# BURNET COUNTY TECHNOLOGY SECURITY AND COMPLIANCE STANDARDS POLICY

Policy Number: TD-2025-001

Effective Date: _____

Last Revised: 2026.06.02

## PURPOSE

The purpose of this policy is to establish minimum technology security, operational, and compliance standards for any system, device, application, or service connected to Burnet County network infrastructure.

This policy is intended to promote cybersecurity, protect public resources, reduce operational risk, support interoperability among county systems, and ensure the availability, integrity, and confidentiality of county information systems.

Nothing in this policy is intended to diminish, supersede, or interfere with the constitutional, statutory, or administrative authority of independently elected officials or their offices. Rather, the policy establishes baseline security and technical standards necessary to protect county-owned network infrastructure and interconnected systems.

## SCOPE

This policy applies to:

County-owned network infrastructure and technology resources.

- Any device, system, application, or service connected to County network infrastructure.
- County employees, contractors, vendors, and third parties authorized to access County technology resources.
- All County departments and offices utilizing County-provided network services.

# POLICY STATEMENT

## 3.1 Network Security and Compliance Standards

To protect County technology resources and public information, all systems connected to County network infrastructure shall comply with applicable security, operational, and technical standards established by the Technology Department.

These standards are intended to:

Reduce cybersecurity risks. • Support network reliability and continuity of operations. • Promote interoperability and compatibility among County systems. • Protect against unauthorized access, malware, ransomware, data loss, and service disruptions. • Align County practices with recognized governmental cybersecurity frameworks and industry best practices.

## 3.2 County Network Infrastructure

The Technology Department is responsible for the administration, maintenance, monitoring, and security of County-owned network infrastructure, including but not limited to network routing, switching, wireless infrastructure, firewalls, internet connectivity, and related security systems.

Departments and elected offices may maintain technology systems necessary to fulfill their statutory responsibilities; however, any system connected to County network infrastructure must comply with established security and technical standards.

## 3.3 Compliance Requirements

Devices and systems connected to County networks shall:

Meet minimum cybersecurity requirements established by the Technology Department. • Maintain current operating system and security updates. • Utilize approved endpoint protection and security controls when applicable. • Participate in vulnerability management or security assessment processes when necessary to protect County infrastructure. • Comply with applicable state and federal regulatory requirements.

Failure to meet minimum security standards may result in restrictions or limitations on network connectivity until identified risks are mitigated.

## 3.4 Third-Party Access

Third-party vendors, contractors, consultants, and service providers requiring access to County network infrastructure must:

Have a documented business purpose. • Receive appropriate authorization. • Utilize least-privilege access principles. • Comply with applicable County security requirements. • Be subject to monitoring and auditing when connected to County systems.

# SECURITY REQUIREMENTS

## 4.1 Device Security Standards

Devices connected to County infrastructure should:

Be properly inventoried or identified. • Maintain supported operating systems and software. • Utilize approved authentication controls. • Implement endpoint security protections. • Be configured in accordance with established security standards.

## 4.2 Network Changes

Changes affecting County network infrastructure shall be coordinated with the Technology Department to evaluate security, operational, and interoperability impacts.

## 4.3 Cybersecurity Incident Reporting

All users shall promptly report suspected cybersecurity incidents, unauthorized access attempts, malware infections, or other technology security concerns to the Technology Department.

## 4.4 Prohibited Activities

The following activities are prohibited when connected to County infrastructure:

Circumventing established security controls. • Introducing unauthorized devices that create significant cybersecurity risk. • Sharing authentication credentials. • Knowingly installing malicious software. • Engaging in activities that threaten the security, integrity, or availability of County systems.

# ROLES AND RESPONSIBILITIES

## 5.1 Technology Department

The Technology Department shall:

- Maintain County network infrastructure.
- Establish and publish security standards.
- Monitor network health and cybersecurity threats.
- Provide guidance regarding compliance requirements.
- Coordinate incident response activities.
- Support cybersecurity awareness and training initiatives.

### 5.2 County Departments and Offices

County departments and independently elected offices shall:

- Support compliance with established security standards for connected systems.
- Coordinate with the Technology Department regarding network connectivity requirements.
- Report technology security incidents and concerns.
- Maintain systems under their control in a secure manner.

### 5.3 Users

All authorized users shall:

- Follow applicable technology and security policies.
- Protect County information resources.
- Complete required cybersecurity training.
- Report suspected security incidents promptly.

## EXCEPTIONS

Exceptions to specific technical standards may be approved when justified by operational, legal, statutory, or business requirements, provided appropriate compensating controls are implemented to manage cybersecurity risk.

## POLICY REVIEW

This policy shall be reviewed annually and updated as necessary to address evolving cybersecurity threats, operational requirements, regulatory changes, and industry best practices.

## CONTACT INFORMATION

Burnet County Technology Department

# APPROVAL

Approved:

---

Burnet County Commissioners Court

Date: _____

---

Technology Director

Date: _____

---

County Attorney

Date: _____