Georgia Department of Public Safety

Policy Manual

SUBJECT **INFORMATION SECURITY AWARENESS & TRAINING**	POLICY NUMBER **26.02**
DISTRIBUTION **ALL EMPLOYEES**	REVISED DATE **11/20/2023**
	POLICY REVIEWED **11/20/2023**

26.02.1 Purpose

To ensure that the appropriate level of information security awareness training is provided to all Information Technology (IT) users.

26.02.2 Policy

This policy is applicable to all Georgia Department of Public Safety members and users of DPS IT resources and assets.

A. Information Security Awareness Training

The Department shall:

1. Schedule information security awareness training as part of initial training for new users. This training should be completed within 30 days of hire date.

2. Schedule information security awareness training when required by information system changes and then at least every six months thereafter.

3. IT shall determine the appropriate content of information security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

    a. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

    b. Address awareness of the need for operations security. Information security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

B. Information Security Awareness – Inside Threat

The Technology Section shall:

Include information security awareness training on recognizing and reporting potential indicators of an insider threat.

C. Role-Based Security Training

1. Provide role-based security training to personnel with assigned security roles and responsibilities:

    a. Before authorizing access to the information system or performing assigned duties.

    b. When required by information system changes and annually thereafter.

2. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

D. Physical Security Controls

The Technology Section shall:

1. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

2. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

E. Practical Exercises

The Technology Section shall:

Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (*e.g.,* buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

F. Suspicious Communications and Anomalous System Behavior

The Technology Section shall:

Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

G. Security Training – User Training

All users of DPS technology shall:

1. Take information security awareness training as part of initial training for new users within 30 days, and then at least every six months thereafter.

    Any user who is on extended or military leave and does not utilize any network resources during such leave, including agency email, is excused from training for the duration of the leave. However, any current assignment that is in process at the time of the user's return, shall be taken before its due date.

2. Take any role-based training is needed for certain security roles, when assigned.

3. Retain individual training records for three years (including the current year).

H. Security Training Records

The Department shall:

1. Designate personnel to document and monitor individual information system security training activities including basic information security awareness training and specific information system security training.

2. Retain individual training records for three years (including the current year).

I. Compliance

Employees who violate this policy may be subject to appropriate disciplinary action, up to and including termination, as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.