	Policy Title IT: Acceptable Use Policy		
	Control Number SC005.2	**Policy Date** 05/06/2024	**Revision Date** 5/5/2025

Purpose

The purpose of this policy is to outline the acceptable use of computer 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.
- Any individual with Scotland County network access (governing board members, employees, contractors, consultants, temporary staff, 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 all equipment that is owned or leased by Scotland County.

Overview

- Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Scotland County's established culture of openness, trust and integrity. Management is committed to protecting Scotland County 's employees, partners and the County from illegal or damaging actions by individuals, either knowingly or unknowingly.
- Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP (File Transfer Protocol), are the property of Scotland County.
- These systems are to be used for business purposes in serving the interests of the County, and of our clients and customers in the course of normal operations.
- Effective security is a team effort involving the participation and support of every Scotland County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.
- Scotland County's systems shall not be used as a forum to promote religious or political causes, or any illegal activity.
- Likewise, offensive or improper messages or opinions, transmission of sexually explicit images, messages, cartoons or other such items, or messages that may be construed as harassment or disparagement of others based on race, color, age, national origin, religion, sexual orientation, gender identity, veteran, disability, or any other status protected under applicable international, federal, state, and/or local law are also prohibited on Scotland County systems.

General Use and Ownership

- Scotland County proprietary information stored on electronic and computing devices whether owned or leased by Scotland County, the employee or a third party, remains the sole property of Scotland County. You must ensure through legal or technical means that proprietary information is protected in accordance with data protection standards.*
- All devices capable of connecting to the Scotland County network are included under this policy. You have a responsibility to immediately report the theft, loss or unauthorized disclosure of Scotland County proprietary information.
- You may access, use or share Scotland County proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Scotland County may monitor equipment, systems and network traffic at any time.
- There is no guarantee of privacy while using Scotland County's infrastructure. Information created or stored on Scotland County equipment is considered the intellectual property of Scotland County.

Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with current OS (Operating System) patching and Antivirus/Anti-Malware software installed.
- System level and user level passwords must comply with Scotland County password policies. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

- Postings by employees from a Scotland County email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Scotland County, unless posting is in the course of business duties.

- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

- Once an employee is no longer employed with Scotland County, Human Resources will notify IT to remove the employee from all systems.

Unacceptable Use

Any questions may be addressed to the Management.

The following activities are, in general, prohibited.

- Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Under no circumstances is an employee of Scotland County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Scotland County-owned resources.

- The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Viewing, downloading, saving inappropriate or offensive material including, but not limited to, pornographic material as defined in G.S. 14-190.13, which includes pictures, drawings, video recordings, films or other visual depictions or representations, digital or computer-generated visual depictions or representations created, adapted, or modified by technological means, such as algorithms or artificial intelligence. (NC GS 143-805) Exception only exist when:
    - investigating or prosecuting crimes, offering or participating in law enforcement training, or performing actions related to other law enforcement purposes;
    - identifying potential security or cybersecurity threats;
    - protecting human life;
    - establishing, testing, and maintaining firewalls, protocols, and otherwise implementing G.S. 143-805;
    - participating in judicial or quasi-judicial proceedings.

- Violations of the rights of any person or County protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Scotland County.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Scotland County or the end user does not have an active license is strictly prohibited.

- Accessing data, a server or an account for any purpose other than conducting Scotland County business, even if you have authorized access, is prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Your supervisor should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Using a Scotland County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any Scotland County account.

- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to Management is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Scotland County network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Scotland County employees to parties outside Scotland County that are not business related.

Email and Communication Activities

When using County resources to access and use the Internet, users must realize they represent the County. Whenever employees state an affiliation to the County, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the County".

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Scotland County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Scotland County or connected via Scotland County's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

- Social Media refers to communication tools and resources similar to, but not all-inclusive, Facebook, Twitter, YouTube, Flickr, LinkedIn, Google+, Instagram, Alignable, or others as they evolve.

- The County's primary means of internet communication is through our Scotland County Website, Scotland County Facebook page, and the Scotland County Twitter page. Individual Departments may request specific social media tools as part of their strategic communications to targeted populations.

- Information of Scotland County Government business will be managed by the Public Information Officer (PIO) and released by the PIO via the County's social media outlets.

- Reference the Scotland County Social Media Policy for detailed information on appropriate and inappropriate use as it relates to social media.

Data Identification and Classification

- Data classifications will be defined based on the sensitivity, criticality, and value of the information. When information of various classifications is combined, the resulting collection of data or new data must be classified at the most restrictive level among the sources.

- All data must be classified into one of four sensitivity levels, which are referred to as Restricted/Proprietary, Confidential, Sensitive and Public.

- All Scotland County data is to be reviewed on a periodic basis and classified according to its use, sensitivity, and importance to Scotland County and in compliance with federal and/or state laws.

LEVEL I: RESTRICTED/PROPRIETARY

- Restricted/Proprietary information is information of a strategic and proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only.

LEVEL II: CONFIDENTIAL

- Confidential information is information whose unauthorized disclosure, compromise or destruction would result in severe damage to Scotland County, its customers, or employees (e.g., social security numbers, dates of birth, medical records, credit card or bank account information). Level 2 data is intended solely for use within Scotland County and is limited to those with a "business need-to-know."

LEVEL III: SENSITIVE

- Sensitive Information must be guarded due to ethical or privacy considerations. Unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to Scotland County's reputation, or violate an individual's privacy rights. This includes information confined for use only within purposes related to its business.

LEVEL IV: PUBLIC

- Public information is information that is not publicly disseminated, but accessible to the public. These data values are either explicitly defined as public information, intended to be readily available to individuals, or not specifically classified elsewhere in the protected data classification standard.

- Knowledge of Level IV information does not expose Scotland County to financial or reputational loss or jeopardize the security of Scotland County data. Publicly available data may be subject to appropriate review or disclosure procedures to mitigate potential risks of inappropriate disclosure data in order to organize it according to its risk of loss or harm from disclosure.

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. In the event of a violation of the law, law enforcement will be contacted.

Reference

Replaces: IT: Acceptable Use Policy, Date 5/2024