
	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

Logging and Event Monitoring Standard

Table of contents

PURPOSE	1
AUTHORITY	2
SCOPE	2
RESPONSIBILITY	2
COMPLIANCE	3
STANDARD STATEMENTS	3
Logging and Monitoring	3
System Types	9
CONTROL MAPPING	10
RELATED DOCUMENTS	10
DOCUMENT CHANGE CONTROL	10

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

1. PURPOSE

1.1. This standard establishes requirements for security monitoring and event management to detect unauthorized activities on Pinal County information systems. This standard defines the following related controls and acceptable practices:

- Audit requirements for user activities, exceptions and information security events.
- Logging activities and actions required to resolve system fault errors.
- Guidelines for the frequency of reviewing audit logs.
- Protection of audit logs through technical controls such as file permissions.
- Integration of suspicious audit events and investigation into incident response processes.

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 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 and offices to assist in 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 contacting the Security Program Office at <mailto:ITSecurity@Pinal.gov>.

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

4.4. Additional information regarding this standard 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 boards, commissions, 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 Team (<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. Logging and Monitoring

Pinal County Offices and Departments must ensure that a process to capture key security events associated with information system components (e.g., network devices, servers, databases) shall be developed and implemented to monitor system activity. Logging must be enabled on all systems and networking devices throughout the entire environment. These processes must be routinely tested to ensure accuracy, efficiency and reliability.

6.1.1 Audit logging

Record user activities, exceptions and information security events where technically feasible; at a minimum, record:

6.1.1.1. User IDs.


6.1.1.2. Dates, times and details of key events .

6.1.1.3. Logon success or failure indication.

6.1.1.4. Identity or name of affected data, system component, or resource and location (if possible).

6.1.1.5. Records of successful and rejected data and other resource access attempts (e.g., user attempts to query database, improper modification of data).

6.1.1.6. Changes to critical system configuration.

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

6.1.1.7. Escalation of privileges.

6.1.1.8. Use of system utilities and applications.

6.1.1.9. Network addresses and protocols.

6.1.1.10. Alarms raised by the access control system.

6.1.1.11. Activation and deactivation of protection systems (e.g., antivirus systems and intrusion detection systems).

Audit logs may contain confidential personal data or user information. Appropriate security measures must be taken to ensure all confidential information is adequately protected and handled (see Asset Management policy 11.004).

6.1.2 Monitoring system use

Pinal County Offices and Departments must ensure that they have enabled audit functionality for systems and system components linked to individual user accounts (i.e., Pinal County personnel).

6.1.2.1. Pinal County Offices and Departments must ensure that Information Custodian shall work with the Information Owner to identify required information system components that require monitoring system use such as those that process, store or transmit confidential information and/or are public facing (e.g., web server).


6.1.2.2. Pinal County Offices and Departments must ensure that the Information Owner must employ technical solutions at the network, host, application and database tiers to detect anomalous activity.

6.1.2.3. Intrusion-detection systems and/or intrusion prevention systems must be used to monitor traffic at the network perimeter and at critical entry points to the internal network (e.g., network segments that host confidential information).

6.1.3 System event monitoring

Pinal County Offices and Departments must ensure that at a minimum, the following system events shall be monitored:

6.1.3.1. All authorized user access to confidential information and audit trails, including:

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

6.1.3.1.1. User ID.

6.1.3.1.2. Date and time of key events.

6.1.3.1.3. Types of events.

6.1.3.1.4. Files accessed.

6.1.3.1.5. Program/utilities used.

6.1.3.2. All privileged operations, including all actions taken by any individual with root or administrative privileges:

6.1.3.2.1. Use of privileged accounts, e.g., supervisor, root, administrator.

6.1.3.2.2. System startup and stop.

6.1.3.2.3. System clock time changes.

6.1.3.2.4. I/O device attachment/detachment.

6.1.3.2.5. Modification/flushing of log files.

6.1.3.3. Unauthorized access attempts:

6.1.3.3.1. Failed or rejected user actions.

6.1.3.3.2. Failed or rejected actions involving restricted or confidential information or system components.

6.1.3.3.3. Access policy violations and notifications for network gateways and firewalls.


6.1.3.3.4. Alerts from proprietary intrusion detection systems.

6.1.3.4. System alerts or failures:

6.1.3.4.1. Console alerts or messages.

6.1.3.4.2. Network management alarms.

6.1.3.4.3. Alarms raised by the identity and access control systems.

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

6.1.3.5. Changes to, or attempts to change, system security settings and controls, including initialization, stopping or pausing of the audit logs.

6.1.3.6. Use of and changes to identification and authentication mechanisms — including but not limited to creation of new accounts and elevation of privileges — and all changes, additions or deletions to accounts with root or administrative privileges.

6.1.3.7. Creation and deletion of system-level objects (e.g., database tables or stored procedures).

6.1.3.8 Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

6.1.4 Administrator and operator logs

Pinal County Offices and Departments must ensure that Information Owner activities must be logged and monitored. An intrusion detection system managed outside of the control of the Information Owner (e.g., system and network administrators) should be used to monitor Information Owner activities for compliance. Logs shall include:

6.1.4.1. Time at which an event (success or failure) occurred.

6.1.4.2. Information about the event (e.g., files handled) or failure (e.g., error occurred and corrective action was taken).


6.1.4.3. Which account and which administrator or operator was involved.

6.1.4.4. Which system processes were involved (e.g., boot process, loading kernel modules).

6.1.4.5. Where possible, Information Owners shall not have permission to erase or deactivate logs of systems they own.

6.1.5 Log review and reporting

Pinal County Offices and Departments must ensure that logs must periodically be reviewed by personnel from the Information Security Department (or personnel with a security role in the agency) to detect anomalous events and apply resolution in a timely manner. Mechanisms shall be implemented to retrieve and report information on the logged events. Where technically possible, logs should be fed to the appropriate SIEM.

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

6.1.5.1. The Information Security Department shall use multiple log harvesting, parsing and alerting tools to help facilitate the identification of log events that need to be reviewed, including:

6.1.5.1.1. All security events.

6.1.5.1.2. Logs of all system components that store, process or transmit confidential information, or that could impact the security of confidential information.

6.1.5.1.3. Logs of all critical system components.

6.1.5.1.4. Enable and collect logs for servers and system components that perform security functions (e.g., Active Directory, firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS) and authentication servers).

6.1.5.1.5. Where third parties are providing and managing information systems for a Pinal County Office and Agency, contractual obligations shall include considerations for capturing log capturing log information.

The frequency of reviews shall be as follows (unless superseded by regulatory requirements):


Asset value	Log review frequency
Critical	Weekly
High	Weekly
Medium	Monthly
Low	Quarterly

6.1.5.2. Forward logs to a central log collection service and analyze through automated data correlation tools.


6.1.5.3. Any interruption to the logging process (failure) must be reported to the Security Office promptly. The report should include details on the cause, expected duration, expected remediation timeline and classification of information impacted.

6.1.6 Log protection

Pinal County Offices and Departments must protect logs from unauthorized access and in accordance with legal, regulatory and contractual obligations.

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

- 6.1.6.1. Restrict access to audit logs to those in need to know. The Information Security Department must approve log access for individuals who are not pre authorized to access logs.
- 6.1.6.2. Implement controls to safeguard and protect the integrity of logs, including:
 - 6.1.6.2.1. Limit read access of audit trails to those with a job-related need.
 - 6.1.6.2.2. Protect the audit logs from unauthorized modification using file-integrity monitoring tools; compare logs for consistency at least weekly.
 - 6.1.6.2.3. Use a secure transmission protocol to send log data from one system to another for processing.
 - 6.1.6.2.4. For external-facing technologies, write logs to a secure internal log server or media device.
 - 6.1.6.2.5. Back up audit trails to a centralized log server.
 - 6.1.6.2.6. Use hashing or other approved forms of integrity protection to protect logs under legal hold.
- 6.1.6.3. Prohibit disclosure of audit logs with confidential information to third parties unless authorized by Pinal County CISO and Legal. Remove confidential information if technically possible.
- 6.1.6.4. Retain audit trails for the required retention periods per business, legal or regulatory need. Audit log history must be retained for at least three (3) months and be immediately available for analysis.
- 6.1.6.5. Synchronize operating systems clocks for information systems with an approved Network Time Protocol (NTP) server or similar device.
 - 6.1.6.5.1. Critical systems have the correct and consistent time.
 - 6.1.6.5.2. Time data must be protected.
 - 6.1.6.5.3. Use at least three synchronized time sources from which all that servers and network devices retrieve time information on a regular basis so timestamps in logs are consistent.


	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

- 6.1.6.6. Ensure that all systems that store logs have adequate storage space for the logs generated.
- 6.1.6.7. Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
- 6.1.7.8. Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
- 6.1.7.9. On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.
- 6.1.7.10. Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
- 6.1.7.11. Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
- 6.1.7.12. Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
- 6.1.7.13. Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

6.2. System Types

The following types of information systems should have logging enabled.

Category	System type
Infrastructure components	<ul style="list-style-type: none"> • Intrusion detection and intrusion prevention systems • Web proxies • Core network switches • Network routers • Network and web application firewalls • Domain Name Servers (debug logging) • Authentication servers • Domain Host Configuration Protocol (DHCP) • Web servers • Network Time Protocol (NTP) servers • Mail servers • File Transfer Protocol (FTP) servers

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

Service applications	<ul style="list-style-type: none"> • Remote access software • Virtualization management (e.g., Citrix, VMware) • Active Directory • File servers • Anti-Malware protection services • Host-based firewalls • Host-based intrusion detection • Vulnerability management software
Business applications	<ul style="list-style-type: none"> • Applications and enabling services (e.g., web server) • Operating systems • Databases

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	NIST CSF
6.1 Logging and Event Monitoring	AU-1	-	ID.GV-1
	AU-6	CSC 6	PR.PT-1
	AU-7	CSC 6	PR.PT-1
	AU-9	CSC 6	PR.PT-1
	PE-6	-	PR.AC-2
	PE-8	-	-
	SC-7	CSC 9	PR.AC-5
	SI-4	CSC 4	ID.RA-1
	AU-2	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1
	SI-2	CSC 4	ID.RA-1
	AU-8	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-10	CSC 6	PR.PT-1
	AU-13	CSC 6	PR.PT-1
	AU-15	CSC 6	PR.PT-1
	AU-16	CSC 6	PR.PT-1
SA-13	-	-	

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes

	PINAL COUNTY Logging and Event Monitoring		
	DATE: NUMBER: 11.011 REVISED:	PAGES: 08/26/2020	POLICY 10

1.0	Jerry Keely	08/26/2020	Approved by Board of Supervisors

The owner of this document is the 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 should be submitted to the document owner.