ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8330 System Security Audit

What?

This policy outlines how State agencies must manage audit logs, which are records of events that happen on their computer systems. This includes what events to log, how to store and protect those logs, and how to review them.

When?

This policy is always in effect and applies to all State agency systems.

Why?

To help agencies detect and respond to security incidents, ensure accountability, and demonstrate compliance with regulations. Audit logs provide a valuable record of what happened on a system, who did it, and when.

Who?

Anyone involved in or responsible for managing agency systems.

How?

- **Event Logging:** Determining which events to log, such as login attempts, file access, and system changes.
- **Audit Record Content:** Ensuring that audit records contain important information (who, what, when, where).
- **Storage and Protection:** Storing audit logs securely and protecting them from tampering.
- **Review and Analysis:** Regularly reviewing audit logs for suspicious activity.
- **Backups and Retention:** Back up audit trails to a centralized log on a separate system. Retain logs to meet requirements.

Remember:

- The policy emphasizes the importance of complete and accurate audit logs.
- It requires agencies to have procedures for responding to audit log failures (e.g., if the system can't store any more logs).
- Audit logs are a critical part of a comprehensive security program.

Where?

You can find more specifics on this policy HERE

If you have ANY questions about this or any other IT policy, **please contact** grc@azdohs.gov.

Effective: January 16, 2024