or cloud-based applications containing sensitive data.

IV. Authorized MFA Methods:

To ensure accessibility and security, Storey County IT permits only the following three methods for identity verification:

Method	Description	Usage Note
Microsoft Authenticator App	A mobile application that provides a push notification or a 6-digit rolling code.	**Preferred Method.** Recommended for all users with a smartphone.
Text Message (SMS)	A one-time passcode (OTP) sent via Short Message Service (SMS) to a registered mobile device.	Secondary option for users without the app.
Storey County IT Token	A physical hardware device that generates a time-based code.	Issued to users without mobile devices or those working in secure areas.

V. User Responsibilities:

1. Enforcement: Users must not attempt to bypass or disable MFA.
2. Device Security: Users utilizing personal or county-issued mobile devices for MFA must maintain a lock screen (PIN, pattern, or biometrics) on that device.
3. Lost/Stolen Factors: If a hardware token is lost, or if a mobile device used for MFA is stolen, the user must notify Storey County IT Help Desk within one (1) hour of discovery to revoke the credentials.
4. Suspicious Activity: Users must never approve an MFA prompt they did not initiate. Any unsolicited prompts must be reported to IT as a potential security incident.

VI. Procurement of Hardware Tokens:

Hardware tokens are the property of Storey County.

1. Tokens will be issued by the IT Department upon request or based on job requirements.
2. Lost hardware tokens may be subject to a replacement fee at the discretion of the County Manager.

VII. Compliance and Enforcement:

Failure to comply with this policy may result in the immediate suspension of network access. Unauthorized attempts to circumvent MFA are considered a violation of the Acceptable Use Policy and may lead to disciplinary action, up to and including termination.

VIII. Responsibility for Review: The IT Director will review this policy every 5 years, or more frequently is necessary.