ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8120 Information Security Program

What?

This policy establishes the State's Information Security Program. It provides a framework for each BU to follow; protecting all state agency information systems and data.

When?

This policy applies at all times when handling agency information systems and data. This includes:

- **Designing and implementing new systems**
- **Developing and using systems**.
- **Assessing risks**
- **Responding to incidents**

Why?

- **Legal Compliance:** Arizona law (A.R.S. § 41-4254 and § 41-4282) requires state agencies to have a strong information security program.
- **Risk Management:** This policy helps agencies identify and address potential security risks before they cause problems.
- **Data Protection:** The main goal is to protect sensitive State information from unauthorized access, use, disclosure, disruption, modification, or destruction

Who?

This policy applies to anyone who handles state data.

How?

This policy requires agencies to:

- **Categorize Systems:** Determine the sensitivity of information systems (e.g., Standard or Protected).
- **Develop and Implement Security Controls:** Ensure the agency is utilizing secure development practices by putting measures in place to protect systems and data (e.g., access controls, encryption, vulnerability scanning).
- **Conduct Risk Assessments:** Regularly evaluate and update security measures to identify potential threats and vulnerabilities.
- **Create Security Plans:** Document how each system will be secured.
- **Perform Control Assessments:** Test the effectiveness of security controls by conducting an annual penetration test**.
- **Continuously Monitor Systems:** Leverage monitoring tools, such as *Crowdstrike* and *Tanium*, to identify and remediate threats or vulnerabilities.
- **Respond to Incidents:** Have a response plan in place to respond to and mitigate security breaches.

Remember:

- **Annual SSPs:** Please be sure to submit these to AZDOHS no later than *June 30* each year, for all agency systems.
- **Prioritize Security:** Is your agency using the tools provided by the Enterprise Security Program?
- **Report Concerns:** Voice your concerns and report any potential security risks to your ISO or CIO.

***Note: this can be conducted by the National Guard*

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