Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P2000

P2045 – RISK MANAGEMENT PROGRAM

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-831 through § 67-833

II. ABSTRACT

This policy requires state agencies to adopt a risk management program strategy to manage risks to the State of Idaho that result from threats to the confidentiality, integrity and availability of agency data and information systems.

III. DEFINITIONS

See ITA Guideline G105 (Glossary of Terms) for any definitions.

IV. POLICY

This policy applies to all electronic data created, stored, processed, or transmitted by State agencies, and the information systems used with that data.

All agencies must have and maintain a Risk Management Program which requires agencies complete risk and security assessments of their critical systems and infrastructure and that ongoing processes are in place to assess the current posture of the environment.

The Risk Management Program is designed as a three-year cyclic program. To be completed in the order decided upon by the agency. Agencies must:

- complete an independent third-party risk assessment to include a vulnerability assessment and penetration test.
- complete a policy and procedure audit.
- conduct internal risk assessments.

It is the agency's responsibility to ensure that an appropriate budget amount is requested. ITS-CISO is available to conduct "staff assistance" visits at agency's request to help prepare for and/or remediate after the assessments and audits.

Within 30 days of receiving the findings of the assessment, all agencies are required to create a Corrective Action Plan (CAP) to track and remediate their findings. This will be used to track those deficiencies noted during the current cyclical period, and will ensure:

1. Accurate reporting on the status of corrective actions.
2. Development of a process to evaluate supporting documentation and the time to monitor recommendations.
3. Residual risks may only be accepted on behalf of the agency by a person with the appropriate level of authority as determined by the agency Administrator or Director.
4. Agencies may, as appropriate, coordinate with the ITS-CISO to address residual risks for those controls that cannot be implemented.

Date of assessments should be included with the agency's annual IT security plan.

V. EXEMPTION PROCESS

Refer to ITA Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

VI. PROCEDURE REFERENCE

Guidelines for Risk Assessment are detailed in ITA Guidelines: G210 (IT Project Profile) and G215 (Risk Assessment).

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

Date established: July 7, 2023