PINAL COUNTY Enriching Lives Beyond Expectation	PINAL COUNTY Access Management		
	DATE: 08/26/2020 REVISED:	PAGES: 14	POLICY NUMBER: 11.003

Access Management Standard

Table of contents

1. PURPOSE

1.1 Access Management — this standard defines the requirements for protecting the County's information assets throughout their life cycle from the original request for access to the revocation of privileges. This standard addresses the following:

- User access management to verify authorized user access to information assets
- User password management to control allocation of account passwords
- User responsibilities to prevent unauthorized access and compromise of information assets
- Network access control to verify the security of network services and information assets
- System authentication control to verify authorized access to information assets
- Provisioning of contractors' access to information assets through a formal management process

2. AUTHORITY

2.1. Pinal County provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all departments shall adhere to the policies, procedures and objectives established by the Information Security Department with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of Pinal County. The document applies to all county departments including all boards, commissions, divisions, councils, bureaus, offices and vendors. Other County entities that voluntarily use or participate in services provided by the Information Technology Department, such as Pinal.gov, must agree to comply with this document, with respect to those services, as a condition of use. Departments and offices are required to implement procedures that ensure their personnel comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

4.1. The Information Security Department is responsible for the development and ongoing maintenance of this standard.

4.2. The Information Security Department is responsible for compliance with this standard and may enlist other departments in maintaining and monitoring compliance with this standard.

4.3. Any inquiries or comments regarding this standard shall be submitted to the Information Security Department by sending an email to mailto:ITSecurity@Pinal.gov.

4.4. Additional information regarding this document and its related ***policy*** and ***standards*** can be found at https://www.pinalcountyaz.gov/HR/Pages/PoliciesProceduresRules.aspx

5. COMPLIANCE

5.1. Compliance with this document is mandatory for all departments including all executive offices, boards, commissions, departments, divisions, councils, bureaus, offices and vendors. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the County. Exceptions to any part of this document must be requested via email to the IT Security Department (ITSecurity@Pinal.gov). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the County Chief Information Security Officer (CISO) or appointed designee.

6. STANDARD STATEMENTS

6.1. User and System Access Management

User or system access shall be managed throughout the account life cycle from the identification of a user to the granting, modification or revocation of a user's access privileges. User accounts shall be bound to proofed credentials.

6.1.1. Access types: Access by County accounts fall under the following categories:

6.1.1.1 Privileged access: Any account type that grants users elevated or increased application or information system capabilities that may affect computing systems; network communication; or the accounts, files, data or processes of County systems, including the ability to read, update or distribute highly sensitive information or make changes to system configurations and security settings.

6.1.1.2 Interactive access: Any account type that allows one individual to log into an information system, through either a remote or direct connection, by entering appropriate credentials and supplying commands.

6.1.1.3 Non-interactive access: Any account type (i.e., non-human) used solely by a process, service or application to communicate with other systems.

6.1.1.4 Shared access: Any account type that is shared by two or more users or systems and may or may not provide the ability to associate a login or activity with a particular user or system (e.g., built-in account).

6.1.1.4.1. The creation and/or existence of non-built-in shared accounts must be managed as an exception using a formal risk management process. All exception-based shared account access should be time-boxed (where technically feasible), and the use of passwords should be controlled with an approval (e.g., Information Security Department or department CISO) driven checkout process. Shared account passwords should be changed every 30 days (see *Password Management 6.4 in this Standard*).

6.1.2. Account types: County accounts fall under the following categories:

6.1.2.1 User account: A unique ID or login account owned by a single individual.

6.1.2.2 Administrator account: A privileged interactive account that is assigned to one and only one user. Passwords for these accounts must not be shared. Administrator accounts provide individuals with a frequent need for elevated access to have the associated privileges and segment their regular access from the administrative access.

6.1.2.3 System account: A built-in account that enables administration, communications or processing services within infrastructure systems, platforms, applications and databases. Some system accounts are not intended for use by humans and are simply in place to start and stop various processes.

6.1.2.4 Service account: Interactive or non-interactive accounts that are not built in but are put in place by an organization to enable functionality such as communications or processing services within and between infrastructure systems, platforms, applications and databases. These types of accounts can also be used to grant specialized elevated rights to applications, systems or shared mailboxes.

6.1.3. Where technically feasible (and available), certain types of privileged accounts shall be managed by a privileged access management (PAM) solution, maintained or approved by the Information Security Department, or manual process, as follows:

Account type	Control and Usage
Administrator	Administrator accounts are generally allocated to individuals; their use needs to be constrained by strong security policies. • PAM functionality: Not required although process to audit account access should be implemented • Example/use: account used to reset passwords
Service	Service accounts have elevated rights but should generally not be shared unless required by business or technical constraints. • PAM functionality: Strong passwords, centrally manage passwords; Example/use: Oracle DB account used to read data; accounts configured to enable particular functionality; accounts used to read log directories or manage group email lists
System/Built-in	The applicable controls required for system accounts are highly dependent on the operational nature of an application, the technical constraints, and underlying technology and/or vendor restrictions. • PAM functionality: Check-in, check-out; complex passwords; and enhanced monitoring • Example/use: Sys DBA for Oracle; Root access for Unix (sudo)

6.1.4. Request access privileges: User requests for access privileges shall follow a formal process.

6.1.4.1 Departments must ensure that personnel sign and agree to the *Acceptable Use* Policy prior to obtaining any system access (see *Acceptable Use Policy 11.002)*.

6.1.4.2 User registration and revocation procedures shall be implemented for all information systems and services.

6.1.4.3 User access requests shall be recorded (paper or tool-based) and approved by the requestor's supervisor and the appropriate Information Owner or authorized delegate.

6.1.5. Grant access privileges: Departments must ensure that personnel with Security administration roles (hereafter, "security administrators") are responsible for the creation of accounts and the assignment of privileges after receiving the required access approvals.

6.1.5.1 Access authorization: The Information, application or system owner shall verify that the type of access requested is required for the user's role and responsibilities.

6.1.5.2 Least privilege: Access and permissions shall be granted using the least privilege principle, i.e., only entitlements required to perform an individual’s job responsibilities shall be granted. Vendor accounts will have the minimum privilege and security levels required to perform services.

6.1.5.3 Segregation of duties: The Information, application or system owner shall confirm that conflicting access is separated to prevent fraud and/or misuse of the organization’s assets.

6.1.6. Revoke access privileges: Upon a transfer, termination or other significant change to a user’s employment status or role, County Executive Offices and Department Heads must ensure that the user’s previous supervisor shall be responsible for informing security administration personnel to take appropriate action.

6.1.6.1 Privileges that are no longer required by a user to fulfill his or her job role shall be removed.

6.1.6.2 If the termination date of personnel is known in advance, the respective access privileges — specifically those with access to confidential information — shall follow the approved termination process.

6.1.6.3 ***Security administrators*** in consultation with the Information Security Department may temporarily suspend or restrict a user’s level of access to the network if his or her account is suspected of privilege abuse or violation of the *Acceptable Use* policy.

6.1.7. Review of user access rights: Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

6.1.7.1 Audit logs for account creation/ modification, deletion and access change shall be retained and reviewed in accordance with *the Logging and Event Monitoring* standard #11.011.

6.1.7.2 Review of user’s access must be conducted, at a minimum, semiannually, and all unauthorized accounts and access must be removed.

6.1.7.2.1. Login accounts inactive for 90 days will be disabled.

6.1.7.2.2. Disable accounts for personnel scheduled to go on an extended leave of absence of more than 90 days.

6.1.7.2.3. Remove or disable user accounts that no longer require access to information assets.

6.1.7.2.4. Revoke access for any user no longer employed or under contract with a County department within 24 hours of notice.

6.1.7.2.5. More frequent reviews are encouraged commensurate to the risk level of the information asset or to meet regulatory requirements.

6.1.7.3 Privileged access reviews for Critical and High rated information systems shall be reviewed on a semi-annual basis.

6.1.7.3.1. More frequent reviews are encouraged commensurate to the risk level of the information asset or to meet regulatory requirements.

6.1.7.3.2 Configure systems to issue a log entry when an account is added to or removed from any group assigned administrative privileges.

6.1.7.3.3 Configure systems to issue a log entry on unsuccessful logins to an administrative account.

6.1.7.3.4 Limit access to scripting tools to only administrative or development users with the need to access those capabilities.

6.1.8. Manage privilege access for system utilities: Access to system tools that have the capability to override system and application controls shall be restricted by County Departments and Offices to authorized personnel.

6.1.8.1 Privileged accounts (e.g., root or administrator level accounts) shall be used only for system administration where such access is required.

6.1.8.2 Administrative accounts shall not be used for non-administrative purposes (e.g., browsing the Internet).

6.1.8.3 Privileged user access shall be logged and monitored to prevent misuse of ***information assets*** where available.

6.1.9. Emergency access management: Procedures shall be established (or implemented as needed) for obtaining necessary access to information assets during an emergency in accordance with *Business Continuity and Disaster Recovery Standard #11.005.*

6.2. Account Management

County departments and offices shall document and implement proper user identification and authentication processes, including:

6.2.1 Control and log the addition, deletion and modification of user IDs, credentials and other identifier objects.

6.2.2 Verify user identities prior to allowing password resets.

6.2.3 Require the use of a unique ID for system administration and other privileged access, including the management of network devices or information systems that contain confidential information, and for remote user access.

6.2.4 Disallow use of standard user accounts for domain administrative activities; as well, do not use domain administrative accounts for everyday use.

6.2.5 Time-box and monitor accounts used by third parties for remote access.

6.2.6 Disconnect remote-access sessions after county business is completed.

6.2.7 Restrict access to any database containing confidential information (including access by applications, administrators and all other users) by:

6.2.7.1 Limiting user access to user queries of and user actions on databases to programmatic methods.

6.2.7.2 Limiting the ability to directly access databases containing confidential information to only database administrators and only for administrative purposes.

6.2.7.3 Limiting the use of application IDs for database applications to application processes (i.e., non-interactive).

6.2.8 Access attempts shall be limited by locking user IDs after no more than ten (10) failed login attempts within 15 minutes.

6.2.8.1 In the event a user account is locked out, the user must call the IT Help Desk to re-enable account access. A self-service password reset function managed and monitored by the Information Security Department may be used.

6.2.8.2 “Reset account lockout counter after” policy shall be set to 15 minutes to mitigate against password timing and guessing attacks.

6.2.9 Maintain an inventory of each of the organization’s authentication systems, including those located on-site or at a remote service provider.

6.2.10 Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.2.11 Require multi-factor authentication for all user accounts accessing email, County Intranet, whether managed on-site or by a third party provider.

6.2.12 Encrypt or hash all authentication stored credentials when available.

6.2.13 Ensure that all account usernames and authentication credentials are transmitted securely using VPN to access county resources.Utilize Multi-factor on any system that supports it across networks using encrypted channels, where available.

6.2.14 Automatically lock workstation sessions after a standard period of inactivity.

6.2.19 Monitor attempts to access deactivated accounts through audit logging.

6.2.20 Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

6.3 *Information system controls*

Information systems (e.g., operating systems, databases and applications) shall be configured with appropriate authentication controls designed to prevent unauthorized disclosure, modification or access to information.

6.3.1 No system or database containing non-public information shall be directly accessible from an untrusted network or information system.

6.3.2 Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

6.3.3 Logon processes shall be customized wherever possible to display only the information required for the user to authenticate. Minimal information about the information system shall be disclosed to avoid providing an unauthorized user with contextual information.

6.3.4 Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use complex passwords.

6.3.5 Workstations left unattended for extended periods of time must be locked or logged off.

6.3.5.1 The time-out delay shall reflect the security risks of the system, the classification of the information being handled and the risks related to the users of the system.

6.3.5.2 An automatic screen saver lock timer shall be set to reflect the security risks of the system for workstations used by personnel with access to any County network and information system.

6.3.5.3 Put devices into a sleep or locked mode any time they are not in active use.

6.3.6 Network devices and systems shall be configured with appropriate access controls to prevent unauthorized modification or access to information assets and internal and external networked devices

6.4 Password Management

County Executive Offices and Departments must ensure that systems and processes to manage the enforcement of password controls for access to the network, operating systems, databases or applications shall be interactive and require strong passwords.

6.4.1 Passwords shall be configured securely using complexity and expiration requirements, as follows:

6.4.1.1 User passwords must be a minimum of eight (8) characters and contain all of the following four (4) characteristics:

6.4.1.1.1. Special characters (e.g., ‘, %, $, #)

6.4.1.1.2. Numerical characters (e.g., 1, 2, 3)

6.4.1.1.3. Alphabetic characters (e.g., a, b, c)

6.4.1.1.4. Combination of uppercase and lowercase letters

6.4.1.2 Passwords shall not use repeating, ascending, or descending character sequences (e.g., 12345, or abcde).

6.4.1.3 Passwords shall not use common words found in a dictionary, contain any part of a user’s name, or the organization’s name.

6.4.1.4 Passwords shall not be the same as any of the last nine previously used passwords.

6.4.1.5 Privileged accounts (e.g., administrator) passwords shall consist of a minimum of fifteen (15) characters and contain the four (4) characteristics mentioned above.

6.4.1.5.1. If the system is limited to less than fifteen (15) alphanumeric characters, then the administrator’s password length must be set to the maximum number of characters allowed by the operating system or application.

6.4.1.5.2. If it is less than eight (8) alphanumeric characters, an exception shall be submitted to the County CISO for consideration.

6.4.1.6 For instances of two-factor authentication, user defined Personal Identification Numbers (PINs) must be a minimum length of at least six (6) characters. This PIN will be used in conjunction with a six-digit randomly generated token PIN.

6.4.1.6.1. Authentication mechanisms (e.g., hard or soft tokens) must be assigned to an individual account and not shared among multiple accounts.

6.4.1.7 Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

6.4.1.8. Physical and/or logical controls must be in place to confirm that only the intended account can use that mechanism to gain access.

6.4.1.9 Password must expire or change, as follows:

6.4.1.9.1. Require change of initial (or temporary) password upon first-time login/use. Initial passwords shall be unique for each user and received in a secure manner.

6.4.1.9.2. Passwords/PINs must be changed immediately if a compromise is suspected.

6.4.1.9.3. User accounts passwords must be changed at least once every 180 days and administrator accounts must be changed at least once every 90 days. Shared account passwords must be changed every 30 days.

6.4.1.9.4. Enforce a minimum password age of at least one (1) day.

6.4.2. PINs used with approved two-factor authentication solutions do not have to be regularly changed. Passwords for IDs used for non-interactive system access (e.g., IBM Mainframe batch IDs, Microsoft Windows service accounts or password disabled Unix IDs) may be exempt from the 90-day password change requirement. The system-specific technical standards shall be referenced for additional and/or qualifying controls.

6.4.3. Departments must ensure that one-time use and temporary passwords must adhere to the following:

6.4.3.1 Passwords must not be sent via fax.

6.4.3.2 Passwords and usernames should be sent in separate emails.

6.4.3.3 Passwords must not be given via telephone unless the password administrator has positively identified the caller’s identity.

6.4.3.4 Initial passwords must be forced to be changed immediately upon their first use.

6.4.3.5 Initial passwords must be in compliance with password composition and password selection requirements noted in this standard.

6.4.4. Departments must ensure that security administrators must positively identify the identity of a user prior to a password reset.

6.4.4.1 Only the individual to whom the user ID is assigned can request a password reset.

6.4.4.2 Password resets shall not be performed prior to verification of the requestor’s identity.

6.4.4.3 If a self-service portal is not available, a “reset” password shall function as a one-time password required to be changed upon first use or login.

6.4.5. A user ID and password shall be authenticated in its entirety. If authentication fails, the system error message shall not indicate which component of the user’s input (user ID or password) is incorrect (e.g., “incorrect login,” or “incorrect password”).

6.4.6. Devices that are not AD authenticated must have unique complex passwords

6.4.7. Passwords usage and storage must be secure.

6.4.6.1 Default passwords for software or hardware shall be disabled or changed.

6.4.6.2 Where technically feasible, password filtering and password masking shall be implemented.

6.4.6.3 Password credentials shall be encrypted and shall never be transmitted in clear text.

6.4.6.4 Password files shall be stored in an encrypted form separate from the object or application data they protect.

6.4.6.5 Users must not share or reveal passwords to anyone.

7. CONTROL MAPPING

This chart is used to provide an efficient way to cross-reference this policy's components with the different industry-standard information security controls.

Section	NIST SP800-53 R4 (1)	CIS 20	NIST CSF
6.1 User and System Access Management	AC-1	-	ID.GV-1
	AC-2	CSC 16	PR.AC-1
	AC-3	CSC 5	PR.AC-4
	AC-5	CSC 5	PR.AC-4
	AC-6	CSC 5	PR.AC-4
	CM-5	CSC 3	PR.IP-1
	IA-2	CSC 16	PR.AC-1
	IA-8	CSC 16	PR.AC-1
	IA-9	CSC 16	PR.AC-1
	AC-21	-	PR.IP-8
	IA-1	-	ID.GV-1
		CSC 5	PR.PT-3
6.2 Account Management	AC-7	-	-
	AC-8	-	-
	AC-9	-	-
	AC-10	-	-
	AC-11	-	-
	AC-12	-	-
	AC-14	-	-
	AC-17	CSC 12	PR.AC-3
	IA-2	CSC 16	PR.AC-1
	IA-4	CSC 16	PR.AC-1
	IA-5	CSC 16	PR.AC-1
	IA-6	CSC 16	PR.AC-1
	IA-10	CSC 16	PR.AC-1
	IA-11	-	-
	PE-2	-	PR.AC-2
	PE-3	-	PR.AC-2
	SC-10	-	-
	AC-23	-	-
	AC-25	-	-
6.4 Password Management	IA-2	CSC 16	PR.AC-1
	IA-5	CSC 16	PR.AC-1

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
1.0	Jerry Keely	08/26/2020	Approved by Board of Supervisors