PINAL COUNTY
Enriching Lives Beyond Expectation

PINAL COUNTY
Acceptable Use of Information Technology

DATE:	PAGES:	POLICY NUMBER:
08/26/2020	11	11.002
REVISED:		

Acceptable Use of Information Technology Policy

Table of contents

1. Purpose

1.1. Pinal County collects, manages, and stores information on a regular basis in order to support its organizational operations. Pinal County is committed to preserving the confidentiality, integrity, and availability of its information assets.

Pinal County must protect its information assets, provide for the integrity of organizational processes and records, and comply with applicable laws and regulations.

This document, the *Acceptable Use of Information Technology Policy,* documents the responsibilities of all County Departments. Departments and offices are required to implement procedures that ensure their personnel, including vendors, contractors, and consultants, comply with requirements in regard to safeguarding information owned or entrusted to Pinal County.

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, executive offices, boards, commissions, departments, departments, divisions, councils, bureaus, offices, and vendors. Other County entities that voluntarily use or participate in services provided by the County, such as PinalCountyaz.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 policy.

4.2. The Information Security Department is responsible for monitoring compliance with this policy and may enlist other departments to assist in the enforcement of this policy.

4.3. Any inquiries or comments regarding this policy shall be submitted to the Information Security Department by contacting the security team at ITSecurity@Pinal.gov.

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

5. Compliance

5.1. Compliance with this document is mandatory for all County departments, and offices. 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 Pinal 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 Pinal County Chief Information Security Officer (CISO).

6. Policy Statements

6.1. Information Security Awareness Training

Pinal County is committed to establishing an information security-aware culture to help protect its information assets. To support this goal, Pinal County has established the following practices:

6.1.1. New hires: All new hires must complete an information security awareness training within the established new hire training timeline and regularly thereafter. Records demonstrating the completion of such training shall be maintained and reported to the Human Resources Department. Security awareness training will be made easily available for County Departments and Offices to provide to County employees.

6.1.2. Ongoing: All County Departments and Offices must ensure that their personnel participates in regular information security awareness training, including mandatory participation in periodic social engineering (e.g., phishing) training exercises and secure authentication. Records demonstrating the completion of such training shall be maintained and reported to the Information Security Department.

6.1.3. Job-specific: County departments may have some job functions that require additional information security training. The department will provide additional training requirements as needed. Examples may include personnel who have access to systems that store confidential information or job responsibilities such as developers and database administrators. The Pinal County CISO determines the job functions that require additional training.

6.1.4. A training report will be sent to the Information Security Department to track overall completion rates.

6.1.5. Training materials and subject matter will be regularly updated (at least annually) to address new technologies, threats, standards, and business requirements.

6.1.6. Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.

6.1.7. Deliver training to address the skills gap identified to positively impact workforce members' security behavior.

6.1.8. Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.

6.1.9. Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

6.1.10. Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

6.2. Acceptable Use of Information Assets

Pinal County's information assets further organizational goals and priorities. In using Pinal County's information assets, county departments and offices should encourage their personnel to act in a professional and ethical manner and comply with their applicable Code of Conduct, relevant enterprise, and department-level policies and/or applicable contractual obligations.

6.2.1 Use of information technology resources

6.2.1.1. It is unacceptable for any person to use department information technology resources:

6.2.1.1.1. In furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether County or federal.

6.2.1.1.2. For any political purpose.

6.2.1.1.3. For any commercial purpose.

6.2.1.1.4. To send threatening or harassing messages, whether sexual or otherwise.

6.2.1.1.5. To access or share sexually explicit, obscene, or otherwise inappropriate materials.

6.2.1.1.6. To infringe any intellectual property rights.

6.2.1.1.7. To gain or attempt to gain, unauthorized access to any computer or network.

6.2.1.1.8. For any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs.

6.2.1.1.9 To intercept communications intended for other persons.

6.2.1.1.10.To misrepresent either the department or a person's role in the department.

6.2.1.1.11.To distribute chain letters.

6.2.1.1.12.To access online gambling sites.

6.2.1.1.13.To libel or otherwise defame any person.

6.2.2 Email use:

The following instructions are designed to prevent personnel from engaging in harmful email practices:

6.2.2.1 Do not use email accounts for commercial purposes unrelated to County business.

6.2.2.2 Do not conduct government business through or send confidential information to a personal email account.

6.2.2.3 Do not send confidential information to any recipient not authorized to receive such information.

6.2.2.4 Do not transmit confidential information in an unencrypted format.

6.2.2.5 Do not collect and/or transmit material in violation of any federal, County, or local law or organizational policy.

6.2.2.6 Access to only county approved email providers will be permitted.

6.2.3 Use of technology assets

Personnel must use Pinal County's technology assets appropriately and comply with the following requirements:

6.2.3.1 Do not download or install unauthorized (e.g., unlicensed, pirated) software onto County-issued devices.

6.2.3.2 Avoid excessive use of system information technology resources for personal use, including but not limited to network capacity (e.g., high use of video streaming technologies).

6.2.3.3 Do not circumvent, attempt to circumvent or assist another individual in circumventing the information security controls in place to protect County-issued devices.

6.2.4 Secure transfer of information

6.2.4.1 Confidential information shall be securely exchanged through only authorized methods. Confidential Information shall not be electronically transferred in an unencrypted or unprotected format. Refer to Cryptography Policy # I-11.008 for additional details on data protection.

6.2.5 Record retention

6.2.5.1 Information storage and retention time frames shall be limited to what is required for legal, regulatory, and business purposes.

6.2.6 Secure workspace

6.2.6.1 Personnel must keep their assigned workspace secure (e.g., lock confidential information in drawers, use cable locks if issued by County).

6.2.6.2 Personnel must be mindful of using mobile devices (e.g., smartphones and tablets) with access to County information. Mobile devices must be secured with a password that meets or exceed the access control requirements and must not be left unattended.

6.2.6.3 When personnel are telecommuting or working remotely, County-owned devices must not be left unattended in public spaces, such as on public transportation, in a restaurant or coffee shop, or in a doctor’s office.

6.2.6.4 Documents containing confidential information that is sent to a shared printer must be retrieved immediately to reduce the risk of unauthorized access.

6.2.7 Privacy and monitoring

The use of County-owned information systems and assets is subject to monitoring and review.

6.2.7.1 Personnel should have no expectation of privacy with respect to Pinal County's communications systems.

6.2.7.2 County's communications systems (e.g., emails, instant messages, Internet usage) may be monitored, logged, reviewed, recorded, and/or investigated.

6.2.7.3 Records of activity on these systems may be used by Pinal County and/or turned over to law enforcement authorities and other third parties.

6.2.7.4 Personnel must be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic.

6.2.7.5 The department retains, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the department will exercise the right to inspect any user's computer, any information contained in it, and any information sent or received by that computer.

6.3. Information Protection

6.3.1 Information classification.

All County Executive Offices and Departments must ensure that County employees/personnel adhere to these requirements:

6.3.1.1 Personnel must adhere to the information classification system and ensure that appropriate measures are taken to protect information commensurate with its value to Pinal County. The information classification system includes Confidential, Internal Use, and Public. See Information Classification in the Asset Management Standard # 11.004 for additional details.

6.3.2 Information protection requirements

The confidentiality and integrity of information must be protected at rest, in use and in transit. Personnel must adhere to the following guidelines:

Information governed by compliance standards requires additional information protection requirements that are not addressed in this policy.

6.3.2.1 Information at rest

The following are guidelines to safeguard confidential information at rest:

6.3.2.1.1. Store all information on access-restricted and/or -controlled Shared Folders or Drives (e.g., S: and P: drives) or Google Drive.

6.3.2.1.2. Encrypt or password-protect removable media that contains confidential information such as USB drives and mobile devices.

6.3.2.1.3. Dispose of confidential information only after confirming compliance with records retention laws.

6.3.2.2 Information in use

The following are guidelines to safeguard confidential information in use:

6.3.2.2.1. For access to systems that host confidential information, personnel must request access using an approved access request process/tool and be positively authenticated (i.e., have an established user identity in Active Directory or another authentication source).

6.3.2.2.2. Use the minimum amount of confidential information (such as Social Security numbers) to the minimum necessary to support business operations (e.g., last four digits). Store the information in approved information repositories.

6.3.2.2.3. Where possible, do not store confidential information on laptops or desktops. Confidential information must be stored in Shared Folders, Shared Drives, or other secure County systems.

6.3.2.3. Information in transit

Use County-issued encryption solutions to protect the integrity of confidential information that will be transmitted outside of Pinal County. This can be achieved by the following:

6.3.2.3.1. Use the secure mail feature of email clients by adding “[secure]” in the subject line to encrypt the email.

6.3.2.3.2. Password-protect files that contain confidential information (See I-11.008 Cryptographic Management Standard).

6.3.2.3.3. Use Pinal County-approved secure transfer solution for larger transfers.

6.4. Access Management

Departments and offices must ensure that personnel is positively authenticated and authorized prior to receiving access to County information resources. Access to systems shall be based on the user's role and must be limited to the minimum rights necessary to perform his or her job function. Access to information assets must be controlled through a defined process, which includes a periodic review of information system privileges. (Refer to Access Management Standard)

6.4.1. User access to information systems

6.4.1.1 Authorization: Users must have an active user ID to access information assets on the Pinal County family of networks.

6.4.1.2 Authentication: Information assets that access or store confidential information must authenticate a user's identity (e.g., password) prior to granting access.

6.4.1.3 Access requests: Users must request access to technology infrastructure and/or applications required for job responsibilities using Pinal County-approved access request tools.

6.4.1.4 Least privilege: Users must not be granted access to technology infrastructure and/or applications that are not required to perform his/her job responsibilities. Managers are responsible for ensuring their direct reports have the appropriate access to systems.

6.4.1.5 Reviews of user's access to applications and/or technology infrastructure will be performed by Managers at least annually to ensure access is appropriate to perform his/her job responsibilities.

6.4.2 Protect your password

Passwords provide a foundational security control to protect access to systems, technology, infrastructure, applications and information.

6.4.2.1. Do not reveal passwords to others or allow others to use your passwords.

6.4.2.2. Maintain passwords in a secure manner. Do not write down or store passwords in an insecure manner.

6.4.2.3. Change default passwords upon the first login.

6.4.2.4. Passwords must be designed to meet the risks and threats of the technology environment and comply with the password standard, specified in the Access Management Standard.# 11.003

6.5. Network Access

County network access is restricted to authorized users only. Users must have a domain user identity to access the network.

6.5.1 Wireless Access

To improve mobility, connectivity, and collaboration opportunities, Pinal County provides two wireless (wifi) networks, ‘secured’ and ‘public’, at certain office locations. Users must be aware that not all internal applications will be available through public wifi. Personnel who wish to use wireless connections to conduct County business may be required to connect to the secured wifi.

6.5.2 Remote Access

Users who access the Pinal County network remotely must be authenticated prior to establishing a network connection.

6.6. Physical Access

County facilities and information assets must have appropriate physical access controls to protect them from unauthorized access. The important points that must be considered in physical security are as follows:

6.6.1 Users must have a County-issued badge and be prepared to present it if requested by building security.

6.6.2 Only authorized persons are allowed into access-controlled areas. Visitors are allowed but must be escorted in controlled areas.

6.6.3 Circumventing established access control systems (e.g., propping doors open or tampering with turnstiles and tailgating) is prohibited.

6.6.4 Tailgating is allowing a person to enter a secure access badge area without using their badge to be read by the door reader, this is prohibited.

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 SP800-50 R4 (1)	CIS Security 20 v6	NIST CSF
6.1 Information Security Awareness Training	PR.AT-1	CSC-17.3	ID.AM6
	RS.CS-4	CSC-19.6	-
6.2 Acceptable Use of Information Assets	PR.DS-3	CSC-14	-
	-	CSC-15	-
	-	CSC-16	-
	-	CSC-13.2	-
6.3 Information Protection	PR.DS-5	CSC-14.7	ID.AM6
	PR.DS-6	CSC-2.7	-
		CSC-2.8	-
		CSC-2.9	-
			-
			-
6.4 Access Management	PR.DS-7	CSC-18.9	ID.AM6
	PR.IP-1	CSC-15.5	-
			-
			-
			-
			-
			-
6.5 Network Access	PR.DS-5	CSC-14.7	ID.AM6
	PR.IP-1	CSC-16.7	
6.6 Physical Access	PR.AC-2	-	ID.AM6

8. Document Change Control

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