STATE *of* MISSOURI
ADMINISTRATIVE POLICY

POLICY: SP-18

POLICY TITLE: Electronic Data Security Training

ISSUED: July 15, 2025

AUTHORIZED BY: Kenneth J. Zellers, Commissioner

I. Purpose

The purpose of this policy is to ensure that individuals authorized to access electronic data of the State of Missouri's consolidated executive branch agencies receive training regarding data security and handling data appropriately based on the nature of the data.

II. Applicability

This policy applies to all employees, contractors, consultants, volunteers, and others authorized to access electronic data of the agencies ("employees"). "Agencies" are the consolidated executive branch agencies for which the Office of Administration's Information Technology Services Division (ITSD) provides information technology services.

III. Requirements

A. Agency employees shall receive all training required by this policy.

B. ITSD shall provide the following for all agencies:
1. Monthly security awareness training to all employees.
2. Role-based security training to employees whose work involves cybersecurity operations and infrastructure.
3. Core security awareness training for new employees.

C. Where appropriate, ITSD shall also provide role-based security training to employees in the areas of application development, systems administration, network operations, and cloud operations.

D. Each agency shall:
1. Ensure that its employees complete the monthly security awareness training provided by ITSD as referenced above. Employees who do not complete this training in a timely manner may have their access to information technology resources removed by ITSD until training is complete.
2. Ensure that new employees complete core security awareness training provided by ITSD as a part of the onboarding process for new employees.

3. Provide additional specific security training required by each Employee's role, applicable contracts, applicable law, and when necessary due to information system changes.
4. Provide training regarding physical security. Examples include requiring employees to use badges and requiring visitors to sign in before accessing secured areas.

IV. Practical Exercises

ITSD may provide practical exercises in security training that reinforce training objectives. Practical exercises may include simulated cyberattacks exploiting common vulnerabilities such as phishing, social engineering and attacks targeted at senior leaders.

V. Security Training Records

Security training records will be maintained, and reporting will be made available to the agencies, using an appropriate method as determined by ITSD.