PINAL COUNTY Enriching Lives Beyond Expectation	PINAL COUNTY Organization of Information Security
	DATE: 08/26/2020 REVISED: PAGES: 10 POLICY NUMBER: 11.001

Organization of Information Security Standard

Table of contents

1. PURPOSE

1.1 The purpose of this standard is to:

- Protect the County’s business information by establishing, implementing and managing risk-based administrative, technical and personnel safeguards.
- Establish responsibility and accountability for information security in the organization.
- Comply with relevant laws, regulations and contractual obligations related to information security.

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 executive offices, 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.

4. RESPONSIBILITY

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

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

5. COMPLIANCE

5.1. Compliance with this document is mandatory for all County departments. 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 Security Department (mailto:ITSecurity@Pinal.gov). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by Pinal County Chief Information Security Officer (CISO) or designee.

6. POLICY STATEMENTS

6.1. Information Security Organization Structure

6.1.1 The Pinal County Information Technology Security Department is responsible for cyber security across Pinal County.

6.2. Roles and Responsibilities

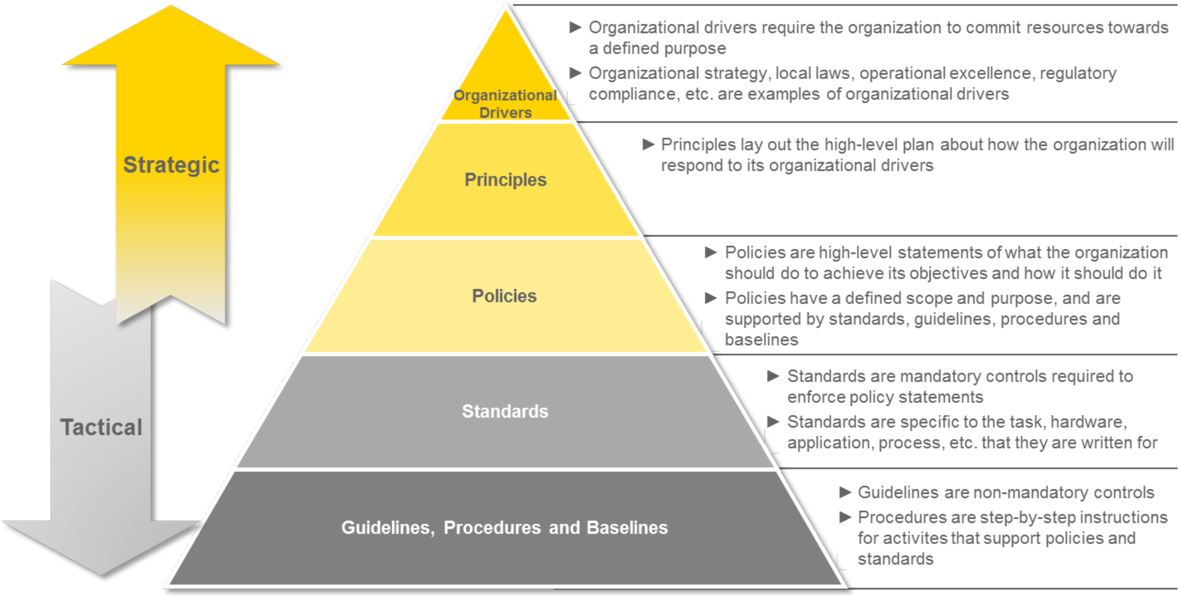
The information security function covers a broad range of activities that touch on multiple organizational facets. In order to effectively and consistently manage information security across the organization, the following roles and responsibilities are defined and referenced across relevant policies and standards.

Role	Responsibility
Chief Information Security Officer (CISO)	The person responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that communication systems, ***confidential information*** and technologies are adequately protected.
Information Security Team	The team responsible for the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Custodian	The person responsible for overseeing and implementing the necessary safeguards to protect communication systems and confidential information, at the level classified by the ***Information Owner*** (e.g., System Administrator, controlling access to a system component).
Personnel	The County's County employees, contractors, consultants, vendors, and interns, including full time, part-time, temporary, or voluntary regardless of rank, position or title on Pinal County payroll.

6.3. Information Security Policy Framework

The Information Security Policy serves as a foundation for the County's information security program and outlines the governance framework that has been adopted by the County's leadership to govern information security across the organization.



- ▶ Organizational drivers require the organization to commit resources towards a defined purpose
- ▶ Organizational strategy, local laws, operational excellence, regulatory compliance, etc. are examples of organizational drivers
- ▶ Principles lay out the high-level plan about how the organization will respond to its organizational drivers
- ▶ Policies are high-level statements of what the organization should do to achieve its objectives and how it should do it
- ▶ Policies have a defined scope and purpose, and are supported by standards, guidelines, procedures and baselines
- ▶ Standards are mandatory controls required to enforce policy statements
- ▶ Standards are specific to the task, hardware, application, process, etc. that they are written for
- ▶ Guidelines are non-mandatory controls
- ▶ Procedures are step-by-step instructions for activites that support policies and standards

Figure 1 - Information Security Policy Framework (ISPF)

6.3.1. Policy framework details

The County's ISPF consists of the set of policies, standards, guidelines and procedures (PSGP). The framework is defined as follows:

6.3.1.1. Policies are mandatory, management statements, instructions or organizational rules that guide behavior and set operational goals. Policies shall be concise and easily understood.

6.3.1.2. Standards are a mandatory set of technical configurations used to ensure that a minimum level of security is provided across multiple implementations of business services, systems, networks and products used throughout Pinal County.

6.3.1.3. Procedures contain process-specific operational steps or methods to support the requirements contained in the related policy and/or standard. Executive Offices and departments are encouraged to develop internal procedures that comply with these policies and standards.

6.3.1.4. Guidelines are the statements that provide optional control recommendations based on leading practices.

6.3.1.5. Policy Areas

Pinal County has defined 1 enterprise-level information security policy, 1 enterprise acceptable use of information technology policy and 10 core enterprise security standards as follows:

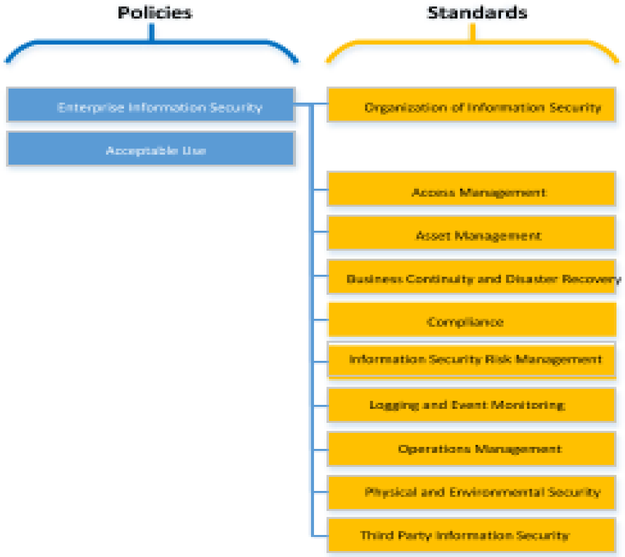

Policies
Standards
Enterprise Information Security
Acceptable Use
Organization of Information Security
Access Management
Asset Management
Business Continuity and Disaster Recovery
Compliance
Information Security Risk Management
Logging and Event Monitoring
Operations Management
Physical and Environmental Security
Third Party Information Security

Figure 2 — Information Security Policy Framework

6.4. Policy Life Cycle Management

The Information Security policy framework serves to govern the life cycle of the County’s Information Security PSGPs.

6.4.1. Implementation and compliance monitoring

6.4.1.1. The Information Security Department is responsible for implementing procedures for monitoring compliance with information security PSGPs.

6.4.1.2. The Information Security Department shall assist departments to develop tools and enablers to measure their compliance with policies and standards.

6.4.2. Policy exceptions

6.4.2.1. All County departments that receive or expect to receive IT/IS services from Pinal County are expected to comply with enterprise information security policies and standards. Departments and offices are required to implement procedures that ensure their personnel, including consultants, contractors, and vendors, comply with these requirements.

6.4.2.2. In the event that a policy, procedure or technical standard cannot be adhered to, a policy exception request must be submitted via email to (ITSecurity@Pinal.gov).

6.4.2.3. An exception will 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 or Delegate.

6.4.2.4. Compliance progress shall be validated at the exception expiration date.

6.4.2.5. Exceptions may be closed if the agreed-upon solution has been implemented and the exception has been resolved.

6.4.2.6. An extension may be requested if more time is required to implement the long-term solution by completing an extension request.

6.4.2.7. Compliance with policies and standards will be enforced through regular audits by the

Information Security Department. The Information Security department will also offer support if needed to rectify any gaps in the capacity of a county entity to ensure compliance.

6.4.3. Additions, changes, and deletions to policies and standards

6.4.3.1. County departments may request a new or modification to an enterprise policy or standard by submitting a change request to the Information Security Department.

6.4.3.2. Each request must include the business justification for requesting a change.

6.4.3.3. The Information Security Department shall review each request and recommendations. The CISO will provide approval or denial.

6.4.3.4. The Information Security Department is responsible for ensuring all approved changes or additions to information security policies and standards are documented and communicated to County departments in a timely manner.

6.4.4. Review process

6.4.4.1. Information security PSGPs shall be reviewed on a regular basis to ensure they are consistent, practical and properly address the following:

6.4.4.1.1. Legal, regulatory and contractual requirements.

6.4.4.1.2. Organizational needs and impact: Controls remain effective from both a cost and process perspective and support the business without causing unreasonable disruption on the timely execution of those processes.

6.4.4.1.3. Emerging technology environment: Opportunities and threats created by changes, trends and new developments are taken into account.

6.4.4.1.4. Internal technology environment: Strengths and weaknesses resulting from the County's use of technology are considered.

6.4.4.1.5. Other requirements specific to new or unique circumstances are evaluated.

6.4.5. Review intervals

6.4.5.1. A review of information security policies, procedures and standards shall be performed by the Document Owner, as follows:

6.4.5.1.1. Policies: Review at least once every year.

6.4.5.1.2. Standards: Review at least once every year.

6.4.5.1.3. Procedures: Review at least once a year by process owner.

6.4.5.2. In addition to the defined review cycle, relevant information security PSGPs shall be considered for review and update:

6.4.5.2.1. When a significant change is identified in the technology, business, or regulatory environment that may have a substantial impact on the County’s risk posture.

6.4.5.2.2. As part of the post-mortem of security incident response process.

6.4.5.2.3. After the performing of an internal or external review that identifies a need for change.

6.4.6. Dissemination

6.4.6.1. Information Security PSGPs shall be published and made accessible to the entities covered under the scope of this policy.

6.4.6.2. ***Policies*** and ***Standards*** are public documents that are published on the PinalCountyAZ.gov web site. ***Guidelines*** and ***Procedures*** contain specific information about County infrastructure and are therefore ***Internal Use Only*** documents that should be distributed on a limited basis outside of Pinal County with vendors and partners on a need to know only basis.

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 Security 20 v6	NIST CSF
6.1 Information Security Organization Structure	PM-1	-	ID.GV-1
	PM-8	-	ID.BE-2
	PM-11	-	ID.AM-6
6.2 Roles and Responsibilities	-	-	-
6.3 Information Security Policy Framework	PM-9	-	ID.GV-4
	PM-15	CSC 4	ID.RA-2
	PM-16	CSC 4	ID.RA-2
	PM-12	-	ID.RA-3
	PM-4	-	ID.RA-6
	PM-13	CSC 17	PR.AT-1
	PM-6	-	PR.IP-7
	PM-14	CSC 19	PR.IP-10
			ID.GV-2
			ID.GV-3
6.4 Information Security Policy Lifecycle Management	AT-2	CSC 17	PR.AT-1
	AT-3	CSC 5	PR.AT-2
	PL-1	-	ID.GV-1
	PL-2	-	PR.IP-7

	PL-3	-	-
	PL-6	-	-
	PL-9	-	-

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
1.0	Jerry Keely	8/26/2020	Approved by Board of Supervisors

The owner of this document is Pinal County CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement shall be submitted to the document owner.

9.1 Annual Review

This *Organization of Information Security Standard* shall be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.