PINAL COUNTY
Enriching Lives Beyond Expectation

PINAL COUNTY
IT Information Security Policy

DATE:	PAGES:	POLICY NUMBER:
08/26/2020	9	11.000
REVISED:		

IT Information Security Policy

1. PURPOSE

1.1. Pinal County collects, manages and stores information on a regular basis in order to support business 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 business processes and records and comply with applicable laws and regulations. This document, the Information Security Policy (hereafter, the "Policy"), reinforces Leadership's commitment, establishes high-level functions of an information security program, and outlines information security requirements to safeguard information *assets* and assist Pinal County to achieve its strategic objectives.

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 and offices 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 the Pinal County. The document applies to all County departments including all executive offices, boards, commissions, divisions, councils and bureaus. Other Pinal 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.

4. RESPONSIBILITY

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

4.2. The Pinal County Information Security Department is responsible for compliance with this policy and may enlist other departments and offices in the maintaining and monitoring compliance with this policy.

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

5. COMPLIANCE

5.1. Compliance with this document is mandatory. 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.

6. INFORMATION SECURITY OBJECTIVES

The goal of the Information Security Program is to manage risk within Pinal County and achieve its information security objectives through the establishment of supporting policies, processes, and functions. The information security objectives of Pinal County are:

6.1. Enable organizational strategy through the protection of customer data and material nonpublic information.

6.2. Comply with applicable laws, regulations and contractual obligations with relevant stakeholders.

6.3. Establish a governance structure to effectively and efficiently manage information security risk.

6.4. Manage identified security risks to an acceptable (i.e., risk tolerance) level through design, implementation, and maintenance risk remediation plans.

6.5. Establish a culture of accountability and increase the level of awareness of all personnel in order to meet information security requirements.

6.6. Establish responsibility and accountability for information security policies and governance across Pinal County.

6.7. Communicate the effectiveness of protection technologies with all of Pinal County's organizations to establish standards, baselines and instill confidence in the county;'s ability to protect against threats.

Pinal County is committed to continually improving the Information Security Program to help ensure that its applicable information security objectives are met and it is able to adapt to changes in the cyber threat landscape and account for evolving organizational, legal and regulatory requirements.

7. COMMUNICATIONS

7.1. Pinal County's Information Security policies and standards will be publicly available on the Pinal.gov web site.

8. REPORTING REQUIREMENTS

8.1. Policy Violations

Compliance with this document is mandatory for all County departments and offices. Violation of this document may cause irreparable injury to Pinal County. 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.

8.2. Reporting of Policy Violations

Any violation of this policy should be reported to a supervisor and/or the Information Security Team. Information security incidents (e.g., security breaches) shall follow the reporting requirements outlined in the Information Security Incident Management Standard ISI.009.

8.3. Exceptions from Policy

The policy applies to all county departments including all executive offices, boards, commissions, divisions, councils and bureaus. In the event that a policy or procedure cannot be adhered to, a policy exception request must be submitted to and approved by Pinal County Chief Information Security Officer (CISO), or delegate. An exception may be granted only if the benefits of the exception outweigh the increased risks for the approved length of the exception, as determined by Pinal County CISO and the associated Information Owner. Compliance progress shall be validated at the exception expiration date. Exceptions may be closed if the agreed-upon solution has been implemented and the exception has been resolved. An extension may be requested if more time is required to implement the long-term solution by completing an extension request.

9. STANDARD STATEMENTS

9.1. Organization of Information Security

All departments and offices shall adhere to Pinal County’s information security program to safeguard the confidentiality, integrity, and availability of its information assets, as directed by Pinal County’s technology leadership.

9.2. Acceptable Use

Personnel are the first line of defense and have a shared responsibility to safeguard information owned or entrusted to Pinal County.

9.3. Access Management

Access shall be managed throughout the account lifecycle from the initial identification of a user to the granting, modifying and revoking of user access privileges to confirm that information assets are protected from unauthorized access. Accounts shall be provisioned using the least privilege access principle. Access privileges shall be monitored and reviewed periodically commensurate with their risk classification. Passwords must meet Pinal County’s complexity requirements and be changed on a regular basis.

9.4. Asset Management

Establish an information system classification schema to promote a consistent approach to risk management, business continuity and disaster recovery for information assets. Maintain an asset inventory and establish a program to manage the asset life cycle (i.e., procurement through end-of-support/end-of-life). Implement security controls to protect endpoints and mobile devices from malware and information leakage.

9.5. Business Continuity and Disaster Recovery

The organization's place in critical infrastructure and its industry sector is identified and communicated. The county must protect mission-critical information assets, processes, and facilities from the effects of major failures or disasters by developing and implementing a business continuity strategy that is consistent with organizational objectives and priorities. Backup critical data, such as confidential information, and strive to prevent disasters and implement timely recovery from disasters as well as continue critical organizational functions during a disaster or major disruption while maintaining confidentiality.

9.6. Communication and Network Security Management

Implement network security controls such as firewalls, intrusion prevention/detection systems (IPS/IDS), virtual private networks (VPNs) and segmentation techniques so that Pinal County protects its information assets from compromise both from external and internal actors.

9.7. Compliance

Establish a compliance framework that will enable Pinal County to comply with all relevant legislative, regulatory, statutory and contractual requirements related to information security.

9.8. Cryptographic Management

Define requirements for encrypting data at rest, data in transit and data in use, commensurate with the information classification of the information requiring protection. Maintain cryptographic keys to preserve the integrity of cryptographic controls. Use of encryption controls shall be determined after a risk assessment has been performed.

9.9. Information Security Incident Management

Establish a program to effectively detect, respond and resolve incidents that affect the security of Pinal County's information assets, including establishing a Cyber Incident Response Team (CIRT) to manage the incident response process. Develop incident response procedures/plans and identify relevant stakeholders (both internal and external). Test incident response plans periodically for relevancy.

9.10. Information Security Risk Management

Identify and analyze information security risks that could compromise the confidentiality or integrity of Pinal County's information assets, and mitigate them to an acceptable level to meet organizational objectives and compliance requirements. All relevant statutory, regulatory and contractual requirements that include security and privacy controls and Pinal County's approach to meet these requirements must be explicitly defined, documented and kept up to date.

9.11. Logging and Event Monitoring

Develop and implement a process to monitor and review activity on information systems. So that information system problems are identified and corrected, and operator logs and fault logging are enabled, collected and reviewed. Pinal County must comply with all relevant legal, regulatory and contractual requirements applicable to logging and event monitoring.

9.12. Operations Management

Develop and document standard operating procedures, change management, configuration management, capacity management and release management processes for technology environments. Back up information in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

Establish standards to support the secure implementation of applications and services in public and private cloud environments, including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

9.13. Physical and Environment Security

Enforce physical security controls to manage access to information assets. Physically protect facilities with safeguards to protect information assets against environmental hazards.

9.14. Secure System and Software Life Cycle Management

Perform information security reviews throughout all phases of the system and software management lifecycle to ensure risks are properly identified, addressed and mitigated in a timely and cost-efficient manner. Configure systems using security hardening standards and review configurations periodically.

9.15. Third-party Information Security

Establish a process to perform initial and ongoing due diligence of third parties that enter into formal business arrangements with Pinal County departments and offices. Contractual agreements between third parties and Pinal County departments and offices must address baseline information security clauses, including, but not limited to, the right to audit and adhere to data protection requirements.

9.16. Vulnerability Management

Implement security controls to manage and monitor risks to Pinal County's information technology environment. Vulnerability management personnel must be able to identify and respond to vulnerabilities within established and predictable timeframes. Vulnerability management activities must be reported to management periodically.

10. POLICY FRAMEWORK COVERAGE

Policy ref.	Policy/Standard name	Topics covered
11.001	Organization of Information Security	• Information Security Organization Structure • Roles and Responsibilities • Policy Framework • Policy Life Cycle Management
11 002	Acceptable Use of Information Technology	
11.003	Access Management	• User and System Access Management • Account Management • Password Management
11.004	Asset Management	• Information Asset Management • Information Protection Requirements • Information Classification • Information System Classification • Information Labeling and Handling • Endpoint Security • Information Disposal • Mobile Device Management
11.005	Business Continuity and Disaster Recovery	• Business Continuity • Disaster Recovery
I-11.006	Communication and Network Security	• Network Security Management • Remote Access Security Management • Secure File Transfer • Management of Third-party Network Access

11.007	Compliance	• Compliance with Policies, Standards, Guidelines, and Procedures • Reporting Security Incidents and Violations • Security Compliance Reviews • External Attestation of Compliance
I-11.008	Cryptographic Management	• Key Management • Approved Cryptography Techniques
I-11.009	Information Security Incident Management	• Information Security Incident Management
11.010	Information Security Risk Management	• Information Security Risk Management • Security Awareness and Training
11.011	Logging and Event Monitoring	• Logging and Event Monitoring
11.012	Operations Management	• Standard Operating Procedures • Change Management • Configuration Management • Capacity Management • Release Management • Data Backup and Restoration • Cloud Computing
11.013	Physical and Environment Security	• Facility Controls and Secure Areas • Equipment and Other Media Security
I-11.014	Secure System and Software Lifecycle Management	• Security in System and Software Life Cycle • Security in SDLC Support Processes • System Hardening
11.015	Third Party Information Security	• Contractual Security Risk Identification • Third-party Selection • Contractual Security Provisions • Third-party Life Cycle Management
I-11.016	Vulnerability Management	• Vulnerability and Patch Management
N/A	Glossary of Terms	N/A

Table 1 — Policy Structure

11. DOCUMENT CHANGE CONTROL

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