Nueces County

Password and Authentication Policy

A. Purpose

*Password*s are the primary form of user authentication used to access to *NUECES COUNTY*'s information systems. To ensure that *password*s provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that *password*s will be created that are easy to break, thus allowing easier illicit access to *NUECES COUNTY*'s information systems, and thereby compromising the security of those systems.

B. Scope

The policy applies to all information systems, information components, and employees/volunteers of *NUECES COUNTY*, including all temporary or contract workers. To ensure that *password*s provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that *password*s will be created that are easy to break, thus allowing easier illicit access to *NUECES COUNTY*'s information systems, and thereby compromising the security of those systems.

Examples of items that should always have *password*s:

- Devices that provide centralized computing capabilities (i.e. servers, mainframe computers, etc.)
- Devices that provide centralized storage capabilities (i.e. any network storage systems).
- Desktops, laptops, smart phones, tablets, and other devices that provide *distributed computing* capabilities.
- Network devices (i.e. routers, switch, access points, etc.).
- Security devices that provide dedicated capabilities (i.e. firewalls, intrusion and detection sensors, security appliances, etc.)
- Cloud services (i.e. infrastructure as a service, platform as a service, and/or software as a service)

C. Definitions

Distributed computing - is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another.

Password - set of characters meant to secure an account with at least 8 but not more than 23 characters

Passphrase - set of characters meant to secure an account exceeding 23 characters

Passcode - set of numbers meant to secure a device with at least 4 but not more than 6 numbers; also referred to as a Personal Identification Number (PIN)

Biometric authentication - is a security process to secure an account or a device that relies on unique biological characteristics of an individual

D. Governing Laws & Regulations

E. Policy Statements

1. *Password*s must be constructed according to set length and complexity requirements. As such, *password*s must be 8 characters in length and must include upper case, lower case, numbers, and special characters.
2. *Password*s will have both a minimum and maximum lifespan. As such, *password*s must be replaced at a maximum of 180 days and at a minimum of 90 days.
3. *Passphrase*s must be constructed according to set length and complexity requirements. As such, *passphrase*s must be a minimum of 23 characters in length and must include a minimum of 3 words.
4. *Passphrase*s will have both a minimum and maximum lifespan. As such, *passphrase*s must be replaced at a maximum of 1 year and at a minimum of 1 year.
5. *Password*s and *passphrase*s may not be reused any more frequently than every 10 *password* refreshes. Reuse includes the use of the exact same *password* or the use of the same root *password* with appended or pre-pended sequential characters.
6. *Password*s, *passphrase*s, and *passcode*s are to be used and stored in a secure manner. As such, *password*s are not to be written down, or electronically, stored in an unsecure location. *Password*s are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
7. *Password*s, *passphrase*s, and *passcode*s are to be individually owned and kept confidential and are not to be shared under any circumstances. If a *password*, *passphrase*, or *passcode* is shared or discovered, it should be changed immediately.
8. If available, the **use of *biometric authentication* for securing a device and/or account is STRONGLY RECOMMENDED** because it reduces the chance of *password*, *passphrase*, or *passcode* from being discovered unintentionally.

F. Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at *NUECES COUNTY*. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources.
2. Disciplinary action by Department Head/Elected Official according to applicable *NUECES COUNTY* policies/rules.
3. Disciplinary action up to Termination of employment.
4. Legal action, if any, according to applicable laws and contractual agreements.

Revision History

Version ID	Date of Change	Author	Rationale