ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8220 System Security Maintenance

What?

This policy sets the rules for keeping state agency information systems secure and well-maintained. This includes everything from managing system configurations and software updates to protecting against malware and responding to security incidents.

When?

This policy applies throughout the entire lifecycle of a system:

- **Prior to utilization:** When setting up new systems or making changes to existing ones.
- **During operations:** Regularly monitoring, maintaining, and performing security checks.

Why?

- **Protect State Data:** Safeguard sensitive information from unauthorized access and security threats.
- **Prevent Problems:** Proactive maintenance and security measures help avoid system failures and breaches.
- **Ensure System Stability:** Regular updates and proper configuration keep systems running smoothly.
- **Meet Legal Requirements:** Comply with Arizona laws and federal standards for system security.

Who?

This policy applies to everyone involved in managing and using state systems, including:

- **Agency Leadership:** Directors, CIOs, and ISOs who oversee system security.
- **IT Staff:** Those responsible for maintaining and managing systems.
- **Security Personnel:** Those who monitor systems for threats and respond to incidents.

How?

This policy requires agencies to:

- **Manage Configurations:** Keep track of all hardware and software and ensure they are set up securely.
- **Control Changes:** Follow strict procedures for any system updates or modifications.
- **Protect Against Malware:** Implement and maintain anti-malware software and procedures.
- **Monitor Systems:** Continuously track system activity and watch for security threats.
- **Remediate Flaws:** Address security vulnerabilities promptly and effectively.
- **Maintain Systems:** Perform regular maintenance to keep systems up-to-date and running smoothly.

Remember:

- **Document Everything:** Maintain detailed records of system configurations, changes, and maintenance activities.
- **Stay Informed:** Keep up with the latest security threats and best practices for system maintenance.
- **Prioritize Security:** Make system security an ongoing priority, not just a one-time task.

Note: *For detailed guidance on specific security controls and procedures, refer to the full policy document and consult with your agency's IT and security staff.*

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