

Cybersecurity and Information Security Policy

Adopted: [DATE]

Reviewed: [DATE]

Resolution No. [NUMBER]

Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of **[District Name]** information systems, electronic records, financial systems, and operational technology from unauthorized access, disruption, loss, fraud, misuse, or cyberattack.

[District Name] recognizes that cybersecurity is essential to protecting public resources, maintaining public trust, and ensuring continuity of operations.

Scope

This policy applies to:

- All District employees
- Board members
- Contractors
- Consultants
- Volunteers
- Third-party vendors with access to District systems or information

This policy applies to:

- District-owned computers
- Mobile devices
- Servers
- Cloud systems
- Email systems
- Financial software
- Operational technology (if applicable)
- Personal devices used for District business

CONTROLS / PROTECTIONS IN PLACE

Access Control

[District Name] shall:

- Assign unique user accounts to authorized users.
- Prohibit shared user accounts.
- Require strong passwords.
- Require Multi-Factor Authentication (MFA) for:

- Email systems
- Financial systems
- Remote access
- Administrative accounts
- Remove access immediately upon employee separation.

District-Specific Information

Responsible Person/Title: _____

Network Security

The District shall maintain:

- Firewall protection
- Anti-virus/endpoint protection software
- Security updates and patch management
- Secure remote access through VPN or equivalent technology
- Network monitoring tools where available

District-Specific Information

IT Provider: _____

Managed Security Provider (if applicable): _____

Data Protection

[District Name] shall:

- Restrict access to sensitive information based on job duties.
- Encrypt sensitive information whenever feasible.
- Protect confidential information including:
 - Employee records
 - Financial information
 - Customer/public records
 - Burial records (cemetery districts)
 - Utility records (CSDs)
 - Patient records (EMS agencies)

District-Specific Information

Primary Data Storage System: _____

Backup and Recovery

[District Name] shall maintain:

- Regular automated backups
- Offsite or cloud backups
- Backup retention schedules
- Periodic backup restoration testing

District-Specific Information

Backup Vendor: _____

Backup Frequency:

- Daily ☐
- Weekly ☐
- Other ☐ _____

Financial System Security

[District Name] shall implement:

- Segregation of duties
- Dual approval for ACH or wire transfers
- Independent verification of vendor banking changes
- Bank account reconciliation
- Fraud detection controls

District-Specific Information

Banking Institution(s): _____

Authorized Financial Administrators: _____

Vendor Security

All technology vendors with access to **[District Name]** systems shall:

- Protect District information
- Notify the District of cybersecurity incidents
- Maintain reasonable security controls

District-Specific Information

Primary IT Vendor: _____

TRAINING / MONITORING

Employee Cybersecurity Training

All employees shall receive cybersecurity awareness training:

- At hire
- Annually thereafter

Training topics should include:

- Phishing awareness
- Password security
- Social engineering

- Safe internet practices
- Incident reporting procedures

District-Specific Information

Training Provider: _____

Training Schedule: _____

Monitoring and Auditing

[District Name] may monitor:

- Email systems
- Network activity
- Internet usage
- Financial system access
- Remote access activity

[District Name] shall conduct:

- Annual cybersecurity review
- Periodic access reviews
- Periodic risk assessments

District-Specific Information

Review Conducted By: _____

Risk Assessment Frequency: _____

Policy Review

This policy shall be reviewed annually by:

Responsible Party: _____

Review Date: _____

INCIDENT RESPONSE

Reporting Cybersecurity Incidents

Employees shall immediately report:

- Phishing emails
- Malware infections

- Lost or stolen devices
- Unauthorized access
- Financial fraud attempts
- Suspicious system activity

Reports shall be made to:

District-Specific Information

Primary Contact: _____

Title: _____

Phone: _____

Email: _____

Incident Response Procedures

Upon receiving notice of a cybersecurity incident, **[District Name]** shall:

Step 1 – Identify

Determine:

- Nature of incident
- Systems affected
- Potential impact

Step 2 – Contain

Actions may include:

- Disconnecting affected devices
- Disabling compromised accounts
- Blocking malicious activity

Step 3 – Investigate

[District Name] or its IT provider shall:

- Determine the cause
- Assess data exposure
- Preserve relevant evidence

Step 4 – Recover

[District Name] shall:

- Restore systems from backups
- Reset passwords
- Verify system integrity

Step 5 – Notify

When required, **[District Name]** shall notify:

- Law enforcement
- Cyber insurance carrier
- Banking institutions
- Affected individuals
- Regulatory agencies

District-Specific Information

Cyber Insurance Carrier: _____

Policy Number: _____

Claims Contact: _____

Post-Incident Review

Following any significant incident, **[District Name]** shall:

- Document lessons learned
- Identify corrective actions
- Update procedures as necessary
- Report findings to the Board if appropriate

15. Enforcement

Failure to comply with this policy may result in:

- Revocation of system access
- Disciplinary action
- Termination
- Legal action where appropriate

Board Adoption

This policy was adopted by the Board of Directors/Trustees of the:

[DISTRICT NAME]

On: _____

Chairperson: _____

General Manager / Fire Chief / Executive Director: _____