
	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

Operations Management Standard

Table of contents

PURPOSE	2
AUTHORITY	2
SCOPE	2
RESPONSIBILITY	2
COMPLIANCE	3
STANDARD STATEMENTS	3
Standard Operating Procedures	3
Change Management	3
Configuration Management	4
Capacity Management	5
Release Management	6
Data Backup and Restoration	6
Cloud Computing	8
CONTROL MAPPING	11
RELATED DOCUMENTS	12
DOCUMENT CHANGE CONTROL	12

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

1. PURPOSE

1.1. Operations Management Standard -The purpose of this standard is to document the requirements and key information security considerations for information technology operations, including the definition of standard operating procedures, change management, configuration management, release management, information backup and restoration and cloud computing.

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 Pinal County 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 County. The document applies to all of Pinal County departments, and all boards, commissions, divisions, councils, bureaus, offices and vendors. Other County entities that voluntarily use or participate in services provided by the Pinal County Department of Technology Services and Security, such as PinalCountyaz.gov, must agree to comply with this document as a condition of use. Pinal County 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 this policy and may enlist other departments to assist in the monitoring and maintenance of compliance with this policy.
- 4.3. Any inquiries or comments regarding this policy shall be submitted to the Information Security Department by sending an email to <mailto: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>.

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

5. COMPLIANCE

5.1. Compliance with this document is mandatory for all of Pinal County including all boards, commissions, offices, 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 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. Standard Operating Procedures


County Offices and Departments must document standard operating procedures for critical and high-risk information systems, which should be defined by the incident response policy including technical details to include:

- 6.1.1. Secure installation and configuration of systems.
- 6.1.2. Secure processing and handling of information (automated and manual).
- 6.1.3. Job scheduling requirements, including interdependencies with other systems.
- 6.1.4. Error and exception handling procedures.
- 6.1.5. System restart and recovery procedures to restore service in a timely manner in the event of system failure.
- 6.1.6. Logging requirements, including maintaining an audit trail for operational and security events, monitoring procedures and log management procedures (see Logging and Event Monitoring Standard for additional details).
- 6.1.7. Support and escalation procedures, including contact information of technical support staff.

6.2. Change Management

County Offices and Departments must implement a change management process that includes:

- 6.2.1. Definition of change request categories (High, Medium, Low risk).


	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

- 6.2.2. Definition of the change request approval process, including the level of involvement of the Change Advisory Board — High and Medium risk must be approved by the Change Advisory Board.
- 6.2.3. Identification and documentation of all change requests in a system of record.
- 6.2.4. Planning and testing of changes prior to implementation.
- 6.2.5. Verification that information security and compliance (e.g., regulatory) requirements have been met.
- 6.2.6. Identification of stakeholders and definition of communication channels to communicate change details.
- 6.2.7. Fallback procedures to recover from unsuccessful changes and unforeseen events.
- 6.2.8. Definition of the emergency change request process.
- 6.2.9. Definition of a process (define the frequency of review) to perform a periodic review of the change management process to ensure compliance.
- 6.2.10. Emergency change requests should be regularly audited to ensure the process is being used for its intended purpose.

6.3. Configuration Management

Pinal County offices and departments must establish controls to maintain the integrity of information systems, including:

- 6.3.1. Maintain an asset inventory of authorized hardware and software. Update the asset inventory on a regular basis. Maintain information
 - 6.3.1.1 Only vendor supported Software and Hardware are to be considered authorized and reported as such. All other software should be tagged as unsupported in the inventory.
- 6.3.2. Deploy network Discovery tools (e.g., Tripwire IP360, NMAP, Cisco CDP) to monitor the presence of hardware and software operating within the environment. Establish an action plan to address unauthorized or unsupported information systems on the network.


	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

- 6.3.3. Create, maintain and update standard operating procedures for the secure configuration of information systems. Assess compliance with configuration requirements at least annually.
- 6.3.4. Establish security hardening guideline for information systems, including commercial off-the-shelf (COTS) products. Assess compliance with security hardening requirements at least quarterly.
- 6.3.5. Deploy automated configuration management tools to track configuration settings of information systems deployed within the County’s environment (where technically feasible). Develop action plans to address exceptions or open a risk exception.
- 6.3.6. Obtain County CISO (or most senior security executive for departments) approval prior to implementing changes to network devices that may have an adverse effect on the County security posture. Changes must be implemented by qualified personnel.
- 6.3.7. Maintain standard, documented security configuration standards for all authorized network devices.
- 6.3.8. Log and audit configuration changes to information systems and applications that may affect county security posture or system operation or functionality. Changes must be consistent with details recorded in the change request ticket.
- 6.3.9. To the extent possible, prohibit the use of generic and shared user IDs for configuration management activities. Change requests shall be logged and monitored on a regular basis.
- 6.3.10. All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and if an expected duration of the need has an ending period, note on the infrastructure calendar to change.
- 6.3.11. Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

6.4. Capacity Management

County Offices and Departments must establish a capacity management process, including:

- 6.4.1. Document a capacity management plan for mission critical systems.


	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

- 6.4.2. Perform periodic server consolidation assessments to reduce the IT footprint.
- 6.4.3. Decommission applications, databases and systems that are not required within an acceptable time frame. Information systems that must remain operational beyond their end-of-life (e.g., vendor support life cycle) must be approved by the County CISO (or designee).
- 6.4.4. Optimize application logic, database queries, batch processing (e.g., mainframe), etc. to reduce processing power requirements and bandwidth utilization.
- 6.4.5. Deny or restrict bandwidth for resource-hungry services that are not critical for business operations when bandwidth is an issue (e.g., video streaming).
- 6.4.6. Rationalize disk space and remove unnecessary data that is not subject to record retention requirements.
- 6.4.7 Regularly evaluate system hardware to validate system integrity.

6.5. Release Management

County Offices and Departments must document release management processes for IT environments and/or platforms.


- 6.5.1. Maintain separate development, test and production environments where required or practical.
- 6.5.2. Source code must be reviewed and tested in a lower environment prior to promotion to the production environment.
- 6.5.3. Production data may be used in a lower environment (non-production) only if security controls for the lower environment are consistent with the production environment.
- 6.5.4. Developers must not have the ability to migrate code into production environments without an appropriate check and balance system in place..
- 6.5.5. If a dedicated release management role is not in place, County Offices and Departments must ensure that personnel are issued separate accounts to perform their release management duties. Monitoring shall be implemented and audited where technically feasible.

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

6.6. Data Backup and Restoration

The County Information Technology department has an established process to backup information in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

- 6.6.1. Data backup and retention requirements and timeframes are detailed in the internal IT guideline I-11.012.6.6-Gdln-Backup and Restoration
- 6.6.2. The decision to backup must be informed by a business impact analysis (BIA) or a risk assessment that considers the following factors:
 - 6.6.2.1. Business needs.
 - 6.6.2.2. Security requirements.
 - 6.6.2.3. Criticality of the information.
- 6.6.3. Backup and recovery must be included as part of the business continuity and disaster recovery planning.
- 6.6.4. Backup and recovery documentation must be reviewed, tested and updated regularly.
- 6.6.5. Backup records must be accurate and complete, including exception tracking (i.e., success/failures to backup). Documented restoration procedures must be maintained for assets critical to the organization.
 - 6.6.5.1. At a minimum, data owner, classification of data, time of capture, retention duration and storage location must be captured.
- 6.6.6. Backup data must not be stored on the same media (i.e., electronic) or physical location (e.g., magnetic tapes) as the primary data source.
 - 6.6.6.1. Backup on removable media that will be transferred or stored offsite must be encrypted.
 - 6.6.6.2. Backup on removable media shall be protected from physical and environmental hazards.
 - 6.6.6.3. Backup on removable media shall be stored in secure areas under lock and key. Only authorized individuals should have physical access to backup tapes. Access logs must be maintained and reviewed on a regular basis.

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

6.6.6.4. Backup on removable media shall be disposed of using secure deletion methods upon the end of life as defined in the Physical Media Handling in the Asset Management Standard.

6.6.7. Backup records subject to legal holds shall be managed in accordance with guidance provided by Legal.

6.6.8. Implement data protection controls such as encryption to protect the confidentiality and integrity of backups.

6.6.8.1. For backup data that is encrypted and requires long or indefinite retention timeframes, consider key rotation in accordance with the Cryptographic Management Standard.

6.6.8.2 Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

6.6.8.3 Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

6.6.8.4 Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.


6.7. Cloud Computing

County Offices and Departments must establish standards to approve and support the secure implementation of new applications and services in public and private cloud environments.


6.7.1. The following are general requirements for all applications regardless of application tier (See Information System Classification in Asset Management Standard 11.004 for application tiers):

6.7.1.1. The cloud provider shall provide a mechanism to track performance metrics against contractual obligations, including information on major outages and time for resolution.

6.7.1.2. Prior notification must be provided for maintenance activities, specifically, for any update, upgrade or maintenance of software or hardware equipment that may impact system performance.

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

- 6.7.1.3. Contracts must include minimum security clauses, the right to audit and relevant data protection requirements.
- 6.7.1.4. The cloud service provider must be able to produce vulnerability assessment reports such as SOC 1 type 2, SOC 2 type 2, PCI self-assessment questionnaire (if applicable) upon request.
- 6.7.1.5. Application owners must be assigned for each application hosted in the cloud.
- 6.7.1.6. Operational policies, standards and procedures must be defined for cloud based applications, including:
 - 6.7.1.6.1. Access control.
 - 6.7.1.6.2. Cryptography.
 - 6.7.1.6.3. Operations security (change and configuration management).
 - 6.7.1.6.4. Service development and maintenance.
 - 6.7.1.6.5. Information security incident management.
 - 6.7.1.6.6. Business continuity and recovery plan.
- 6.7.1.7. Business continuity and disaster recovery plans must be documented and consistent with Business Continuity and Disaster Recovery 11.005.
- 6.7.1.8. Service level agreements, including system uptime, availability and scalability (bandwidth, storage and transactional volume) must be defined during the contracting phase and codified in contractual agreements.
- 6.7.1.9. Backup, data restoration and data retention must be consistent with the Data Backup and Restoration section of this standard.
- 6.7.1.10. Data retention and retrieval periods, including the length of time within which the County can retrieve its data from the cloud provider post contract termination must be codified.
- 6.7.1.11. Incident response plans and escalation procedures must be defined for applications hosted in the cloud. Periodic metrics of security events must be provided to the County by the cloud service provider.

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

6.7.1.12. Patch management process must be defined, critical security patches must be deployed within a reasonable timeframe.

6.7.1.13. Access to applications must be role-based. Roles must be defined and documented. Quarterly audits of user roles must be conducted to verify appropriate separation of duties.

6.7.1.14. Users with administrative privileges must have separate user accounts for normal activities. Use of administrative accounts must be logged and periodically audited.

6.7.1.15. Generic accounts are prohibited for interactive accounts. Users must be issued individual accounts. Where technically feasible, the cloud service provider shall integrate with a County directory service to obtain identities (e.g., Active Directory).

6.7.1.16. Password policies must be consistent with the Access Management Standard 11.003, any exceptions must have a documented exception agreement and approval from the County CISO (or designee).

6.7.1.17. Security reference and solution architecture diagrams must be defined for cloud-based applications. Application and system dependencies and interfaces must be documented.

6.7.2. In addition to Section 6.7.1, cloud applications that have a High-risk tiering (as per Asset Management Standard 11.004, Section 6.7.4) must:

6.7.2.1. Provide evidence of information security training and background checks for personnel working on cloud computing deployments supporting the County.

6.7.2.2. Develop a contingency plan if a cloud service provider is acquired or goes out of business.


6.7.2.3. Document secure systems development and maintenance life cycle process.

6.7.2.4. Define privacy and data protection requirements, including:

6.7.2.4.1. Control content replication across technology environments.

6.7.2.4.2. Control format, accuracy and encryption.

6.7.2.4.3. Control who can access content.

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12

6.7.2.4.4. Control content life cycle and disposal.

6.7.2.4.5. Encrypt confidential data at rest.

6.7.2.4.6. Encrypt confidential data in transit.

6.7.2.5. Implement security monitoring controls, including the ability to monitor and detect anomalous activity. Logs shall be sent to the enterprise SIEM.


6.7.2.6. Implement intrusion detection and prevention controls.

6.7.2.7. Implement forensics capabilities to assist the investigation in the case of a security incident or breach.

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 800-53	CIS 20	NIST CSF
6.1. Standard Operating Procedures	AU-1	-	ID.GV-1
	AU-2	CSC 6	PR.PT-1
	AU-3	CSC 6	PR.PT-1
	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	AU-8	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1
	SI-11	-	-
6.2. Change Management	CP-2	-	ID.AM-5
	CM-1	-	ID.GV-1
	CM-3	CSC 3	PR.IP-1
	CM-4	CSC 3	PR.IP-1
	CM-5	CSC 3	PR.IP-1
	CM-9	CSC 3	PR.IP-1
6.3. Configuration Management	AC-5	CSC 5	PR.AC-4
	CM-1	-	ID.GV-1
	CM-3	CSC 3	PR.IP-1
	CM-4	CSC 3	PR.IP-1
	CM-5	CSC 3	PR.IP-1
	CM-7	CSC 3	PR.IP-1

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12


	CM-8	CSC 1	ID.AM-1
	CM-9	CSC 3	PR.IP-1
	AC-5	CSC 5	PR.AC-4
	AU-1	-	ID.GV-1
	CM-2	CSC 18	PR.DS-7
	CM-6	CSC 3	PR.IP-1
	AU-2	CSC 6	PR.PT-1
	AU-3	CSC 6	PR.PT-1
	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	AU-8	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1
6.4. Capacity Management	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	CP-2	-	ID.AM-5
	SA-2	-	-
	SC-5	-	PR.DS-4
6.5. Release Management	SC-32	-	-
6.6. Data Backup and Restoration	CP-9	CSC 10	PR.IP-4
6.7. Cloud Computing	AC-16	CSC 5	PR.AC-4
	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

	PINAL COUNTY Operations Management		
	DATE: NUMBER: 11.012 REVISED:	PAGES: 08/26/2020	POLICY 12
