TWO FACTOR AUTHENTICATION POLICY

I. PURPOSE

Hidalgo County is committed to providing a safe and secure workplace for all employees. As part of this goal, the County is instituting a multi factor authentication system for County employees.

This policy specifically applies to the County network authentication access which will be deployed to all county employees. The multi factor authentication system serves the dual purpose of readily identifying County employees and other authorized personnel, while providing measured protection against unauthorized personnel and intruders from gaining access to our secured network infrastructure. The system is effective only if there is active cooperation and compliance by all employees at all times. Any laxity in compliance and enforcement subjects the entire network infrastructure to a potential security breach.

The network infrastructure encompasses windows login, email, remote connection (VPN) and other critical system infrastructures.

In the best interests of the County, CJIS and HIPAA compliance and to secure our data and network infrastructure, this standard will be implemented Countywide. The Information Technology Department will provide software, direction, and instruction for all Departments.

This security measure will also validate employee identity on password reset requests and provide access to county computer and network systems as well as secured county cloud environments. Implementation of the two-factor authentication system will begin in the 4th quarter of 2023 continuing with all departments until full implementation is completed. This system will employ an additional compliance and security measure and will become the county standard.

The authentication method will also be provided to any and all vendors that support and have access to county network infrastructure and or other critical network systems both on premise and cloud based.

1. Elected Officials/Department Heads

All Elected Officials/Department Heads will ensure that this Policy is fully implemented and adapted to the needs of their departments/offices and work locations. This includes ensuring that the requirements of this policy are enforced for their office/department. As party of the County's effort to implement this policy, each Elected Official/Department Head will provide a list of permanent full and part time employees who will have access to the County's network infrastructure to the County's Information Technology Department.

2. Managers and Supervisors

It shall be the direct responsibility of Managers, Supervisors, and other assigned personnel, that are designated in writing by their Department Head/Elected Official, to enforce the requirements of this policy.

3. All Employees

All County employees shall be required to comply with the provisions of this policy as needed to perform the duties of their job. If an employee is assigned a hardware token device for authentication, the County will require employees to bring in the authentication device to work with them at all times. This will allow employees to authenticate into the County network. For the purpose of this Policy, employees include permanent full time, permanent part-time and temporary employees.

II. CONTROL AND DEPLOYMENT of AUTHENTICATION SYSTEM

Methods of Authentication:

- **DUO Mobile Push** (requires the app on a personal or assigned work cellphone or tablet)
- **One Time Passcode via the DUO App** (requires the app on a personal or assigned work cellphone or tablet)
- **Hardware Token** (see description and requirements below)
- **Call Me** (a call to a designated workplace phone line)
- **SMS Text** (a text sent to a personal or assigned work cellphone)

DUO Mobile Push is the most efficient method to utilize and the **most secure**.
OTP via the DUO App and **the Hardware Token** are also **secure**, but will require you to enter a code when prompted.
Call Me and **SMS text** method are supported, but are the **least secure** and not recommended unless no other option is available.

A. Employee Authentication Hardware

1. **Description of (hardware token):** is a small device that you can attach to your key chain, can also be used. If you have a hardware token, when you go to log in, you will be expected to enter in a code that appears on your key fob or token to complete the login process other hardware tokens will require insertion to your computers USB.
   When a hardware device is damaged, lost, stolen or misplaced, the employee must immediately report the incident to the department head and to the cyber security team. The department will in turn immediately notify the Information Technology Department through an official form. The County will require that both the employee and their department head/supervisor sign the official form indicating a token device has been damaged, lost or stolen. Reporting the loss of a token is critical to the security of the County.
   Hardware tokens will only be re-issued if the hardware token is damaged, lost, stolen, misplaced. Employees will be provided an option to login with a call to the IT department with a One Time Passcode until the hardware token is replaced.
2. Upon initial implementation of this Policy, all existing County employees will be registered in the authentication system. Following implementation, new employees will be registered in the authentication system during enrollment.

3. Hardware tokens (where applicable) are the property of the County. At the end of employment, an employee's supervisor shall require the employee to surrender the hardware token. All hardware tokens shall be returned to the Information Technology Department.
4. An Employee who is on extended leave (30 days or more) will be required to turn in his or her hardware token to the supervisor pending return to work.
5. Each Employee must not have more than one hardware token in his or her possession at any one time.

III. REQUIREMENTS AND ENFORCEMENT

A. Employee Authentication Procedure

The County expects all employees to fully comply with all provisions of this policy. All supervisors and staff shall enforce all provisions of this policy.

1. If assigned a hardware token, employees must bring in their hardware tokens at all times for authentication into the county network.
2. Each Employee is responsible for safeguarding his or her own hardware token (where applicable), and must immediately report any lost hardware token to their supervisor and the IT department.
3. Any employee that does not comply with this policy will be subject to disciplinary action, up to and including termination as per the Hidalgo County Civil Service Commission Rules and Personnel Policy.

IDENTIFICATION BADGE HOLDER DUTIES AND RESPONSIBILITIES (only if assigned a hardware token)

- Do not lend your hardware token to anyone.
- Do not allow unauthorized individuals to use the token assigned to you.
- Do not leave hardware token on dash of vehicle or other locations where it may be exposed to extreme temperatures.
- Do not fold, bend, pry open or mutilate your assigned hardware token.
- Do not use your hardware token improperly.
- Do not leave your hardware token unattended.
- Immediately notify your Elected Official/Department Head if your assigned authentication device is no longer in your possession.
- Immediately notify your Elected Official/Department Head of any difficulties or problems with your authentication onto the county network and any authentication notification that seems out of place.