Title: Systems and Data Security	Policy: CP 005
Section: Corporate	

ACCOUNTABILITY TO VISION STATEMENT

Security is vital for protecting the integrity of Flagstaff County's data systems and mitigating risks associated with their misuse. Cybersecurity is fundamental for safeguarding intellectual property and devices, ensuring efficient community support. Flagstaff County is committed to managing information, systems, and devices with the highest priority.

POLICY STATEMENT

This policy establishes standards and responsibilities aimed at eliminating and preventing cyber risks. All data created or stored on Flagstaff County electronic devices is the property of Flagstaff County. Security measures will be implemented to maintain confidentiality, integrity, and availability of this data. The County will only utilize software in compliance with licensed agreements; unlicensed software installation is strictly prohibited.

DEFINITIONS

Electronic Devices - All technical resources owned or leased by Flagstaff County, including phones, computers, software, and services used for County business.

Information - Data managed, analyzed, or communicated for the purpose of serving Flagstaff County.

Information Systems – Integrated components for collecting, storing, processing data, and providing information and digital products.

IT – Information Technology, encompassing all aspects of data management and processing.

MSP – Managed Service Provider

Users – All employees, elected officials, volunteers, or contractors authorized to access County resources.

IMPLEMENTATION

This policy applies to all individuals working for, reporting to, or providing services to Flagstaff County. Adherence to safe internet and technology practices is mandatory.

GUIDELINES

1. **Device Use:** County-provided electronic systems must be used ethically and lawfully. Users must report lost or stolen devices to IT immediately.
2. **Monitoring:** The County reserves the right to monitor and log network activity without notice. Users should have no expectation of privacy.

3. **Personal Use:** Incidental personal use is allowed outside normal working hours, provided it incurs no additional costs and adheres to this policy. Personal use for gain or illegal activities is strictly prohibited.

GUIDELINES continued

SECURITY MEASURES

- **Patching:** Regular updates of operating systems and third-party applications to maintain security and functionality. Patches are deployed during off-peak hours with prior backups.
- **Passwords:** Users must create strong passwords to protect data access. Password management is essential to prevent unauthorized access.
- **Mobile and Remote Access:** Access to the network is restricted to approved devices registered with IT. All devices must have secure passwords, and remote access must use a secure, encrypted connection.

INFORMATION SECURITY

- **Training:** All employees must complete security awareness training upon hiring and annually thereafter.
- **Data Classification:** Information should be classified by sensitivity, with restricted access based on security credentials.
- **Facility Access:** Access to areas with sensitive information is limited to authorized personnel.
- **Security Measures:** Security cameras, alarms, and other protective measures must be installed and tested regularly.
- **Software Protection:** Antivirus and antimalware software must be installed and updated regularly.
- **Password Management:** Strong password practices and multi-factor authentication are mandatory and regularly reviewed.
- **Data Backup:** All data must be backed up regularly, encrypted, and securely stored, with recovery tests conducted periodically.
- **Third-Party Compliance:** All third parties with access to the County's data must adhere to this policy.

Council Approved: November 20, 2024	**Resolution #:** FC20241120.1017
Reference: Municipal Government Act	**Signature:**

Review Cycle:	**Next Review Year:** 2027
Every three (3) years	