ARIZONA DEPARTMENT OF HOMELAND SECURITY

Statewide Policy: 8230 Contingency Planning

What?

This policy requires all state agencies to have a plan in place in the event something happens that disrupts their technology systems. This includes things like natural disasters, cyberattacks, or power outages. The plan must outline how the agency will keep operating or get back up and running quickly.

When?

This policy is in effect all the time and covers a wide range of situations, from minor disruptions to major disasters. It focuses on making sure essential services can continue even if technology systems are down.

Why?

- **Minimize Downtime:** Reduce the amount of time that systems and services are unavailable.
- **Protect Essential Functions:** Ensure that critical services provided by state agencies are not severely impacted during an emergency, such as an information system disruption, compromise, or failure.
- **Preserve Data:** Protect important information and ensure it can be recovered.
- **Meet Legal Requirements:** Comply with state and federal laws related to data protection and disaster recovery.

Who?

This policy applies to all state agencies and everyone involved in maintaining and operating their technology systems. Specific roles and responsibilities are defined for different individuals and teams.

How?

Agencies must:

- **Identify Critical Functions:** Determine which systems and services are absolutely essential.
- **Develop a Contingency Plan:** Create a detailed plan that outlines how to respond to various disruptions. This includes:
  - Backup and recovery procedures
  - Alternate processing and storage sites
  - Emergency communication plans
- **Train Staff:** Ensure everyone knows their role in the plan.
- **Test the Plan:** Regularly test the plan to make sure it works and is up-to-date.
- **Coordinate with Others:** Work with other agencies and organizations as needed.

Remember:

- The policy emphasizes having alternate locations and backup systems ready to go.
- Agencies must prioritize their services to ensure the most important ones are restored first.
- Strong security measures must be in place to protect data at all times.

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