
	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

Asset Management Standard

Table of contents

PURPOSE	2
AUTHORITY	2
SCOPE	2
RESPONSIBILITY	2
COMPLIANCE	3
STANDARD STATEMENTS	3
6.1 Information Asset Management	3
6.2 Inventory of information assets	4
6.3 Ownership of information assets	5
6.4. Acceptable use of assets	6
6.5 Information Asset Disposal	6
6.6 Information Protection Requirements	7
6.7 Information System Classification	8
6.8 Endpoint Security	9
6.9 Mobile Device Management	10
CONTROL MAPPING	12
RELATED DOCUMENTS	13
DOCUMENT CHANGE CONTROL	13

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

1. PURPOSE

- 1.1. The purpose of this standard is to document the requirements and key security considerations to enable the ongoing ownership and effective management of County's information assets.

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 boards, commissions, divisions, councils, bureaus, and offices. 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.

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 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 ITSecurity@Pinal.gov.
- 4.4. Additional information regarding this standard and its related standards may be found at <https://www.pinalcountyz.gov/HR/Pages/PoliciesProceduresRules.aspx>

5. COMPLIANCE

- 5.1. Compliance with this document is mandatory for all departments including all executive offices, boards, commissions, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

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 Security Office (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) or appointed designee.

6. STANDARD STATEMENTS

6.1 Information Asset Management


The Information Technology Department will track sensitive equipment assets valued below \$5000 in a manner consistent with Pinal County Capital Asset Policy pnp 8.80.

- 6.1.1. Pinal County Finance issues Fixed Asset Tags for equipment and systems valued at \$5000 and greater.
- 6.1.2. Pinal County IT Shipping and Receiving (S&R) will issue an IT Tracking Tag for equipment listed in Table 1.0; that is delivered or processed through S&R and is valued below \$5000 and greater than the value assigned in Table 1.0

Sensitive Equipment Assets to receive IT Tracking Tags
Table 1.0

	Type	Tracking Tag	Serial Number	Value Greater than
1	Computers	X	X	\$1.00
2	Laptops	X	X	\$1.00
3	Servers	X	X	\$1.00
4	Monitors (PC Display)	X	X	\$1.00
5	Printers / Multi Function Printers	X	X	\$100.00
6	Scanners	X	X	\$100.00
7	Projectors	X	X	\$100.00
8	Television Monitors	X	X	\$500.00
9	UPS (uninterruptible power supply)	X	X	\$500.00
10	Network Equipment	X	X	\$1000.00

software

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004


6.2 Inventory of information assets

County departments shall use software based inventory tools throughout the organization to automate identifying and updating all information assets (i.e., physical, Logical and software) and document the importance of these assets. The asset inventory should include all information necessary in order to effectively manage the information asset throughout its life cycle from creation/receipt through disposal. At a minimum, the following attributes shall be recorded (where applicable):

- 6.2.1. Information system type (e.g., server, router, smartphone)
- 6.2.2. Manufacturer (e.g., Cisco, Dell, Apple)
- 6.2.3. Model and/or version number
- 6.2.4. Asset tag, serial number or some other unique identifier
- 6.2.5. IP address (if applicable)
- 6.2.6. Information Owner (business and technical)
- 6.2.7. Classification level
- 6.2.8. Business criticality
- 6.2.9. Physical location (office building, room, city and county) and details of the virtual environment (if applicable)
- 6.2.10. License information and details regarding ownership, expiration and maintenance (if applicable)
- 6.2.11. End-of-support/end-of-life date and considerations (if applicable)


6.3 Ownership of information assets

Information Owners shall be identified for all information assets. The implementation of specific controls may be delegated by the information owner, as appropriate, but the owner remains

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

responsible for the management and security of the information asset. Specifically, the Information Owner shall:

- 6.3.1. Ensure that the information asset is accurately inventoried and classified.
- 6.3.2. Ensure that the information asset has appropriate access restrictions.
- 6.3.3. Perform periodic reviews to verify appropriate access; review frequency shall be dictated by the application classification level found in section 6.7 of this document.
- 6.3.4. Manage risk to the information asset, including mitigating the risks associated with operating at end-of-support/end-of-life (if applicable).
- 6.3.5. Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
- 6.3.6. Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
- 6.3.6. Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.
- 6.3.7. Pinal County's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.
- 6.3.8. Pinal County's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.
- 6.3.9. Determine frequency and methodologies to perform scheduled hardware integrity checks, and perform these checks as scheduled on all hardware assets.
- 6.3.10. Maintenance and repair of assets should be logged as changes and repairs are made to assure accurate technical representations of the changes applied. The reporting should be done using approved and county maintained tools.
- 6.3.11. Maintenance and repair of assets by a 3rd party should be logged as changes and repairs are made to assure accurate technical representations of the changes applied. Accessing county assets by 3rd party persons or vendors should be tracked and reviewed in such a way that will prevent unauthorized access to county assets. The reporting should be done using approved and county maintained tools.

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

6.4. Acceptable use of assets

Departments and offices with personnel that have access to information assets owned or managed by the County must be aware of their associated permissions and restrictions.

6.5 Information Asset Disposal


Establish procedures for the secure disposal and sanitization of media to minimize the risk of confidential information leakage.

- 6.5.1. Log the disposal of confidential information to maintain an audit trail.
- 6.5.2. Verify that the information assets containing any confidential information have been removed or securely overwritten prior to disposal or reuse.
 - 6.5.2.1. Render media unusable (e.g., degaussing), unreadable or indecipherable prior to disposal.
 - 6.5.2.2. Use acceptable industry standards (e.g., 7-pass overwrite) for information erasure to ensure information is unrecoverable.
 - 6.5.2.3. Use a third-party service that specializes in information or media disposal.
 - 6.5.2.4. Regulatory compliance requirements may supersede this standard.

6.6 Information Protection Requirements


The following table summarizes the information protection requirements for County information.

Security Considerations	Public	Internal Use	Confidential
-------------------------	--------	--------------	--------------

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004





Impact of unauthorized disclosure	No harm.	Limited harm.	Significant harm.
Access restrictions	None.	Access normally restricted to employees and approved nonemployees for business purposes only.	Access granted only to authorized individuals.
Encryption	None required.	None required.	County-approved encryption required (see Approved Cryptographic Techniques in the Cryptographic Management Standard).
Physical labeling (paper, magnetic media, CD/DVD/USB or tape label)	None required.	Information classification label must be visible. All magnetic media assets must be sent in lockable containers with a label affixed across the opening of the container.	Information classification label must be visible. All magnetic media assets must be sent in lockable containers. The label should not be affixed on outside of shipping container.
Electronic labeling (digital file, email or webpage)	None required.	E-mail: non-disclosure disclaimer must be visible.	E-mail: information must be labeled and encrypted.
Physical disposal (paper, tape or hard drives)	None required.	After applicable electronic disposal, secure onsite or off-site physical disposal using County approved methods.	After applicable electronic disposal, secure onsite disposal using County-approved methods. Paper – Shred or use secure disposal bins. Electronic media — render unreadable or unrecoverable, depending on the use case. Disposal audit trail required.
Electronic disposal (Digital file)	None required.	Removal of the directory entry for the file.	Removal of the directory entry for the file. File space should be overwritten using industry standards where possible.

6.7 Information System Classification


	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

To promote a consistent approach to risk management, business continuity and disaster recovery, etc. processes, all information systems shall be classified. Information Owners are responsible for determining the information system classification of their information system.

- 6.7.1. The classification of an information system shall be based on its most critical component (e.g., where information is transmitted, processed or stored).
- 6.7.2. County departments must conduct a business impact analysis or a risk assessment to determine information system classifications for its information assets.
- 6.7.3. Information system classification must be reviewed at least annually and whenever a significant system change occurs.
- 6.7.4. Classify all information systems as follows:


Classification level(s)		Description
	Critical	<ul style="list-style-type: none"> ■ Information assets subject to legal and/or regulatory requirements if breached (e.g., HIPAA, PCI) ■ Critical core network infrastructure, including perimeter firewalls, routers, switches, domain name server (DNS) and cloud services ■ Systems that generate or manage in excess of \$1m or more per annum for the County (e.g., HIX, MMIS) ■ Systems involved in the transmission or processing of financial information
	High	<ul style="list-style-type: none"> ■ High-value assets that store, process or transmit confidential information ■ Core business support systems (e.g., email) ■ Externally facing systems that process or handle confidential information ■ Systems that impact payroll or similar internal processes ■ End-of-life information systems no longer supported by a vendor and without a risk exception on file ■ Confidential information
	Medium	<ul style="list-style-type: none"> ■ Non-core business support systems, including externally facing systems that do not process confidential information Internal Use information
	Low	<ul style="list-style-type: none"> ■ Development, test and quality assurance environments or user workstations Public information

6.8 Endpoint Security

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

Endpoint security controls to protect against malicious software, including viruses and malware, shall be implemented.

- 6.8.1. Implement antivirus solutions on all endpoints.
- 6.8.2. Implement endpoint detection and response (EDR) solutions on high-risk information systems (including endpoints) that store confidential data persistently.
- 6.8.3. Configure antivirus and/or EDR solutions to detect, remove and protect against known types of malicious software.
- 6.8.4. Configure antivirus and/or EDR solutions so that they cannot be circumvented, disabled or removed from an endpoint by an end user.
- 6.8.5. In the event a non-AI (Artificial Intelligence) based Anti-Virus (AV) is used, update antivirus definitions in accordance with their severity rating (Vulnerability Management Guideline I-11.016). Signature definitions must be centrally managed (e.g., System Center Configuration Manager SCCM) and pushed to endpoints. End users must not be able to prevent updates to their County-issued endpoint. Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
- 6.8.6. Retain audit logs for antivirus and EDR solutions for at least three (3) months readily available for analysis (see Logging and Event Monitoring Standard 11.011).
- 6.8.7. Integrate antivirus and EDR solutions with the enterprise Security Information and Event Management (SIEM), where technically feasible.
- 6.8.8. Full-disk encryption must be configured for all laptops. Desktops that store confidential information on a persistent basis must implement full-disk encryption.
 - 6.8.8.1. Encryption keys must be centrally managed. Mechanisms to recover encryption keys in the case of loss shall be available and tested.
- 6.8.9. Implement host-based firewall solutions for information systems with direct connectivity to the Internet (e.g., laptops used by personnel at home or on public Wi-Fi), which are used to access the organization's network.
- 6.8.10. Implement host-based firewalls for end of life (EOL) information systems.
- 6.8.11. Implement host-based intrusion prevention systems (IPS) on high-risk systems.


	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

- 6.8.12. Implement controls to protect endpoints from virus and malware that can be introduced via removable media (e.g., USB storage media).
- 6.8.13. Utilize an antimalware program that will scan the USB before use or if AI will monitor USB devices for malicious behavior.
- 6.8.14. Disable functionality that allows auto-run upon insertion of removable media.
- 6.8.15. Force encryption on removable media prior to allowing information transfer to and from the media that is determined to be sensitive by the owning department.
- 6.8.16. Implement technical controls to restrict the installation of unauthorized software on County-owned or managed endpoints.
- 6.8.17. Restrict the use of local administrator privileges on endpoints to those individuals with a business need (e.g., help desk or designated security administrators).
- 6.8.18. An up-to-date inventory of users with persistent access to administrative privileges must be maintained and reported to the County CISO on a quarterly basis.
- 6.8.19. Third parties that require a connection to the County family of networks must have up-to-date antivirus and antimalware solutions installed.
- 6.8.20. Test all detection systems regularly to ensure effectiveness and accuracy of detections and reporting functionality.

6.9 Mobile Device Management

The County shall implement a mobile device management (MDM) solution to manage mobile devices owned by the County with the exception of certain devices determined to remain un-managed by the Pinal County Chief Information Officer.

- 6.9.1. The MDM solution shall support, at a minimum, the following functionalities:
 - 6.9.1.1. Provides the highest coverage of mobile devices and operating systems.
 - 6.9.1.2. Inventory management (i.e., self-enrollment, directory integration, enforcement of acceptable use policy, remote wipe, backup and restore, etc.).
 - 6.9.1.3. Device policy management (i.e., centralized enforcement of policy, group/location policies, and compliance checks).

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

6.9.1.4. Security management (i.e., information and device encryption, information segmentation, logging and monitoring, password/PIN management, jailbreak detection).

6.9.1.5. Monitoring and reporting (i.e., configurable dashboard, device tracking, canned/custom reporting).

6.9.2. Controls shall be implemented to prevent unauthorized disclosure of information on mobile devices (e.g., mobile phones and tablets).

6.9.3. Users must obtain authorization to use a personal mobile device to directly access County information.

6.9.3.1. Users that voluntarily choose to use their personal mobile device for County businesses must sign off that they understand the risk of using a mobile device and adhere to County policies and standards.

6.9.3.2. Sign off that he/she understands and accepts risks associated with using a mobile device that is owned or managed by the county, including inclusion in the mobile inventory, installation of an MDM solution, enforcement of password policy, authorization to review and retrieve phone information and remote wipe.


6.9.4. Create an inventory of all mobile devices (county-owned and personal) that connect to the County family of networks. The inventory shall be reviewed at least annually and include ownership information and device specifications (e.g., manufacturer, model, OS).

6.9.5. Personal mobile devices that directly connect to the county family of networks or that have direct access to the county's confidential information shall connect via VPN and an inventory of devices authorized to connect must be actively maintained (see *Remote Access in the Communication and Network Security Guideline I-11-006 and Information Asset Management in the Asset Management Standard 11.004*).

6.9.6. County-owned information-at-rest on mobile devices shall be encrypted with an approved software encryption solution (see *Approved Cryptographic Techniques in the Cryptographic Management Guideline I-11.008*).

6.9.7. Enforce password requirements for mobile devices through technical means as outlined in *Password Management in the Access Management Standard 11.003*.

6.9.8. Restrict mobile device users from making modifications of any kind to County owned or installed hardware and software on the mobile device.

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004


6.9.9. Mobile devices, regardless of ownership, housing county information shall be securely decommissioned, when no longer needed for business or legal reasons.

6.9.10. County departments must ensure mobile device users are aware of the risks involved with mobile computing and the types of information that can and cannot be stored on such devices, through regular security awareness training.

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 Information Asset Management	CM-8	CSC 1	ID.AM-1
	CM-9	CSC 3	PR.IP-1
	PM-5	-	-
	PL-4	-	-
		CSC 2	ID.AM-2
6.3 Ownership of Information Assets	RA-2	-	ID.AM-5
6.5 Information Disposal	SI-12	-	-
		-	PR.IP-6
	MP-6	CSC 1	PR.DS-3
6.6 Information Protection Requirements	AC-22	-	-
	AC-3	CSC 5	PR.AC-4
	MP-Family	-	-
	SC-28	CSC 14	PR.DS-1
	SI-12	-	-
6.7 Information System Classification	RA-2	-	ID.AM-5
6.8 Endpoint Security	PE-16	CSC 1	PR.DS-3
	SI-12	-	-
	MP Family	-	-
	PE-2	-	PR.AC-2
	PE-3	-	PR.AC-2
	PE-6	-	PR.AC-2
	PE-7	-	-
	PE-8	-	-
	PE-18	-	PR.IP-5
	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-6	CSC 6	PR.PT-1
	AU-7	CSC 6	PR.PT-1
	AU-9	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1

	PINAL COUNTY Asset Management		
	DATE: 08/26/2020 REVISED:	PAGES: 13	POLICY NUMBER: 11.004

	AU-14	CSC 6	PR.PT-1
	SI-4	CSC 4	ID.RA-1
		-	DE.DP Family
6.9 Mobile Device Management	CM-8	CSC 1	ID.AM-1
	AC-1	-	ID.GV-1
	AC-17	CSC 12	PR.AC-3
	AC-18	CSC 11	PR.PT-4
	AC-19	CSC 12	PR.AC-3
	PL-4	-	-
	PS-6	CSC 13	PR.DS-5
	AC-24	-	-

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