

Virus, Malware, Spyware, Phishing, Ransomware, and Spam Protection

1. Purpose

This document establishes the administrative and technical safeguards required to protect Dothan City Schools' data systems, devices, users, and information assets from malicious software, phishing attempts, ransomware activity, spyware, spam, and other electronic threats.

The District shall maintain a defense-in-depth, multi-layered security strategy designed to prevent, detect, contain, and remediate malicious activity across all District-managed environments.

2. Multi-Layered Protection Requirements

Virus checking, malware prevention, phishing protection, spam filtering, and related threat detection systems approved by the DCS District Technology Department shall be deployed and maintained using a multi-layered approach.

Protection layers shall include, as applicable:

- End-user devices, including desktops, laptops, Chromebooks, tablets, and mobile devices
- Servers, virtual machines, and hosted infrastructure
- Email gateways and cloud mail security platforms
- Web filters and DNS security services
- Firewalls and next-generation security appliances
- Endpoint Detection and Response (EDR/XDR) platforms
- File storage systems, collaboration platforms, and cloud services
- Backup repositories and disaster recovery systems
- Classroom displays and other network-connected instructional devices

All electronic files, attachments, downloads, removable media, cloud-transferred files, and other digital content shall be subject to automated scanning, reputation analysis, and threat inspection where technically feasible.

3. Phishing and Spam Awareness Training

Dothan City Schools shall provide annual mandatory employee training on recognizing and responding to:

- Phishing emails
- Spear phishing and impersonation attempts
- Malicious attachments and links
- Spam and fraudulent communications
- Social engineering attempts through email, text, chat, or phone
- Credential harvesting pages

- Business email compromise and financial fraud attempts

Training shall be documented as part of the District's annual data governance and cybersecurity compliance records.

4. Periodic Phishing Simulations

The District Technology Department shall conduct periodic phishing simulations to strengthen employee awareness and measure organizational susceptibility to phishing and spam attempts.

Simulation results may be used to:

- Identify departments or user groups requiring additional support
- Improve future training content
- Measure year-over-year improvement
- Reduce credential compromise risk
- Support cybersecurity insurance and audit evidence

Users who interact with simulated phishing content may be assigned immediate remedial awareness training.

5. Ransomware Protection and Recovery Controls

To reduce the risk and impact of ransomware, Dothan City Schools shall maintain safeguards that include:

- Advanced endpoint protection and behavioral detection
- Immutable or protected backups where supported
- Network segmentation to limit lateral movement
- Least-privilege administrative access
- Email attachment sandboxing and URL inspection
- Application control and software restriction policies
- Patch and vulnerability remediation processes
- Tested backup recovery procedures

Critical systems supporting student information, finance, HR, instructional delivery, safety, and communications shall receive priority protection and recovery planning.

6. User Responsibilities

All employees and authorized users shall:

- Complete required annual phishing and malware awareness training
- Refrain from opening suspicious links, attachments, or files
- Immediately report suspicious messages or device behavior
- Avoid installing unapproved software or browser extensions
- Use only District-approved storage and collaboration systems
- Follow all password and MFA requirements

Any suspected malware, phishing, ransomware, or spam-related incident shall be reported immediately to the Director of Technology Services.

7. Monitoring and Review

The District Technology Department shall periodically review the effectiveness of malware prevention controls, phishing awareness outcomes, spam filtering effectiveness, and incident trends.

Security controls and response procedures shall be updated as needed to address evolving threats, changes in District systems, or legal and insurance requirements.
