INFORMATION TECHNOLOGY POLICY

Date Adopted: (Insert Date)

Purpose:

The purpose of this comprehensive Information Technology (IT) policy of the DeSoto County Board of County Commissioners is to ensure consistent direction, oversight, and governance of the County's technology environment. These policies define the Board's expectations for the responsible and secure use of technology resources and establish the framework for how technology is selected, managed, and safeguarded across all departments.

By clearly articulating standards for acceptable use, procurement, access, data security, and system management, these policies help protect the County's digital assets, maintain operational integrity, and reduce risks associated with unauthorized use, data loss, and cybersecurity threats. They also guide decision-making, support compliance with legal and regulatory requirements, and reinforce the County's commitment to transparency, accountability, and continuous improvement in the use of information technology.

General Authority:

All County technology systems, devices, and data are under the governance of the DeSoto County Board of County Commissioners and are managed through the centralized oversight of the Information Technology (IT) Department. This authority extends to:

1. All departments, offices, and entities operating under the Board of County Commissioners.
2. All County employees, elected officials, contractors, third-party service providers, or authorized users who access or use County technology resources.
3. All IT-related procurement, licensing, installations, access controls, configurations, and maintenance activities.
4. Enforcement of security standards, software compliance, system compatibility, and data protection.

Department Directors are responsible for coordinating technology-related needs with the IT Department and must ensure compliance with this policy. The County Administrator retains final approval authority for specific items, including mobile communication devices, delegated exceptions, or issues elevated for executive review.

Definitions:

- **Authorized User**: Any County employee, contractor, or third-party service provider granted access to County technology systems under the direction of the Board of County Commissioners or the County Administrator.
- **BYOD (Bring Your Own Device)**: A personally owned mobile device (e.g., smartphone, tablet, or laptop) used to perform work-related functions under limited conditions and with IT Department approval.
- **Cloud Computing**: A model for delivering computing services (e.g., servers, storage, databases, networking, software) over the internet to enable faster innovation and flexible resources.
- **Computer Peripherals**: Devices that attach to a computer to enhance its functionality, such as printers, scanners, webcams, and audio devices.
- **Computer Systems**: Includes all physical and virtual machines used for data processing and communication, including desktops, laptops, and servers managed by the County.
- **Continuity of Operations**: The capability to continue essential functions and services across a wide range of potential emergencies or operational interruptions.
- **Disaster Recovery**: A set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
- **Domain**: The County's officially registered internet domain used for email, website, and online service hosting.
- **Electronic Funds Transfer (EFT)**: The electronic transfer of money from one account to another, either within a single financial institution or across multiple institutions.
- **Encryption**: The process of converting data into a coded format to prevent unauthorized access.
- **External Hardware**: Any physical component that connects to a computer system to provide input, output, or auxiliary support. Examples include monitors, keyboards, mice, external drives, signature pads, and card readers.
- **Firewall**: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Internal Hardware**: Any physical component which makes up the internal functions of a computer system. This includes, but is not limited to, motherboards, hard drives, RAM, processors, and power supplies.

- **Information Security**: The practice of defending information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Patch Management**: The process of managing updates to software and systems to address security vulnerabilities and improve functionality.
- **Phishing**: A type of cyberattack where malicious actors attempt to trick individuals into providing sensitive information, such as passwords or financial details.
- **Software**: Any licensed, freeware, or open-source program or application intended for use on County-owned systems or for County business purposes.
- **Two-Factor Authentication (2FA)**: An additional layer of security requiring two forms of identification to access systems or data.
- **Virtual Private Network (VPN)**: A secure connection that encrypts data transmitted between a user and a network, often used for remote access.

GOVERNANCE AND ADMINISTRATIVE OVERSIGHT

Policy Statement:

It is the policy of the DeSoto County Board of County Commissioners to ensure that all information technology assets, systems, and services are administered in a manner that promotes efficiency, accountability, and operational continuity. All administrative oversight and documentation of technology infrastructure shall be maintained by the IT Department.

Policy Directives:

1. The IT Department shall maintain an accurate inventory of all technology hardware and software, including licensing information, version numbers, and assigned users or departments.
2. All contracts for IT services, including hardware leases, cloud services, managed services, or maintenance agreements, must be reviewed and cataloged by the IT Department. The IT Department will track expiration and renewal dates and ensure contract compliance.
3. The IT Department shall periodically conduct audits of technology systems and usage. Results will be reported to the County Administrator and Department Directors with recommendations for improvements or corrections.
4. Technical infrastructure, including network maps, system architecture, and standard configurations, shall be documented and maintained. This documentation shall be updated as changes occur.
5. The IT Department shall be involved in all technology-related procurement discussions to ensure compatibility and compliance with existing systems and policies.

COMPUTER SYSTEMS AND HARDWARE

Policy Statement:

All computer systems, hardware, peripherals, and mobile devices shall be selected and procured to ensure uniformity, cost-efficiency, system compatibility, and long-term maintainability. The IT Department shall be the sole authority responsible for evaluating and authorizing such acquisitions in compliance with County policy.

Policy Directives:

1. The IT Department shall maintain and regularly update a list of minimum technical specifications for County computer systems and related equipment. All purchases shall conform to these specifications unless otherwise authorized in writing.
2. All computer hardware, including peripherals and external devices, must be evaluated for compatibility with the County's existing infrastructure. Any requests for non-standard hardware shall include justification and must be reviewed and approved by the IT Department.
3. Mobile devices are limited to employees whose duties require mobile communication. The IT Department will manage replacements and evaluate service issues.
4. No hardware, peripherals, or mobile devices may be purchased, leased, or otherwise acquired using County funds without prior review and written approval by the IT Department or the County Administrator. Unauthorized purchases may be subject to denial of support or return at departmental expense.

SOFTWARE

Policy Statement:

All software installed or used on County-owned systems shall be legally obtained, properly licensed, and approved by the IT Department before acquisition or installation. This ensures compliance, cybersecurity, integrity, and consistency.

Policy Directives:

1. All software must be requested through and approved by the IT Department prior to acquisition, download, or use. This includes freeware, open-source, and cloud-based applications.
2. Only the IT Department is authorized to procure, license, and distribute software on behalf of the County, unless otherwise authorized in writing by the County Administrator or as specified in another provision of this policy.

3. All software licenses shall be registered in the name of the DeSoto County Board of County Commissioners. The use of personal or third-party software on County devices is strictly prohibited.
4. All software installations shall be performed or expressly authorized by the IT Department to ensure compatibility, security, and standardization.
5. The IT Department shall maintain list of preauthorized software permitted for use on County systems. Freeware on the list may be downloaded without additional approval. Preauthorized paid software may be procured by Department Directors, subject to budget availability and notification to the IT Department.
6. Periodic audits will verify licensing compliance. Unauthorized or unlicensed software will be removed immediately.
7. Unauthorized software use may be reported to the appropriate Department Director or County Administrator.
8. All software must be compatible with County systems and meet security standards.

BRING YOUR OWN DEVICE (BYOD)

Policy Statement:

The County permits the limited use of personal devices for County-related business if the devices are preapproved, secured, and compliant with County IT policies.

Policy Directives:

1. Users must document their personal devices with the IT Department and receive authorization before use.
2. Under no circumstances may employees install County owned software on personal devices, (i.e. licensed or subscription software such as Adobe or Microsoft)
3. Devices must meet County security standards and may be subject to configuration requirements.
4. Confidential data must not be stored on personal devices without explicit written approval.
5. The County reserves the right to inspect, monitor, and if needed, remotely remove County data from personal devices.
6. Personal device use does not entitle the owner to reimbursement or technical support.
7. Violation of this policy may result in revocation of BYOD privileges or disciplinary action.

SECURITY AND ACCESS CONTROL

Policy Statement:

To protect the confidentiality, integrity, and availability of its information systems and data all County personnel must adhere to appropriate technical and procedural controls that reduce security risks and prevent unauthorized access, use, or disclosure of County information.

Policy Directives:

1. The IT Department, in collaboration with the County Administrator, shall establish and maintain classifications for County data and ensure appropriate security levels are enforced.
2. Access to County systems shall be granted only to those who require it for official duties. Inactive or unnecessary accounts must be removed promptly.
3. All systems must be equipped with current antivirus, antimalware, and endpoint protection software maintained by the IT Department.
4. Servers and networking equipment must be protected in secure environments.
5. All employees must complete mandatory and annual security awareness training.
6. Security incidents must be reported immediately to the IT Department. Investigation and mitigation will be documented.
7. The IT Department will perform audits and report any significant findings to the County Administrator.

CONTINUITY AND DISASTER RECOVERY

Policy Statement

It is the policy of the DeSoto County Board of County Commissioners to ensure uninterrupted operations through robust backup practices, disaster recovery procedures, and coordinated emergency response. The County shall maintain comprehensive plans to prevent, respond to, and recover from incidents impacting critical IT systems. The County may choose to utilize a 3rd party vendor for this service.

Policy Directives:

1. The IT Department shall maintain an updated disaster recovery plan.
2. Daily backups shall be conducted and stored offsite securely.
3. Backup schedules shall be defined and tested annually. A professional service may be utilized to develop and schedule testing.
4. Recovery procedures will be documented and followed in the event of an incident.

5. Failure of any backup system or process will be reported to the County Administrator immediately, and mitigation will be documented.

This policy shall align with broader County emergency protocols.

WEBSITE AND DIGITAL COMMUNICATIONS

Policy Statement:

All County website content, hosting, and maintenance shall be managed for accessibility, accuracy, branding, and legal compliance.

Policy Directives:

1. The IT Department shall manage domain and hosting renewals.
2. Website content must comply with ADA, branding standards, and be reviewed regularly.
3. Only authorized personnel may modify the website.
4. All website data shall meet public records requirements.
5. Use of social media, blogs, and digital engagement tools or platforms shall comply with public records laws.
6. Data collected online shall follow legal privacy standards.
7. All digital content shall comply with branding guidelines.

CYBERCECURITY

Policy Directive:

1. The IT Department, in collaboration with the County Administrator, shall establish a cybersecurity plan that conforms to Section 282.3185, F.S.