| | Policy Title<br>IT: Workstation and Mobile Device Policy | | |
|---|---|---|---|
| | **Control Number**<br>SC009.1 | **Policy Date**<br>03/04/2024 | **Revision Date**<br>05/06/2025 |

## Purpose

The purpose of this policy is to outline the workstation and mobile device equipment at Scotland County. These rules are in place to protect the employee and Scotland County. Inappropriate use exposes Scotland County to risks including virus attacks, compromise of network systems and services, and legal issues.

## Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Scotland County business or interact with internal networks and business systems, whether owned or leased by Scotland County, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Scotland County and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Scotland County policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Scotland County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Scotland County.

## Overview

This policy states the requirements for securing workstations or mobile devices that will access resources on any of Scotland County networks and/or store Scotland County information. Scotland County will implement physical and technical safeguards for all workstations and mobile devices that access sensitive information to restrict access to authorized users.

## Policy Requirements

### Workstation & Mobile Device

- Users must immediately report all lost or stolen Workstations/Mobile devices to Scotland County management and they will notify VC3 immediately.
- Installation of software from untrusted sources is forbidden. If you are unsure if an application is from an approved source, contact VC3 for guidance.
- Mobile devices must not be “Jailbroken” or have any software/firmware installed, which is designed to gain access to functionality not intended to be exposed to the user.
- Scotland County reserves the right to install mobile device management software on any mobile device covered by this policy.

- Only Scotland County purchased and IT approved equipment shall be used regularly. Personal equipment may not be used including computers, tablets, keyboards, monitors, mouse. See “Smartphones” for personal phone use.
- Only Scotland County approved software may be installed on Workstations/Mobile devices owned or leased by Scotland County.
- Workstations/Mobile devices must only be used by authorized personnel.
- Workstations/Mobile devices must have Anti-Virus/Anti-Spyware and Endpoint Detection/Response software installed.
- All Workstations/Mobile devices must have the latest security patches installed.
- If available, all Workstations/Mobile devices must have a password-protected screen saver enabled or automatically lock within no more than 15 minutes of inactivity.
- Workstations/Mobile device users must not use the save password feature for any applications that provide access to sensitive information.
- Scotland County reserves the right to periodically inspect Workstations/Mobile devices for compliance to IT policies.
- When employees are required to store PII, PHI or partner/client credentials on Workstations/Mobile devices during the course of their legitimate job responsibilities, this information must be encrypted. All information on mobile devices must be encrypted.
- Mobile computing equipment carrying important, confidential information must not be left unattended in public and if possible, should be physically locked away. Users must take care that data cannot be read by unauthorized persons.
- Special care must be taken when mobile computing equipment is placed in vehicles, public spaces, hotel rooms, meeting places, conference centers and other unprotected areas outside the organization’s premises.
- Each Scotland County Employee accessing the Scotland County network resources/applications shall maintain a personal cellular telephone which will be equipped with an multifactor authentication application to enable access to the Scotland County network resources/applications.

**Smartphones**

- Employees may use their personal smartphones for limited Scotland County work such as email and Teams. Once a personal smartphone is configured to access Scotland County’s

email/chat applications this MAY allow the ability for FOIA (Freedom of Information Act) requests to have access to your personal smartphones as part of their requests.

- Personal smartphones MUST have the following security configurations: Passcode enabled, Full-disk encryption and the device CANNOT be jailbroken or rooted.

## Compliance

The Management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the County Manager, the IT Services provider and/or IT Personnel in advance.

## Disciplinary Action

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Reference

Replaces: IT: Acceptable Use Policy SC009 dated 5/6/2024