BURNET COUNTY TECHNOLOGY AND CYBERSECURITY POLICY

1. PURPOSE AND POLICY

The purpose of this policy is to establish minimum security, management, and operational requirements for endpoint computing devices owned, leased, or managed by Burnet County. Burnet County shall maintain a secure, standardized, and centrally managed endpoint computing environment designed to:

1. Protect County information and technology resources;
2. Reduce cybersecurity vulnerabilities and operational risk;
3. Protect confidential, sensitive, and legally protected information;
4. Maintain reliable and secure County operations;
5. Provide accountability for County technology assets;
6. Support secure remote access and business continuity; and
7. Comply with applicable law and County policies.

County endpoint devices shall be acquired through approved County purchasing processes, configured and managed in accordance with DoTC standards, protected by appropriate cybersecurity controls, maintained throughout their useful life, and securely retired when no longer needed.

2. AUTHORITY, ADMINISTRATION, AND EXCEPTIONS

2.1 Authority

This policy is issued under the authority of the Burnet County Commissioners Court and administered by the Department of Technology and Cybersecurity (DoTC). DoTC is responsible for establishing and maintaining technical standards reasonably necessary to implement this policy and protect County technology resources. If a departmental procedure conflicts with this policy or an applicable DoTC technical standard, this policy shall govern unless an exception has been approved as provided below. Nothing in this policy supersedes applicable federal or state law. If this policy conflicts with applicable law, the law controls.

2.2 Elected Officials

The Commissioners Court recognizes that Burnet County elected officials have independent duties and responsibilities established by the Texas Constitution and state law. This policy is not intended to prevent an elected official from performing a duty imposed by law. If an elected official determines that application of this policy or a decision made by DoTC under this policy interferes with the performance of the official's legal duties, the official may request an exception or appeal the DoTC decision to the Commissioners Court.

2.3 Exceptions

Exceptions to this policy or DoTC technical standards should be based on a documented operational, legal, or business need. DoTC may require reasonable alternative or compensating security controls as a condition of an exception. Nothing in this section limits the authority of the Commissioners Court to approve an exception or otherwise act within its lawful authority.

3. SCOPE

This policy applies to County-owned, County-leased, and County-managed endpoint computing devices, regardless of physical location.

Covered devices include:

- Desktop and laptop computers;
- Rugged and mobile computers;
- Tablets and mobile workstations;
- Public kiosks and computers;
- Shared workstations;
- Specialized public-safety computing devices; and
- Other endpoint devices capable of accessing County information systems.

This policy applies to all persons authorized to use covered devices or access County information systems through them, including employees, elected officials, contractors, consultants, volunteers, and authorized third parties.

4. DEFINITIONS

Authorized User – A person authorized to access Burnet County information systems or use County technology resources.

County Information Systems – Any technology system, application, platform, network, infrastructure, device, database, or service that is owned, operated, managed, contracted, or otherwise authorized by the County for the purpose of processing, storing, transmitting, accessing, or managing County information or supporting County operations. This includes, but is not limited to, servers, networks, cloud services, enterprise applications, databases, endpoints, telecommunications systems, security systems, and related technology resources.

Endpoint Computing Device or Endpoint – A computing device capable of accessing County information systems or networks, including desktops, laptops, tablets, kiosks, mobile workstations, and specialized computing equipment.

Endpoint Detection and Response (EDR) – Technology used to monitor endpoint activity and detect, investigate, and respond to cybersecurity threats.

Least Privilege – Limiting a user's or system's access and permissions to those reasonably necessary to perform authorized functions.

Management Agents – Authorized software component, service, or system process installed on or associated with a County technology asset that enables the Technology Department to remotely monitor, manage, configure, secure, inventory, update, or otherwise administer the asset.

Multi-Factor Authentication (MFA) – Authentication requiring two or more independent verification factors.

Sensitive Information – Information classified by law, regulation, contract, or County policy as confidential, restricted, or otherwise protected from unauthorized access or disclosure.

DoTC – The Burnet County Department of Technology and Cybersecurity.

5. ROLES AND RESPONSIBILITIES

5.1 Department of Technology and Cybersecurity

DoTC is responsible for the security and centralized management of County endpoint computing systems within its authority. Responsibilities include:

- Establishing and maintaining endpoint security and configuration standards;
- Reviewing and approving endpoint hardware and software;

- Deploying and configuring endpoint devices;
- Maintaining standard configurations and security baselines;
- Managing centralized endpoint-management systems;
- Deploying security patches and software updates;
- Managing EDR, anti-malware, encryption, and other endpoint-security technologies;
- Monitoring endpoint security and performing vulnerability management;
- Maintaining technology asset information;
- Providing technical support;
- Coordinating endpoint-related cybersecurity incident response; and
- Securely sanitizing endpoint equipment before disposal or reuse.

5.2 Department Heads and Supervisors

Department Heads and supervisors are responsible for supporting compliance with this policy within their respective areas of responsibility. They shall, as applicable:

- Ensure personnel appropriately safeguard County equipment;
- Notify DoTC promptly of staffing or responsibility changes affecting system access or assigned equipment;
- Report lost, stolen, or damaged equipment;
- Report suspected cybersecurity incidents and material policy violations;
- Support County technology inventory verification;
- Ensure personnel complete required cybersecurity awareness training; and
- Consult DoTC before acquiring endpoint hardware or software when required by County purchasing procedures.

Technology purchases must comply with the County's purchasing policies and applicable law.

5.3 Authorized Users

Authorized users shall:

- Use County endpoint devices for authorized County business purposes only;
- Safeguard County equipment and information;
- Protect authentication credentials;
- Lock devices when unattended;
- Comply with required security updates and security controls;
- Immediately report suspected cybersecurity incidents and lost or stolen equipment;

- Refrain from installing unauthorized hardware or software;
- Refrain from disabling, removing, circumventing, or modifying County security controls; and
- Cooperate with authorized security investigations.

5.4 Contractors and Third Parties

Contractors and third parties using County-owned or County-managed endpoints shall comply with this policy. The sponsoring department is responsible for communicating applicable County requirements and coordinating necessary access with DoTC for all contractors and third partes.

6. HARDWARE ACQUISITION AND LIFECYCLE MANAGEMENT

6.1 Approved Hardware

Endpoint devices acquired with County funds shall comply with County purchasing requirements and applicable DoTC technical standards. DoTC shall maintain minimum technical specifications based on security, operational requirements, compatibility, vendor support, reliability, and lifecycle considerations. Consumer-grade or nonstandard endpoint devices require DoTC approval when such approval is required under applicable County purchasing procedures.

6.2 Asset Management

County endpoint devices shall be recorded and tracked in accordance with applicable County asset-management and purchasing requirements. Asset information should include, as applicable:

- County asset identification;
- Manufacturer serial number;
- Assigned department or user;
- Physical location; and
- Relevant inventory information.

County asset tags or identifiers shall not be removed or altered without authorization.

6.3 Lifecycle Management

DoTC shall establish endpoint replacement guidelines considering:

- Manufacturer support;
- Security requirements;
- Operational performance;
- Warranty status;

- Reliability; and
- Cost effectiveness.

Devices that no longer satisfy County security or operational requirements shall be upgraded, replaced, reassigned, or retired as appropriate.

6.4 Disposal and Reuse

Before an endpoint device or storage component is disposed of, transferred outside County control, or repurposed, County information shall be securely removed in accordance with applicable DoTC standards.

7. ENDPOINT CONFIGURATION AND MANAGEMENT

7.1 Standard Configuration

County endpoint devices shall use standardized configurations appropriate to their intended purpose. Standard configurations shall address, as applicable:

- Supported operating systems;
- Security baselines;
- Required applications;
- Endpoint protection;
- Encryption;
- Remote management;
- Security monitoring;
- Browser configuration; and
- Device compliance requirements.

7.2 Centralized Management

County-managed endpoint devices shall be enrolled in approved centralized management systems when technically and operationally appropriate. DoTC may use centralized systems for:

- Device enrollment;
- Configuration management;
- Software deployment;
- Patch management;
- Security monitoring;
- Remote support;

- Inventory reporting; and
- Remote isolation or wiping when supported and appropriate.

Users shall not remove management agents or alter centrally managed configurations without authorization.

7.3 Operating Systems

Endpoint devices shall use vendor-supported operating systems approved by DoTC. Operating systems reaching the end of vendor support shall be upgraded, replaced, or subject to an approved exception before continued production use.

7.4 Security Baselines

DoTC shall establish endpoint device configuration baselines using applicable security requirements and recognized security guidance, which may include:

- Microsoft Security Baselines;
- Center for Internet Security (CIS) Benchmarks;
- National Institute of Standards and Technology (NIST) guidance;
- Criminal Justice Information Services (CJIS) requirements;
- Applicable Texas requirements; and
- County technology standards.

DoTC may modify security baselines as technology, legal requirements, or cybersecurity risks change.

7.5 Device Compliance

DoTC may evaluate device compliance based on factors including:

- Operating-system support and update status;
- Encryption;
- Endpoint protection;
- Firewall status;
- Security updates;
- Device risk; and
- Authentication or identity status.

A device that creates an unacceptable cybersecurity risk may be restricted or isolated from County resources until the risk is remediated.

7.6 Unauthorized Modifications

Unless authorized by DoTC, users shall not modify endpoint hardware, firmware, operating-system security settings, or security controls. This includes unauthorized changes to Basic Input/Output Systems, Unified Extensible Firmware Interface settings, Secure Boot, Trusted Platform Module functionality, storage devices, firmware, endpoint protection, management agents, or other security configurations.

8. IDENTITY AND ACCESS SECURITY

8.1 Access

Access to County information systems shall be based on authorized business or governmental need. Access privileges shall follow the principle of least privilege. User accounts shall ordinarily be uniquely assigned to an individual. Shared accounts may be used only when authorized for a legitimate operational purpose and appropriately controlled.

8.2 Account Provisioning and Changes

DoTC shall establish procedures for creating, modifying, and disabling accounts. Departments shall promptly notify DoTC of circumstances requiring access changes, including:

- New personnel;
- Transfers;
- Position or responsibility changes;
- Extended leave when access modification is appropriate;
- Contractor termination; and
- Employee separation.

8.3 Multi-Factor Authentication

MFA shall be required for systems and services designated by DoTC based on security risk and applicable requirements. MFA shall ordinarily be required for:

- Remote access;
- Administrative or privileged accounts;
- Cloud services containing County information;
- VPN access; and
- Other systems designated by DoTC.

DoTC shall maintain approved authentication methods and may modify those methods as technology and security risks change.

8.4 Passwords

Where passwords are used, they shall comply with current County password standards. Users shall not share passwords or reuse County passwords for personal accounts. DoTC may implement passwordless authentication where appropriate.

8.5 Session Security

Endpoint devices shall automatically lock after a period of inactivity established by DoTC. Users shall manually lock endpoints whenever they leave them unattended.

8.6 Privileged Access

Administrative and other privileged access shall:

- Be limited to legitimate administrative needs;
- Be individually attributable where practicable;
- Use multi-factor authentication, when supported and required;
- Be subject to appropriate logging and monitoring; and
- Be periodically reviewed.

Administrative accounts shall not ordinarily be used for routine email, web browsing, or general productivity activities. Local administrator rights require a documented operational need and appropriate approval.

8.7 Service Accounts

Service accounts shall have documented ownership, be limited to necessary permissions, use appropriately managed credentials, and be periodically reviewed. Service accounts shall not be used as ordinary interactive user accounts unless specifically authorized.

9. ENDPOINT SECURITY AND ENCRYPTION

9.1 Endpoint Protection

County-managed endpoint devices shall employ security controls appropriate to their risks and operational requirements. Controls may include:

- EDR;
- Anti-malware protection;
- Host firewalls;

- Device encryption;
- Application protection;
- Threat intelligence;
- Security monitoring; and
- Tamper protection.

Required endpoint-security controls shall remain enabled and shall not be removed, disabled, circumvented, or modified without authorization.

9.2 Endpoint Detection and Response

Endpoints designated by DoTC shall operate approved EDR technology capable of monitoring and responding to potentially malicious activity. DoTC may use EDR or other security tools to investigate threats, isolate devices, contain malicious activity, and protect County systems.

9.3 Security Monitoring and Isolation

DoTC may centrally monitor endpoint security events for purposes of protecting County systems and information. Relevant events may include malware, suspicious authentication, unauthorized privilege escalation, credential theft, ransomware, unauthorized software, lateral movement, and suspected data exfiltration. DoTC may immediately isolate or restrict an endpoint when reasonably necessary to address a cybersecurity risk.

9.4 Encryption

Sensitive County information shall be encrypted when required by law, County policy, applicable security standards, or DoTC requirements. Encryption shall be used as appropriate for:

- Data stored on endpoint devices;
- Data transmitted across networks;
- Approved remote access; and
- Authorized removable media.

DoTC shall establish approved encryption technologies and cryptographic standards.

9.5 Removable Media

Use of removable media may be restricted based on security risk. When removable media is authorized, DoTC may require encryption, malware scanning, documented business justification, and other safeguards appropriate to the information involved. Sensitive information shall not remain on removable media longer than operationally necessary. Encryption recovery keys shall be maintained using approved County systems.

10. SOFTWARE MANAGEMENT

10.1 Approved Software

Software installed on County endpoints shall be authorized by DoTC or otherwise permitted under DoTC standards and appropriately licensed and acquired in accordance with applicable County purchasing requirements. DoTC may maintain an approved software catalog and software-request process for users to obtain necessary software.

10.2 Software Review

Before approving software, DoTC may evaluate:

- Cybersecurity risk;
- Licensing;
- Compatibility;
- Vendor support;
- Operational need;
- Data handling;
- Regulatory requirements; and
- Integration with County systems.

10.3 Prohibited Software

Unless specifically authorized, users shall not install or use software that creates an unacceptable security, licensing, or operational risk, including:

- Unauthorized remote-access applications;
- Peer-to-peer file-sharing applications;
- Cryptocurrency-mining software;
- Password-cracking or unauthorized security-testing tools;
- Unauthorized network-scanning or packet-capture tools;
- Unauthorized virtualization platforms;
- Pirated or unlicensed software; or
- Software intended to circumvent County security controls.

DoTC may remove unauthorized or unsafe software from County endpoint devices.

10.4 Artificial Intelligence Applications

Artificial intelligence applications may be used only in a manner consistent with applicable law and County requirements governing security, privacy, confidentiality, records, and data governance. Unless expressly authorized, users shall not enter non-public County information into publicly accessible artificial intelligence services, including:

- Confidential or restricted information;
- Personally identifiable information;
- Protected health information;
- Criminal justice information;
- Law-enforcement-sensitive information;
- Attorney-client privileged information; or
- Other information prohibited from public disclosure or external processing.

DoTC may evaluate AI platforms before County adoption to determine whether they satisfy applicable security, legal, contractual, and operational requirements.

10.5 Browser Extensions

Browser extensions shall be limited to those authorized by DoTC. Extensions that bypass security controls or create an unacceptable cybersecurity, privacy, or operational risk are prohibited.

11. PATCH AND VULNERABILITY MANAGEMENT

11.1 Updates

County-managed endpoints shall receive operating-system, application, firmware, driver, and security updates in accordance with DoTC maintenance practices. DoTC may test updates before widespread deployment when operationally appropriate. Critical security updates may be deployed on an expedited basis when warranted by risk.

11.2 Supported Software

Software shall be maintained at vendor-supported versions when reasonably practicable. Unsupported software shall be upgraded, replaced, removed, or operated under an approved exception with appropriate compensating controls.

11.3 Vulnerability Management

DoTC shall periodically assess County-managed endpoint devices for security vulnerabilities. Vulnerabilities shall be prioritized and remediated according to risk, operational impact, and applicable security requirements. Unless DoTC determines that circumstances warrant a different response, remediation objectives are:

Severity	Target Remediation
Critical	As soon as practicable, normally within 7 days
High	Within 15 days
Medium	Within 30 days
Low	During normal maintenance cycles

Operational constraints may require alternative remediation measures or compensating controls.

11.4 End-of-Support Systems

A system or software product that is no longer supported by its vendor shall not remain in production unless continued use is justified by an operational need and the cybersecurity risk is appropriately addressed. Where required by County policy, continued use shall be documented and approved by the appropriate County authority.

12. REMOTE ACCESS AND NETWORK SECURITY

12.1 Remote Access

Remote access to County information resources shall use DoTC-approved secure access methods via a County provided VPN (virtual private network) client. Users shall not establish unauthorized remote-access methods or install unauthorized remote-support software.

12.2 Remote Work

When accessing County resources remotely, users shall:

- Maintain reasonable physical control of County devices;
- Use secure network connections;
- Protect sensitive information from unauthorized viewing or disclosure;
- Lock devices when unattended; and
- Promptly report suspected security incidents.

Public computers shall not be used to access County information systems unless specifically authorized.

12.3 Public and Home Networks

When public wireless networks must be used, users shall use County-approved secure remote-access methods when required by DoTC. Employees working remotely should maintain reasonable security for home networks used by County equipment, including current wireless encryption and strong authentication. Default network-device passwords should be changed before County equipment is connected.

12.4 Network Connectivity

County endpoints shall connect only to authorized County network infrastructure or other networks permitted under DoTC standards. Sensitive County information transmitted over networks shall use approved encrypted communication methods when required.

12.5 Wireless and Network Devices

Users shall not install or connect unauthorized network infrastructure or devices to County systems, including:

- Wireless access points;
- Routers;
- Network switches;
- Cellular gateways;
- Network extenders;
- Internet-of-Things devices; or
- Personal network appliances.

Unauthorized devices may be disconnected when necessary to protect County systems.

12.6 Network Security Controls

DoTC may use network segmentation, firewalls, access controls, or other security mechanisms to reduce cybersecurity risk. Users shall not circumvent or attempt to bypass County network-security controls.

13. EXCEPTIONS, ENFORCEMENT, AND REVIEW

13.1 Security Response

DoTC may take reasonable and proportionate technical action to protect County information systems from an identified cybersecurity risk, including restricting access, isolating an endpoint device, removing unauthorized software, or disconnecting unauthorized equipment. When practicable, DoTC shall coordinate with the affected department or elected official regarding actions that materially affect County operations.

13.2 Policy Violations

Suspected violations of this policy shall be reported to the appropriate Department Head, elected official, DoTC, or other appropriate County authority. Violations may result in restriction or removal of technology access and may be addressed under applicable County personnel policies, contracts, or law.

13.3 Exceptions

Requests for exceptions shall identify the operational, legal, or business need supporting the request. DoTC may approve technical exceptions within its authority and may require compensating security controls.

Matters requiring Commissioners Court approval shall be submitted to the Commissioners Court. An elected official may appeal a DoTC determination to the Commissioners Court when the official determines that the application of this policy interferes with the performance of duties imposed by law.

13.4 Review and Technical Standards

This policy shall be reviewed at least annually and may be revised as necessary to address changes in law, technology, cybersecurity threats, or County operations. DoTC may establish and update technical standards, procedures, approved-product lists, configuration baselines, and implementation guidance necessary to administer this policy without amending this policy, provided those requirements are consistent with applicable law, County purchasing requirements, and authority established by the Commissioners Court.

[Signature page]