Statewide Policy: 8110 Data Classification

What?

This policy outlines the State's framework for classifying data. Data classification categorizes information based on its sensitivity and the potential impact of unauthorized access, modification, or destruction.

When?

This policy applies **whenever** you are creating, storing, processing, or transmitting data on agency systems. This includes:

Determining the data classification: Is the data Confidential or Public?

Handling data: Storing, accessing, transporting, and disposing of data.

Developing or procuring systems and apps: Ensuring that systems and applications handle data according to this policy.

Making decisions about data security: This policy provides the framework for making informed decisions about data security.

Why?

Legal Compliance: A.R.S. § 41-4254 and § 41-4282 mandate the protection of state information. This policy fulfills that requirement.

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**.

Risk Management: Classifying data allows the agency to apply appropriate security controls based on the sensitivity of the information.

Data Protection: This policy ultimately aims to protect the State's confidential data.

Who?

Any personnel who handle confidential information.

Remember:

Assume Confidential: If data doesn't have a clear classification, treat it as Confidential.

Need-to-Know: Only authorized individuals with a legitimate need can access Confidential Data.

Secure Handling: Confidential Data must be protected at all times, including during transport and when unattended.

Encryption: Encrypt Confidential Data when transmitting it externally.

How?

Data is classified into two categories:

Confidential Data is data that contains information that is sensitive in nature and can include but is not limited to the following:

- System Security Parameters and Vulnerabilities
- Health Information
- Financial Account Data
- Criminal Justice Information
- Critical Infrastructure/Fuel Facility Reports
- Eligible Persons
- Risk Assessment and State Audit Records
- Personal Identifying Information
- Other records protected by law

Public data* is data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

Note: An AZRAMP Low Impact authorization is the minimum requirement for public data transfers out of State control.

Effective: January 16, 2024