ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8240 Incident Response Planning

What?

This policy outlines the State's procedures for incident response planning (IRP). The goal is to enable agencies to quickly detect and respond to incidents, minimizing damage and restoring normal operations.

When?

This policy applies to all users and agency systems. Additionally, specific requirements apply to systems handling Protected, Payment Card Industry, Protected Health Information, and Federal Taxpayer Information, respectively.

Why?

This policy is designed to:

- **Establish Agency Requirements:** Agencies must develop, implement, and maintain an IRP that is tested annually.
- **Enhance Incident Response:** Improve the agencies' abilities to detect, respond to, and recover from incidents.
- **Minimize Loss:** Reduce the impact of incidents on agency operations.
- **Mitigate Vulnerabilities:** Address weaknesses exploited during incidents.
- **Restore Services:** Ensure timely restoration of computing services.

Who?

This policy applies to everyone involved in managing and using stat 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 mandates:

- **Incident Response Training:** Regular training for all system users.
- **Incident Response Testing:** Annual testing of incident response capabilities.
- **Incident Handling:** Procedures for handling incidents, including preparation, detection, analysis, containment, eradication, and recovery.
- **Incident Monitoring, Reporting, and Response:** Continuous monitoring, prompt reporting, and appropriate response to incidents.
- **Incident Response Plan:** Development, maintenance, and annual review of a comprehensive IRP.
- **Incident Response Assistance:** Provision of support resources for incident handling and reporting.

Remember:

- **Report Concerns:** Voice your concerns and report any potential security risks or incidents within one hour of knowledge of the event to your ISO or CIO.
- **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.

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