Detroit ISD Cybersecurity Manual

Updated 2025-05-14

Introduction

This manual documents the policies and procedures Detroit ISD will use to ensure the security of information systems used by the district and to protect the data stored therein.

Table of Contents

Change Log

The Cybersecurity Manual will be reviewed annually and be properly coordinated with the district's other plans.

The Cybersecurity Manual's notable modifications are included in the table along with the date of the Manual's review.

This Record of Changes and Review identifies only significant changes made to this Manual. If no significant changes were made, the phrase "Cybersecurity Review Conducted" has been placed in the Summary of Significant Changes and Review column.

Date of Change	Person Making the Change	Summary of Changes
2024-06-19	David Williams	Initial creation
2025-04-03	David Williams	Annual review
2025-05-14	David Williams	Clarified password reset procedures for Staff accounts.

Access Control

These policies guide the process of creating, managing, suspending, and deleting user accounts on the systems maintained by Detroit ISD. The Technology Director or someone designated by them will be responsible for maintaining user accounts for students, staff, and other users.

Account Creation

Student Accounts

Student accounts will be created when new students are registered in the district's Student Information System (SIS). Office staff will notify the Technology Director or designee when a new student is enrolled. The Technology Director or designee will also generate a report from the SIS from time to time to find students who are registered and don't have an account.

Student usernames and passwords will be generated using a formula and shared in the Student Logins Sheet, accessible to district teachers and staff. All student accounts created by the Detroit ISD Technology Department will use these usernames and passwords. Students may change the password on their accounts if they prefer but the district will reset them to the values listed in the Student Logins Sheet if a password reset is required.

The district may also use Single Sign-On (SSO) and rostering systems to automate the creation of student user accounts.

Staff Accounts

Staff accounts will be created when the Technology Director or designee are notified by District Administrators. This will be documented in the Staff Changes Sheet. Access to the Staff Changes Sheet will be limited to Administrators who are involved in the hiring process.

When staff members request a password reset, Technology staff will verify the identity of the person making the request and take appropriate actions to ensure accounts are kept secure. These may include the following. Password reset requests will be documented in the ticketing system.

- Talking to the staff member in person.
- Talking to the staff member via phone at their internal extension.
- Emailing the temporary password to the staff member's immediate supervisor.

The district may also use SSO and rostering systems to automate the creation of staff user accounts.

Other Accounts

Outside consultants, services, or other special circumstances may require other user accounts to be created on district systems. These will be managed by the Technology Director or designee.

Account Suspension

Staff Accounts

Staff accounts will be suspended when their employment with the district ends. The timing of that suspension will be as follows.

- On the date their employment ends, their accounts will be changed to “Pending Suspension” status and their membership in all district maintained groups will be removed. A message will be appended to any emails sent from their account making it clear they are no longer employed with the district.
- The district may allow a reasonable time for them to forward any personal messages or documents to a personal account before suspending their Detroit ISD account.
- If the circumstances warrant, account suspension will be immediate.

Other Accounts

Accounts for outside consultants, services, and other special circumstances will be suspended when they are no longer needed.

Account Deletion

Staff Accounts

Staff accounts will be deleted after 10 years of inactivity.

Student Accounts

Student accounts will be deleted when their enrollment at Detroit ISD ends. Office staff will notify the Technology Director or designee when a student is no longer enrolled at the district. The Technology Director or designee will also generate a report from the SIS from time to time to find students who are no longer enrolled at the district.

Graduates will continue to have access to their accounts through the summer after they graduate, at which time they will be deleted.

Other Accounts

Accounts for outside consultants, services, and other special circumstances will be deleted after 10 years of inactivity.

Awareness and Training

Annual Cybersecurity Training

All staff who handle confidential or sensitive information or are required to access district information systems to complete their duties will complete an annual cybersecurity training that meets the requirements set forth by Texas Department of Information Resources (DIR).

Additional Training and Updates

The Technology Director or designee will share information on cybersecurity threats from time to time with staff to help them recognize risky actions and protect district systems. Additionally, the Technology Director or designee will conduct simulated Phishing campaigns at least twice per year for staff.

Staff with access to the SIS, confidential information, or other sensitive information will receive training on how to properly handle that information before being granted access.

See Board Policy DMA- Professional Development: Required Staff Development and CQB-Technology Resources: Cybersecurity.

Audit and Accountability

User Accounts Audit

The Technology Director or designee will conduct an audit of user accounts to ensure unused accounts are suspended or deleted and that staff and students have the appropriate permissions at least annually. Additional user account audits will be conducted if there is an indication of inappropriate access or privileges.

Security Assessment and Authorization

Annual Cybersecurity Assessment

The Technology Director or designee will conduct an annual assessment of the district's cybersecurity posture in accordance with relevant laws and regulations.

Vulnerability Scanning

The Technology Director or designee will review monthly Dorkbot and Cybersecurity and Infrastructure Security Agency (CISA) scan reports of public IPs and address any vulnerabilities found.

Penetration Testing

The district does not develop custom applications that would require testing.

Configuration Management

Backups of system configurations will be kept when possible in order to help restore systems to an operational state in the event of an outage.

When upgrading or replacing equipment, care will be taken to ensure that the new or upgraded systems provide the same or better performance, security, and functionality. Any updates to the configuration settings will be recorded in the Detroit ISD Systems Change Log.

Systems will be configured to perform the needed functions without exposing the district to additional risk by leaving unnecessary ports and functions enabled.

Access Restrictions for Change

Changes to the system may only be made by authorized Systems Administrators. Systems shall be configured to require elevated access to perform change, and access to System Administrative accounts will be restricted to those who require elevated access to perform their job functions.

Information System Component Inventory

Detroit ISD Technology Staff shall maintain an inventory of production systems that accurately reflects the current systems. The inventory will include:

- Public and Private IP address
- Hostname
- System description
- Hardware type
- Serial number
- Additional notes

The information system component inventory shall be kept up to date at all times, and is reviewed no less than annually by the Technology Director or designee.

Detroit ISD Technology Staff will maintain an inventory of all physical information system assets. This inventory includes district-owned servers, desktops, laptops, and tablets. This inventory will record asset tags, serial numbers, and a description of the assets, and is audited annually.

Detroit ISD Technology Staff maintains a software inventory of all licensed and approved software in the environment. This software inventory is updated as new software is purchased or old software is deprecated. It is reviewed at a minimum annually.

Configuration Management Plan

Mission critical systems may be repurposed for other functions when they are no longer viable for their original purpose. The Technology Director is responsible for the reallocation of hardware resources and approves all reallocations. These changes are documented within the change management system when they occur, and the information system component inventory is updated. Any media that may have stored sensitive information is to be sanitized in accordance with the Media Protection policy: Media Sanitation section.

Software Usage Restrictions

On all systems, personnel are required to report any unauthorized use of software that they encounter to the Technology Director. Use of software in violation of copyright laws or EULA's is not tolerated or permitted.

User Installed Software

Personnel, other than Systems Administrators, are specifically prohibited from installing software on mission critical systems. Mission critical systems shall be configured such that elevated privileges are required to install software.

If business need is documented, personnel users may be granted elevated privileges to non-mission critical systems. The Technology Director maintains the list of users and the approval for elevated privileges. These users are permitted to install software on their non-mission critical systems so long as it does not violate copyright law and it does not compromise the security of the system.

Contingency Planning

Cybersecurity incidents will be included as part of the district's Cybersecurity Incident Response Plan. This plan will be reviewed and updated annually by the Technology Director or designee in consultation with other district staff and outside consultants as appropriate.

Contingency Plan

The district's Cybersecurity Incident Response Plan will include a contingency plan for the information system that identifies essential missions and business functions and associated contingency requirements, provides recovery objectives, restoration priorities, and metrics, addresses contingency roles, responsibilities, assigned personnel with contact information, addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure, addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and is reviewed and approved by the Detroit ISD Superintendent.

Detroit ISD will distribute copies of the contingency plan to personnel or groups with mission-critical responsibilities. Contingency plan changes will be communicated to personnel or groups with mission-critical responsibilities upon approval. The contingency plan shall be protected from unauthorized changes.

The contingency plan development shall be managed in consultation with relevant district staff and outside consultants as appropriate.

Contingency Training

Detroit ISD will provide contingency training to personnel consistent with their assigned roles and responsibilities. Training shall occur within 30 days of assuming a contingency role, when an information system change merits, and annually thereafter.

Telecommunications Services

Detroit ISD will establish alternate telecommunications services to include necessary agreements to permit the resumption of mission critical information system operations and/or business functions when the primary telecommunications capabilities are unavailable.

Information System Backup

Detroit ISD will conduct backups of user-level information and system-level information contained in the information system, and information system documentation to include security-related documentation, all in support of recovery time and point objectives.

Detroit ISD will protect the confidentiality, integrity, and availability of backup information at all storage locations.

Information System Recovery and Reconstitution

Detroit ISD will provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure as documented in the system baseline.

See Detroit ISD Cybersecurity Incident Response Plan.

Identification and Authentication

Account Privileges

All user accounts will be granted access to district systems according to the principle of least privilege. Least privilege means users will have access to perform their job duties but will be restricted from accessing information or systems that are not needed for that purpose.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) will be required for all staff who handle confidential or sensitive district information to login to their email accounts. Additional systems, like the district's SIS, will also implement MFA in the future.

Sharing of Login Credentials

Staff will not share their login credentials with others. Shared login accounts will be created only in very limited circumstances, with the approval of the Technology Director, and will be limited in what systems they have access to.

Incident Response

The district will develop a cybersecurity incident response plan as part of the district's Detroit ISD Cybersecurity Incident Response Plan.. This plan will be reviewed and updated annually by the Technology Director or designee in consultation with other district staff and outside consultants as appropriate.

See Board Policy CQB- Technology Resources: Cybersecurity.
See Detroit ISD Cybersecurity Incident Response Plan.

Maintenance

Controlled Maintenance

The Detroit ISD Technology Director or designee:

- Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and Detroit ISD requirements.
- Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
- Must approve the removal of the information system or system components from Detroit ISD facilities for off-site maintenance or repairs before.
- Sanitizes equipment to remove all information from associated media prior to removal from Detroit ISD facilities for off-site maintenance or repairs.
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Maintenance Tools

The Detroit ISD Technology Director or designee approves, controls, and monitors information system maintenance tools. Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. Checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Non-Local Maintenance

The Detroit ISD Technology Director or designee:

- Approves and monitors nonlocal maintenance and diagnostic activities.
- Allows the use of non-local maintenance and diagnostic tools only as consistent with Detroit ISD policy and documented in the security plan for the information system.

- Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions.
- Maintains records for non-local maintenance and diagnostic activities.
- Terminates session and network connections when non-local maintenance is completed.
- Documents in the security plan for the information system, the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.

Maintenance Personnel

The Detroit ISD Technology Director or designee:

- Establishes a process for maintenance personnel authorization and maintains a list of authorized Detroit ISD maintenance personnel.
- Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.
- Designates Detroit ISD personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Timely Maintenance

Detroit ISD obtains maintenance support and/or spare parts for all production systems within 48 hours of failure.

Media Protection

Technology Staff:

- Sanitizes media prior to disposal, release out of Detroit ISD control, or release for reuse using sanitization techniques and procedures in accordance with applicable federal and State standards and policies.
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Physical and Environmental Protection

Access to network equipment, servers, and other sensitive equipment will be controlled by keeping the doors locked to the closets they are located in. Only authorized personnel will have keys to access these closets. Outside technicians or other visitors requiring access to these areas will be escorted and monitored by authorized Detroit ISD personnel.

Authorized personnel will sign in when entering secure areas and sign out when leaving secure areas.

The closets where network equipment, servers, and other sensitive equipment exist will be provided with adequate cooling and protection from environmental threats to ensure their continued operation. Battery backup devices will be maintained to protect connected equipment from instability in the power supply.

Planning

The Technology Director or designee, in consultation with appropriate staff and outside consultants, will review this manual annually to maintain compliance with State law and regulations and ensure its effectiveness.

Personnel Security

Personnel Screening

Detroit ISD's Human Resources department will screen personnel for security risks during the hiring process and additionally as warranted.

Personnel Termination

Upon the termination of an employee of Detroit ISD:

- Human Resources will notify the Technology Director or designee who will disable access to sensitive information systems.
- Human Resources will deactivate access control badges.
- The immediate supervisor will collect any devices, keys, and other district property.

Personnel Transfer

The Technology Director will:

- Review and confirm ongoing need for logical and physical access to information systems when personnel are transferred to other positions within Detroit ISD.
- Initiate the necessary reassignment actions.
- Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer.

Access Agreements

Employees of Detroit ISD that need access to sensitive information resources must agree to the access policies contained in the Detroit ISD Employee Handbook annually.

See Board Policy CQ, DH, and GB.

Third-Party Personnel Security

Third-party providers will be required to comply with Detroit ISD's security policies and procedures. If a third-party provider is issued access badges or other secure credentials from Detroit ISD, they will be required to notify the district of any relevant personnel changes or transfers. Compliance with this policy will be monitored by the Technology Director.

Personnel Sanctions

If an employee fails to comply with district policies on information security the Technology Director will refer the incident to their immediate supervisor.

Personally Identifiable Information Processing

The district will ensure Personally Identifiable Information (PII) collected by the district is kept confidential and protected from unauthorized access or disclosure. Staff who have access to PII will receive annual training on confidentiality and responsible use of PII and other sensitive information.

See Board Policy FL- Student Records.

Privacy Notice

The district will develop and publish a privacy notice on the district website.

See Privacy Policy

Risk Assessment

As part of the district's annual cybersecurity assessment, the Technology Director or designee will consider the risks associated with all the systems the district uses. Additional controls and mitigation strategies will be implemented as appropriate based on the district's ability, available resources, and the level of risk presented.

Vulnerability Scanning

The Technology Director or designee will review monthly Dorkbot scan reports of public IPs and address any vulnerabilities found in accordance with Detroit ISD's risk assessment policies.

System and Services Acquisition

Acquisition Process

Detroit ISD will include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and Detroit ISD mission/business needs:

- Security assurance requirements.
- Security-related documentation requirements.
- Requirements for protecting security-related documentation.
- Description of the environment in which the system is intended to operate.

Information System Documentation

For externally developed systems, Detroit ISD shall obtain administrator documentation for the information system, system component, or information system service that describes:

- Secure configuration, installation, and operation of the system, component, or service.
- Effective use and maintenance of security functions/mechanisms.
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

Additionally, Detroit ISD shall obtain user documentation for the information system, system component, or information system service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
- Methods for user interaction, which enables personnel to use the system, component, or service in a more secure manner.

- User responsibilities in maintaining the security of the system, component, or service.

Detroit ISD shall document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and complete a risk assessment in response.

The documentation shall be protected as required, in accordance with the risk management strategy and distributed to appropriate personnel as needed.

External Information System Services

Detroit ISD will require providers of external information system services to comply with Detroit ISD information security requirements and employ equivalent controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Detroit ISD will define and document government oversight and user roles and responsibilities with regard to external information system services where necessary and employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

System and Communications Protection

Application Partitioning

The information system separates user functionality including user interface services from information system management functionality.

Information in Shared Resources

The information system prevents unauthorized and unintended information transfer via shared system resources.

Denial of Service Protection

The information system takes reasonable measures to protect against or limit the effects of denial of service attacks.

Boundary Protection

Detroit ISD's information system:

- Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
- Implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal Detroit ISD networks.
- Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with Detroit ISD security architecture.

Transmission Confidentiality and Integrity

The information system protects the confidentiality and integrity of transmitted sensitive information.
The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information; detect changes to information during transmission unless otherwise protected by Detroit ISD defined alternative physical safeguards.

Cryptographic Protection

The information system implements appropriate cryptographic controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Public Key Infrastructure Certificates

Detroit ISD obtains public key certificates from an approved service provider.

Voice Over Internet Protocol

Detroit ISD Technology staff:

- Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.
- Authorizes, monitors, and controls the use of VoIP within the information system.

Session Authenticity

The information system protects the authenticity of communications sessions.

Wireless Link Protection

The information system protects external and internal wireless links from unauthorized access.

Usage Restrictions

The organization:

- Establishes usage restrictions and implementation guidance for systems based on the potential to cause damage to the information system if used maliciously; and
- Authorizes, monitors, and controls the use of such systems within the information system.

System and Information Integrity

Flaw Remediation

Detroit ISD Technology Staff:

- Identifies, reports, and corrects information system flaws.
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- Installs externally-visible security-relevant software and firmware updates within the timelines indicated below:
    - Critical/High – 48 hours
    - Moderate – 10 business days
    - Low - 40 business days
- Incorporates flaw remediation into the district's configuration management process.
- Detroit ISD employs automated mechanisms to determine the state of information system components with regard to flaw remediation.

Information System Monitoring

Detroit ISD Technology Staff shall:

- monitor the information system to detect:
    - Attacks and indicators of potential attacks
    - Unauthorized local, network, and remote connections.
- Identifies unauthorized use of the information system
- Deploys monitoring devices:
    - (i) strategically within the information system to collect essential information; and
    - (ii) at ad hoc locations within the system to track specific types of transactions of interest, within the core and up to district handoff
- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- Heightens the level of information system monitoring activity whenever there is an indication of increased risk to Detroit ISD operations, assets, individuals, and other Detroit ISD designated systems.

- Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Security Alerts, Advisories, and Directives

Detroit ISD Technology Staff:

- Receives information system security alerts, advisories, and directives from CISA and TX-ISAO on an ongoing basis.
- Generates internal security alerts, advisories, and directives as deemed necessary.
- Disseminates security alerts, advisories, and directives to appropriate personnel.
- Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Spam Protection

Detroit ISD:

- Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
- Updates spam protection mechanisms when new releases are available in accordance with configuration management policy and procedures.

Detroit ISD centrally manages spam protection mechanisms.

Information Handling and Retention

Detroit ISD handles and retains information within the information system and information output from the system in accordance with applicable federal laws, state of Texas laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supply Chain Risk Management

The organization protects against supply chain threats to the information system, system component, or information system service as part of a comprehensive, defense-in-breadth information security strategy.

Trustworthiness

The organization:

- Describes the trustworthiness required in the vendors supporting its critical missions/business functions; and

- Implements policies and requirements to achieve such trustworthiness.