

Physical and Security Controls

1. Purpose

This document establishes the physical, administrative, and technical control requirements necessary to protect Dothan City Schools (DCS) systems, software, access mechanisms, and information assets from misuse, unauthorized access, manipulation, theft, disclosure, damage, or destruction.

All District systems and data are assets of DCS and shall be protected through layered safeguards that include both physical controls and software-based security controls.

2. Definition of Systems

For purposes of this policy, the term systems includes any current or future District-owned, leased, hosted, or managed electronic, digital, or technology-enabled asset, including but not limited to:

- Desktop computers and workstations
- Laptops and mobile computing devices
- Chromebooks and tablets
- DCS owned mobile phones
- Printing, copying, and scanning devices
- Servers, virtual systems, and hosted workloads
- Internal and external storage systems
- Backup repositories and removable media
- Cloud services and SaaS platforms
- Network switches, routers, firewalls, wireless systems, and other network appliances
- Security cameras, NVRs, door access systems, and other security equipment
- Classroom AV systems, ViewSonic boards, projectors, and instructional technology
- Communication systems, telephony, and conferencing systems
- Future technology devices, IoT systems, AI-enabled systems, and connected equipment

All such systems, together with the data they create, process, transmit, or store, are official DCS assets.

3. Protection Requirements

All systems and related data shall be protected from:

- Unauthorized access
- Unauthorized disclosure
- Misuse or inappropriate use
- Alteration or manipulation
- Theft or loss
- Accidental destruction
- Malicious destruction

- Service disruption
- Unauthorized removal from District control

Protection measures may be physical, administrative, software-based, network-based, or cloud-based, depending on the nature of the system and the data involved.

4. Physical Security Controls

DCS shall implement physical safeguards appropriate to the sensitivity and criticality of the asset.

Physical controls may include:

- Locked MDF, IDF, server, and telecommunications rooms
- Badge, key, or controlled access systems
- Security camera monitoring of sensitive areas
- Visitor access controls and escort procedures
- Secure storage for backup media and removable devices
- Cable locks or secure carts for mobile devices
- Asset tagging and inventory controls
- Environmental protections including HVAC, UPS, surge suppression, and generators
- Protection from fire, water, storm, and environmental hazards
- Controlled disposal and physical destruction of storage media

Access to sensitive technology spaces shall be limited to authorized personnel with a legitimate operational need.

5. System and Software Security Controls

Software-based and logical protections shall be implemented to secure systems and data.

These controls may include:

- Role-based access controls (RBAC)
- MFA and secure authentication
- Endpoint protection and EDR/XDR
- Patch management and vulnerability remediation
- Application allow-listing and software restriction policies
- Mobile Device Management (MDM)
- Configuration baselines and hardening standards
- Network segmentation and VLAN controls
- Firewall and content filtering enforcement
- Logging, SIEM, syslog, and alerting
- Backup, immutability, and recovery protections
- Secure remote access controls including VPN
- Device encryption and secure boot controls
- SaaS access governance and SSO enforcement

All controls shall align with District cybersecurity, privacy, and operational continuity requirements.

6. Access Control Standards

Access to District systems and information shall be granted based on:

- Job responsibility
- Instructional purpose
- Operational need
- Least-privilege principles
- Approved vendor or support agreements

The District shall create/maintain procedures for:

- New account provisioning
- Role changes and access modifications
- Periodic entitlement reviews
- Immediate offboarding and access removal
- Temporary vendor or contractor access
- Emergency administrative access procedures

Shared accounts are prohibited unless specifically approved for operational systems where individual authentication is not technically feasible.

7. Information Handling and Device Control

Any system capable of storing, displaying, transmitting, printing, scanning, recording, or exporting District data shall be configured to protect confidential and protected information.

Required controls may include:

- Secure print release
 - Screen lock timeouts
 - Restricted USB and removable media access
 - Controlled export permissions
 - Screenshot and recording restrictions where supported
 - Retention and deletion enforcement
 - Secure disposal workflows
 - MDM enforcement for mobile endpoints
 - Lost or stolen device remote wipe capabilities
-

8. Monitoring and Incident Response

The District Technology Department shall monitor critical systems for misuse, unauthorized access attempts, tampering, outages, and control failures.

Any loss, theft, unauthorized access, suspicious manipulation, or destruction of District systems or data shall be treated as a security incident and handled in accordance with District Incident & Operational Response Procedures.

9. User Responsibilities

All employees, students, contractors, volunteers, and approved users shall:

- Use District systems only for authorized purposes
 - Protect assigned devices and credentials
 - Prevent unauthorized individuals from using District assets
 - Report lost, stolen, or tampered devices immediately
 - Refrain from bypassing security controls
 - Use and/or install only approved software and cloud services
-