

Security Awareness Training Policy

1. Overview

Exposure to sensitive business information or personal customer details can severely damage the County. County devices and the county network are also at risk from ransomware and malware attacks, which can prove to be costly. To prevent breaches of data, infection of county devices, or intrusion of the county network, all employees, contractors, and other users of the county network and devices must be trained in the necessary measures to maintain security.

2. Purpose

The purpose of this policy is to set out why all networks and devices need end users within the County to take up security awareness training and to clearly outline employees' expectations to engage in their security awareness training. This policy will ensure that employees know what is expected of them and that the County can take necessary measures to uphold compliance with its data protection regulatory requirements.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties, who have access to the County's private or personal data, the County's network, or devices owned or controlled by the County.

4. Policy

All county employees must be aware of their responsibilities in protecting the County's data, devices, and network.

The County will provide security awareness training to all employees before and during their use of the county network and County devices. All new employees will receive a gap analysis questionnaire that will gauge their current knowledge of security areas. Employees will then be trained by individualized programs that will address their weakest areas first.

All security awareness training will be sent out periodically, in the form of online security awareness training courses. These courses will be sent out by email and accessed from the county email inbox.

Employees are expected to complete all security awareness training courses received by them within at most 20 working days.

The security awareness training will educate employees on the risks of, or best practices regarding the use of, the following core information security areas:

- Email and internet use
- Phishing
- Social engineering
- Malware

- Adware and spyware
- Ransomware
- Working remotely
- Physical security
- Cloud security
- Passwords and authentication
- Social media use
- Voice- and text-based phishing

5. Compliance

5.1 Compliance Measurement

TSD will verify compliance with this policy through any methods deemed appropriate, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

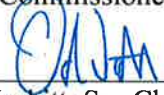
Any exceptions to this policy must be approved by TSD Director or Deputy Director only in advance and have a written record.

5.3. Non-Compliance

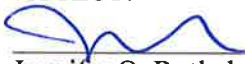
Any employee who violates this policy may be subject to disciplinary action, including termination of employment.

Approved this 9 Day of may

Rockdale County, Georgia
Board of Commissioners


Osborn Nesbitt, Sr., Chairman

ATTEST:


Jennifer O. Rutledge, County Clerk
Executive Director, Government Affairs/County Clerk

Approved as to form:


M. Qader A. Baig, County Attorney