
	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007

Compliance Standard

Table of contents

PURPOSE	2
AUTHORITY	2
SCOPE	2
RESPONSIBILITY	2
COMPLIANCE	2
STANDARD STATEMENTS	3
Compliance with Policies, Standards, Guidelines and Procedures (PSPG)	3
Reporting Security Incidents and Violations	4
Security Compliance Reviews	4
External Attestation of Compliance	5
CONTROL MAPPING	7
RELATED DOCUMENTS	8
DOCUMENT CHANGE CONTROL	8

	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007

1. PURPOSE

- 1.1. Compliance - this standard defines the requirements to ensure that Pinal County complies with all relevant legislative, regulatory, statutory and contractual requirements 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 the county. The document applies to all departments including 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 PinalCountyaz.gov, must agree to comply with this document, with respect to those services, as a condition of use. All 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 this standard and may enlist other departments to assist with the monitoring and maintenance of 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 ITSecurity@Pinal.gov.
- 4.4. Additional information regarding this standard 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 departments including all boards, commissions, divisions, councils, and bureaus. Violations are subject to disciplinary action in

	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007


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 Information 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 the Pinal County Chief Information Security Officer (CISO).

6. STANDARD STATEMENTS

6.1 Compliance with Policies, Standards, Guidelines and Procedures (PSPG)

The Information Security Department shall ensure information enterprise security policies, standards, guidelines and procedures (PSGPs) are in place, communicated, implemented and enforced. The Information Security Department or Internal Audit shall conduct periodic assessments and reviews for compliance with PSGPs.

- 6.1.1. The Information Security Department shall ensure information security PSGPs are in place, communicated, implemented and enforced. Leading information security industry standards shall serve as guidance when developing and updating PSGPs.
- 6.1.2. The Information Security Department, in consultation with the legal department, shall be aware of and ensure that all relevant regulatory requirements are met. The Information Security Department shall use global information security industry standards to serve as guidance when developing and updating the PSGPs.
- 6.1.3. The Information Security Department shall perform periodic assessments and reviews for compliance with IS PSGPs and applicable regulations.
- 6.1.4. The Information Security Departments shall ensure compliance deficiencies identified during compliance reviews are remediated by the responsible Executive Office or Department. County Executive Offices and Departments will in turn ensure that their Information Owner or Information Custodian work to remediate and rectify any gaps in compliance.
- 6.1.5. The Information Owner, in collaboration with the Information Security Department (as needed), shall complete all regulatory reporting or audits as required. This includes compliance with all relevant Pinal County laws as well as federal and commercial compliance requirements including Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) Security Policy, Federal Tax Information (FTI) and others.
- 6.1.6. Reporting frequency shall be strictly respected.

	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007


6.2 Reporting Security Incidents and Violations

- 6.2.1. County Executive Offices and Departments must ensure that County personnel are responsible for knowing and complying with applicable information security requirements.
- 6.2.2. County Executive Offices and Departments must ensure that potential violations shall be reported to an immediate supervisor or to the Information Security Department at ITSecurity@Pinal.gov. Failure to report a violation is itself a violation that may lead to disciplinary action.
- 6.2.3. Personnel who for any reason do not wish to discuss the problem directly may refer their concerns to their Human Resources (HR) representative.
- 6.2.4. Personnel will not be retaliated against for any good-faith complaint or violation report.
- 6.2.5. Information related to data breaches, incidents and investigations shall be managed and communicated in accordance with the *Information Security Incident Management* Guideline I-11.009.

6.3 Security Compliance Reviews

Information security risks that could compromise the confidentiality, integrity or availability of Pinal County's information assets shall be identified, analyzed and mitigated to an acceptable level to meet organizational objectives and compliance requirements.

- 6.3.1. Pinal County shall adopt a structured approach for assessing IS risks, identifying threats and vulnerabilities and implementing mitigation strategies (see *11.010 Information Security Risk Management Standard*).
- 6.3.2. The Information Security Department shall develop, disseminate and review annually a formal, documented security review and accountability plan, with specific review and accountability goals, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and formal documented procedures to facilitate the implementation of the review and accountability plan and associated review and accountability controls.
- 6.3.3. Controls to safeguard operational systems and audit tools during information systems reviews shall be implemented.

	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007

6.3.3.1. Monitoring on mission-critical or high-risk systems must be persistent, and controls shall be implemented to tamper-proof the supporting log collection and analysis mechanisms.

6.3.3.3. Audit logs must be retained in accordance with the log retention requirements (see the *Logging and Event Monitoring Standard 11.011*).

6.3.4. Review of audit events

6.3.4.1. Pinal County shall implement hardware, software, applications and services that shall have the capability of creating audit records containing security events in accordance with logging and monitoring procedures.

6.3.4.2. The Information Security Department shall review and update at a minimum annually the listing of security events to be audited. Information assets owned by Pinal County that log security events shall have their security logging capability operational at all times.

6.3.4.3. Information Security Department or IT Operations, as appropriate, shall employ technology innovation to develop the capability to automate the storage and analysis of security audit records and reduce audit report generation. Audit records for security events of interest based on event criteria shall be analyzed by automated systems. The systems shall also be able to process ad hoc queries of security events.


6.4 External Attestation of Compliance

Pinal County may employ a third party to conduct external attestation or agreed-upon procedure examinations (“Attestation Engagements”) for specific County departments.

Attestation Engagements are designed to provide reasonable assurance that a set of predefined trust principles, which address the information security risks of functions and processes, are achieved, and that Pinal County is equipped to effectively control these risks where they may exist in systems.


6.4.1. Attestation engagements

On an annual basis or as a result of a material change to the organization, Pinal County CISO, in consultation with the Risk Management Department, shall develop as part of the annual security plan a process that initiates independent reviews (e.g., penetration tests, audits and assessments) of Information Security.

	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007

The third party may evaluate County systems based on the following principles and criteria, as applicable:

- 6.4.1.1. Security: the system is reasonably designed and operated to be protected against unauthorized access (both physical and logical).
- 6.4.1.2. Availability: the system is reasonably designed and operated to be available for operation and use as committed or agreed.
- 6.4.1.3. Processing integrity: the system processing is reasonably designed and operated to be complete, accurate, timely and authorized.
- 6.4.1.4. Confidentiality: there are reasonable steps taken to protect confidentiality consistent with applicable County policies or to which otherwise agreed, including access by personnel.
- 6.4.1.5. Privacy: where applicable, privacy policies and procedures are defined and documented.
- 6.4.2. Attestation engagements shall be specific to the Pinal County department being tested and may include different criteria across departments. The third party shall work with county departments individually to determine the appropriate principles and criteria for the specific examination.
 - 6.4.2.1. Prior to undertaking any engagement, all third parties must sign confidentiality agreements and agreements covering their services, and steps must be taken by the relevant departments in accordance with the *Third Party Information Security Policy* 11.015 and other criteria the requesting department may deem necessary.
- 6.4.3. Attestation engagement testing results shall be:
 - 6.4.3.1. Recorded and reported to Information Owners, department management; and as appropriate the Risk Management Department. Report shall include an update on the lifecycle of the mitigation plans for identified risks.
 - 6.4.3.2. Maintained consistent with the records retention requirements identified by the Clerk of The Board.
- 6.4.4. Oversight and organization: County departments shall oversee the schedule of Attestation Engagements for their respective department, coordinate with the third party to begin relevant engagements, and track the progress of engagements as they occur. Results shall be reported to the Information Security Department and relevant parties.

	PINAL COUNTY Compliance		
	DATE: 08/26/202 REVISED:	PAGES: 8	POLICY NUMBER: 11.007

6.4.5. Engagement scoping: In scoping the engagement, the Pinal County department shall clearly establish the boundaries of what is to be assessed. As part of the scoping, ownership of each system, function or process under review, must be clearly established so the assessment remains in scope and the correct individuals are identified to provide any required information. Departments shall take into account that the results of Attestation Engagements may be for external distribution, unlike internal audits.

6.4.6. Storage and distribution:

6.4.6.1. County departments shall securely store and maintain the full results of their Attestation Engagements, and the Information Security Department shall securely store and maintain copies of all department Attestation Engagements.


6.4.6.2. The results of external Attestation Engagements may be shared with county stakeholders, including external entities that wish to gain an understanding and assurance of the security and integrity of the respective departments and functions, and the efficacy of controls in place to reduce risks, should they exist.

6.4.6.3. Any decision to distribute Attestation Engagements results to external entities shall be made in consultation with Legal to address, among other things, any attorney-client privilege protections and requirements for non-disclosure agreements prior to distributing the results to the requestor.

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 v6	NIST CSF
6.1 Compliance with policies, standards, guidelines and procedures	AC-2	CSC 16	PR.AC-1
	CA-2	CSC 4	ID.RA-1
	CA-7	CSC 4	ID.RA-1
	IA-7	CSC 16	PR.AC-1
	PE-8	-	-
	SI-12	-	-
6.2 Reporting security incidents and violations	AU-6	CSC 6	PR.PT-1
	IR-1	-	ID.GV-1
	IR-6	CSC 19	RS.CO-2
	SI-2	CSC 4	ID.RA-1
	SI-4	CSC 4	ID.RA-1
	SI-5	CSC 4	ID.RA-1
6.3 Security compliance reviews	PL-4	-	-
	RA-3	CSC 4	ID.RA-1
	CA-2	CSC 4	ID.RA-1
	CA-7	CSC 4	ID.RA-1

	PINAL COUNTY Compliance		
	DATE: 08/26/202	PAGES: 8	POLICY NUMBER: 11.007
REVISED:			

	RA-5	CSC 4	ID.RA-1
	-	-	PR.IP-7
6.4 External attestation of compliance	IA-7	CSC 16	PR.AC-1
	SC-13	CSC 13	PR.DS-5
	AC-2	CSC 16	PR.AC-1
	CA-2	CSC 4	ID.RA-1
	CA-7	CSC 4	ID.RA-1
	PE-8	-	-
	SI-12	-	-
	AU-1	-	ID.GV-1
	AU-2	CSC 6	PR.PT-1
	AU-9	CSC 6	PR.PT-1
AC-20	-	ID.AM-4	

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