

FSD3 Technology Security and Data Recovery Plan



The background features a blue and white curved design. On the right side, there is a graphic with binary code (0s and 1s), a globe icon, and a series of interlocking gears. The text is positioned on the left side of the white curve.

Internet Content Filtering

- In accordance with federal and state law, FSD3 filters internet traffic for content defined in law as harmful to minors.
- FSD3 acknowledges that technology-based filters are not always effective at eliminating harmful content and due to this, FSD3 uses a combination of technological and supervisory means to protect students from harmful online content.
- In the event that students take devices home, FSD3 will provide a technology-based filtering solution for those devices. However, the district relies on parents to provide the supervision necessary to fully protect students from accessing harmful online content.
- Students shall be supervised when accessing the internet and using district-owned devices on school property.

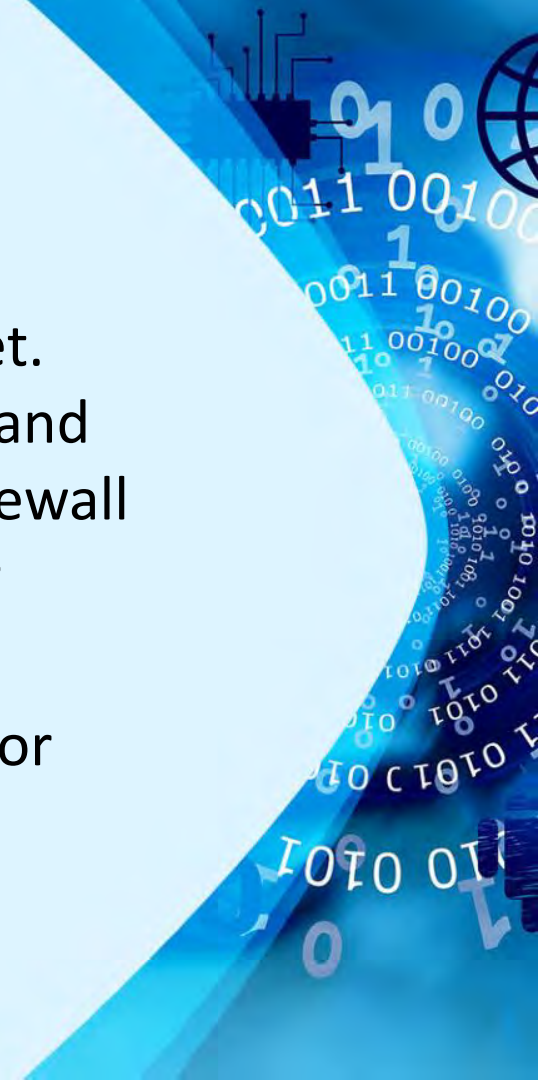


Malicious Software

- Server and workstation protection software are deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
- FSD3 installs, distributes and maintains spyware and virus protection software on all relevant district-owned equipment, i.e. servers, workstations, and laptops.
- FSD3 ensures that malicious software protection will include frequent update downloads, frequent scanning and that malicious software protection is in active state (real time) on all operating servers/workstations.
- FSD3 ensures that all security-relevant software patches (relevant workstations and servers) are applied within 30 days, and critical patches shall be applied as soon as possible.
- All computers must use the relevant district- approved anti-virus solution.

Firewalls

- A firewall acts as a barrier between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents many hacker connections to your computer.
- Firewalls filter network packets that enter or leave your computer.





Physical Security

Computer Security

User's computer should not be left unattended and unlocked, especially when logged in to sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers are used to enforce this requirement.

FSD3 shall ensure that all equipment that contains sensitive information will be secured to deter theft.

Server/Network Room Security

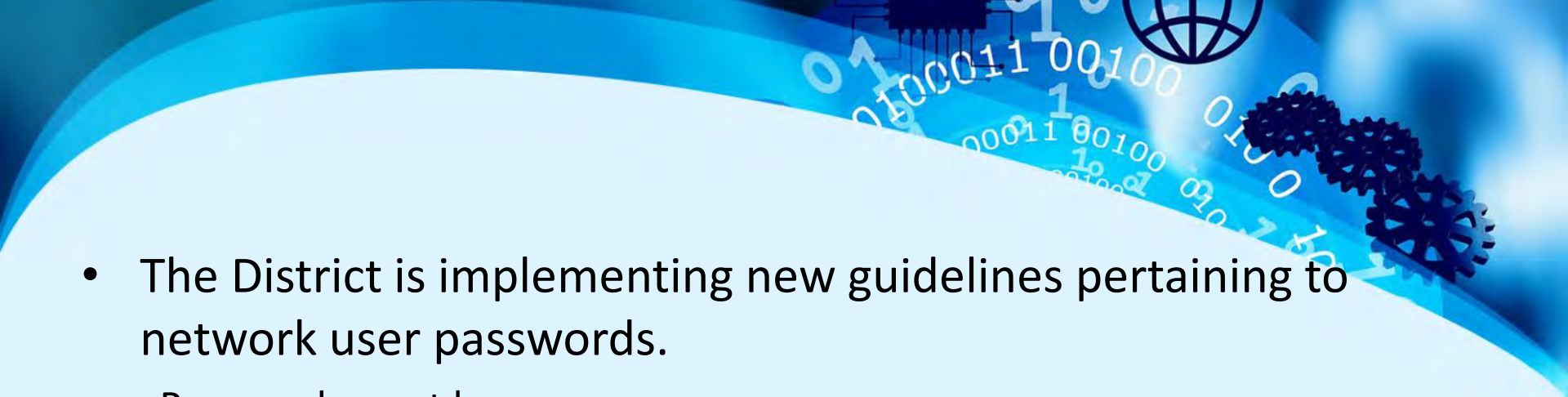
Server rooms and telecommunication rooms/closets should remain locked to restrict access from general school or district office areas. Access control shall be enforced with only those IT or other staff members requiring access necessary to perform their job functions allowed unescorted access.

Telecommunication rooms/closets may only remain unlocked or unsecured when, because of building design, it is impossible to do otherwise, or due to environmental problems that require the door to be opened.



Network Security

- Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities.
- Network Segmentation
 - FSD3 ensures that all untrusted and public access computer networks are separated from main district computer networks, and utilize security policies to ensure the integrity of those computer networks.
 - FSD3 utilizes industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and to minimize potential damage from other compromised systems.
- Wireless Networks
 - No wireless access point shall be installed on FSD3's computer network by anyone other than employees of the FSD3 Technology Department.
 - FSD3 scans for and removes or disables any rogue wireless devices on a regular basis.
 - All wireless access networks will conform to current best practices and shall utilize, at minimal, WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary

- 
- The District is implementing new guidelines pertaining to network user passwords.

Passwords must be:

- Forced by the system to be changed every 90 days.
- Passwords must be at least eight (8) characters in length
- Strong passwords can include a combination of:
 - Numerals
 - Alphabetic characters
 - Upper and lower case letters
 - Special characters

The background features a blue and white color scheme. At the top, there's a blue curved banner. Below it, the background is white with faint, stylized binary code (0s and 1s) scattered across it. In the upper right corner, there's a black silhouette of a globe. To the right of the globe, there are several interlocking black gears of different sizes, suggesting a mechanical or industrial theme related to technology.

Incident Management

- Monitoring and responding to IT-related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.
- In the event of a cybersecurity attack or other unauthorized network activity, appropriate law enforcement agencies (local, state and federal) and/or cybersecurity organizations (such as the Center for Internet Security) will be notified as necessary.

Business Continuity

- To ensure continuous critical IT services, IT will implement a disaster recovery plan which includes at a minimum:
 - Data Backup: All servers will be fully backed up daily as well as a separate backup of critical user files for quicker access. A set of backup media will be stored off-site at a reasonably safe distance from the primary server room.
 - Offsite Location: The district will use an off-site storage provider to hold copies of recent backups.
- Emergency Procedures: Emergency actions will include notification of responsible individuals, recovery of backup data, replacement of damaged hardware, and offsite data/service recovery if location is compromised.



Data Privacy

- FSD3 considers the protection of the data it collects on students, employees and their families to be of the utmost importance
- FSD3 protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (“FERPA”), and 15 U.S. Code §§ 6501–6506 (“COPPA”).
- FSD3 shall ensure that access to employee records shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

Questions?

