MOOSONEE DISTRICT SCHOOL AREA BOARD

ADMINISTRATIVE PROCEDURE GENERAL ADMINISTRATION: N0. 190	
Effective	June 13, 2023
Last Revised	May 28, 2024
Last Reviewed	May 28, 2024

BOARD INFORMATION SECURITY

Part A – Wireless Network Procedure
Part B – Media Content and Advertising Review Procedure
Part C – Authentication / Authorization Control Procedure
Part D – Acceptable Use Procedure
Part E – Portable Media Procedure
Part F – Data Backup and Recovery Procedure
Part G – Secure Information Deletion Procedure
Part H – Disaster Recovery Procedure
Part I – Incident Response Procedure
Part J – Device Secure Configuration Procedure
Part K – 3rd Party Vendor Security Procedure
Part L – Mobile Device Security Procedure

Part A – WIRELESS NETWORK PROCEDURE

1.0 PURPOSE

The purpose of the Wireless Network Procedure is to provide guidelines for secure and efficient use of the wireless network within the Moosonee District School Area Board (MDSAB) and define requirements for connecting to public wireless networks to ensure the integrity, confidentiality, and availability of school board data.

2.0 SCOPE

This procedure applies to all MDSAB employees, students, contractors, vendors, and guests who use wireless devices to access school board networks, data, and systems.

3.0 PROCEDURE

3.1 Internal Wireless Network Use

3.1.1 MDSAB will use Wi-Fi Protected Access 2 (WPA2) or stronger for encryption on all internal wireless networks.

3.1.2 The IT department will monitor and perform regular audits of the wireless network to identify and mitigate any security vulnerabilities.

3.2 Public Wireless Network Use

3.2.1. Employees must not access sensitive school board data when connected to public wireless networks unless using secure, encrypted connections such as a Virtual Private Network (VPN).

3.2.2. Employees must ensure public networks use at least WPA2 encryption. If the security level of the public network is unknown, it should not be used.

3.3 Guest Access

Guest access to the school board's wireless network is provided on a separate network that is isolated from the internal network.

4.0 Compliance

Non-compliance with this procedure may result in temporary or permanent loss of wireless network access privileges, disciplinary action, and potential legal action. Any exceptions to this procedure must be approved by the IT Department.

Part B – MEDIA CONTENT AND ADVERTISING REVIEW PROCEDURE

1.0 PURPOSE

The purpose of the Media Content and Advertising Review Procedure is to ensure all media content and advertising materials related to the Moosonee District School Area Board (MDSAB) are reviewed for potential copyright and trademark infringement, and libel or slander, prior to release.

2.0 SCOPE

This procedure applies to all MDSAB employees, contractors, and third parties creating, developing, or disseminating content on behalf of MDSAB, including but not limited to advertising materials, press releases, social media posts, and website content.

3.0 PROCEDURE

3.1 Copyright and Trademark Infringement

3.1.1. All content must be original or have the appropriate permissions, licenses, or releases before use. Unauthorized use of copyrighted material or trademarks is strictly prohibited.

3.1.2. The designated Review Team (Board Administration or School Administration) will verify the originality of content and the proper usage of copyrighted or trademarked materials.

3.1.3. Any content suspected of infringement will be removed and not used until necessary permissions or licenses are obtained.

3.2 Libel or Slander

3.2.1. All content must be factual and respectful. Defamatory, false, or misleading statements that could harm the reputation of individuals or organizations are strictly prohibited.

3.2.2. The Review Team will assess the content for potential libelous or slanderous statements.

3.2.3. Any content suspected of libel or slander will be edited or removed.

3.3 Review Process

3.3.1. All content must undergo a review process by the designated Review Team before being released publicly.

3.3.2. The Review Team will verify that content aligns with this procedure and other relevant school board policies.

3.3.3. Content creators must allow sufficient time for the review process to take place before the desired publication date.

4.0 COMPLIANCE

Non-compliance with this procedure may result in disciplinary action up to and including termination of employment or contract, and potential legal action. Any exceptions to this procedure must be approved by the Review Team.

Part C – AUTHENTICATION / AUHORIZATION CONTROL PROCEDURE

1.0 PURPOSE

The purpose of the Authentication/Authorization Control Procedure is to ensure that access to IT systems used by the Moosonee District School Area Board (MDSAB) is appropriately controlled and managed through a central directory system to protect the integrity, confidentiality, and availability of school board data.

2.0 SCOPE

This procedure applies to all MDSAB employees, students, contractors, and third parties who access school board systems, networks, or data.

3.0 PROCEDURE

3.1 Central Directory System

3.1.1. All user authentication and authorization will be controlled through a central directory system, such as Active Directory or Azure AD.

3.1.2. The IT department is responsible for the setup, management, and security of the central directory system.

3.2 User Account Management

3.2.1. All users will be assigned a unique identifier (UserID) for their personal and exclusive use.

3.2.2. User access rights will be granted based on the principle of least privilege, providing only those access rights necessary for the execution of an individual’s role.

3.3 Authentication

3.3.1. Strong, unique passwords or other secure authentication mechanisms are required for all user accounts.

3.3.2. Multi-factor authentication (MFA) should be used where possible, particularly for access to sensitive systems or data.

3.4 Authorization

3.4.1. Changes to access rights must be reviewed and approved by appropriate personnel.

3.4.2. Access rights will be reviewed regularly to ensure they are still appropriate for the user's current role.

3.4.3. Access rights will be revoked immediately upon termination of employment or when no longer needed.

4.0 Content Filtering

4.1. Content will be filtered at the DNS level for malicious, inappropriate, and distracting websites or applications based on industry standards and vendor provided block lists.

5.0 COMPLIANCE

Non-compliance with this procedure may result in temporary or permanent loss of access privileges, disciplinary action, and potential legal action. Any exceptions to this policy must be approved by the IT Department.

Part D – ACCEPTABLE USE PROCEDURE

1.0 PURPOSE

The purpose of the Acceptable Use Procedure is to provide guidelines that promote ethical, responsible, and legal use of technology resources within the Moosonee District School Area Board (MDSAB).

2.0 SCOPE

This procedure applies to all MDSAB employees, students, contractors, and third parties who use, access, or interact with the school board's technology resources and systems.

3.0 PROCEDURE

3.1 Acceptable Use

3.1.1. Technology resources must be used in a manner that supports learning, teaching, and daily operations of MDSAB.

3.1.2. Users must respect the rights and privacy of others, adhere to all laws and contractual obligations, and maintain integrity, availability, and confidentiality of information.

3.2 Prohibited Use

3.2.1. Users must not use technology resources to engage in activities that are illegal, unethical, harmful, or not in the best interest of MDSAB.

3.2.2. This includes, but is not limited to, activities such as hacking, cyberbullying, unauthorized access, intentional distribution of malware, and infringing upon copyright and intellectual property rights.

3.3 Internet Safety

3.3.1. Users must follow good internet safety practices, including not revealing personal information online, avoiding inappropriate websites, and reporting any cyber harassment or bullying immediately to an appropriate authority.

3.3.2. Users will be subject to cyber security training provided by a 3rd party vendor.

3.3.3. Users who fail the training will be subject to additional learning and testing until a satisfactory level of competency is reached.

3.4 Personal Responsibility

3.4.1. Users are responsible for their actions while using technology resources and must immediately report any violations of this policy to an appropriate authority.

4.0 COMPLIANCE

Violation of this procedure may result in disciplinary action, up to and including termination of employment for staff, termination of contracts for third parties, and legal action. Any exceptions to this procedure must be approved by the MDSAB Board of Trustees.

Part E – PORTABLE MEDIA PROCEDURE

1.0 PURPOSE

The purpose of the Portable Media Procedure is to establish guidelines for the proper use of removable media, such as USB drives, DVD-R, and CD-R, to protect the confidentiality, integrity, and availability of data collected, stored, and managed by the Moosonee District School Area Board (MDSAB).

2.0 SCOPE

This procedure applies to all MDSAB employees, contractors, and third parties who use removable media to store, transfer, or access school board data.

3.0 PROCEDURE

3.1 Use of Portable Media

3.1.1. Portable media should be used only when necessary. Whenever possible, secure methods such as secure file transfer protocols or secure cloud storage should be used instead.

3.1.2. All data stored on portable media must be encrypted using a method approved by the IT department.

3.1.3. Portable media must not be used to store sensitive or confidential information unless explicitly authorized by the appropriate authority.

3.2 Management of Portable Media

3.2.1. The IT department will maintain a register of all approved portable media devices.

3.2.2. Users must return portable media to the IT department for secure disposal when no longer needed.

3.2.3. Lost or stolen portable media must be reported immediately to the IT department.

4.0 Compliance

Users found to be in violation of this procedure may face disciplinary action, up to and including termination of employment or contract, and legal action. 3.3.2. Any exceptions to this procedure must be approved by the IT Department.

Part F – DATA BACKUP AND RECOVER PROCEDURE

1.0 PURPOSE

The purpose of this Data Backup and Recovery Procedure is to ensure that all critical data and systems within the Moosonee District School Area Board (MDSAB) are appropriately backed up and can be recovered in the event of equipment failure, intentional destruction of data, or a disaster.

2.0 SCOPE

This procedure applies to all MDSAB data and systems, and to all employees, contractors, and third parties involved in managing and maintaining these data and systems.

3.0 PROCEDURE

3.1 Data Backup

3.1.1. All critical data will be backed up regularly as per the determined schedule, with frequency depending on the nature of the data.

3.1.2. The backups will include all necessary information required to restore system functionality, including system state data, application data, and system and application configuration information.

3.1.3. Backup data will be stored on separate, secure, and reliable media.

3.1.4. Backups will be protected with the same level or better of security as the original data.

3.2 Data Recovery

3.2.1. Data recovery procedures will be regularly tested to ensure they are effective and that they can be completed in a timely manner.

3.2.2. In the event of a system failure or data loss, the IT department will prioritize recovery actions based on the critical nature of the systems and data involved.

3.2.3. Users must immediately report any data loss or system failure to the IT department.

4.0 COMPLIANCE

Non-compliance with this procedure may result in disciplinary action, up to and including termination of employment for staff and termination of contracts for third parties. Any exceptions to this procedure must be approved by the MDSAB Board of Trustees.

Part G – SECURE INFORMATION DELETION PROCEDURE

1.0 PURPOSE

The purpose of the Secure Deletion Procedure is to provide guidelines for securely deleting sensitive data within the Moosonee District School Area Board (MDSAB) to protect the confidentiality and integrity of the data and prevent unauthorized access.

2.0 SCOPE

This procedure applies to all MDSAB employees, contractors, and third parties who handle school board data, particularly sensitive or confidential data.

3.0 PROCEDURE

3.1 Secure Deletion Practices

3.1.1. All sensitive data must be deleted in a manner that ensures it cannot be recovered or reconstructed.

3.1.2. Deletion methods may include overwriting, degaussing, physical destruction, or other methods as approved by the IT department.

3.1.3. Digital media used to store sensitive data must be securely wiped before disposal, reuse, or transfer of ownership.

3.2 Data Disposal

3.2.1. Physical media used to store sensitive data, such as paper records, CDs, and DVDs, must be securely destroyed before disposal.

3.2.2. Secure destruction methods include cross-cut shredding, incineration, or other methods as approved by the IT department.

3.3 Compliance

3.3.1. Non-compliance with this procedure may result in disciplinary action, up to and including termination of employment or contract, and legal action.

3.3.2. Any exceptions to this procedure must be approved by the IT Department.

Part H – DISASTER RECOVERY PROCEDURE (DRP)

1.0 PURPOSE

The purpose of this Disaster Recovery Procedure (DRP) is to provide a structured approach for responding to unplanned incidents that could impact the Moosonee District School Area Board's (MDSAB) IT infrastructure, including hardware, software, networks, and data.

2.0 SCOPE

This plan applies to all MDSAB IT systems, data, and networks, and to all MDSAB employees, contractors, and third parties responsible for managing and maintaining these resources.

3.0 PROCEDURE

3.1 Disaster Recovery Team

3.1.1. A Disaster Recovery Team, led by the IT Manager, is responsible for implementing the DRP, including restoring systems and data, coordinating with other teams, and communicating with stakeholders.

3.2 Incident Response

3.2.1. Upon detecting a disaster, the first response should be to ensure the safety of all personnel. Then, the incident should be reported to the Disaster Recovery Team and the severity of the disaster should be assessed.

3.2.2. The Disaster Recovery Team should document the incident, including the nature of the disaster, the affected systems and data, and any steps taken to respond to the disaster.

3.3 Recovery Procedures

3.3.1. The Disaster Recovery Team will implement the necessary procedures to restore systems and data, following the prioritization based on the critical nature of the systems and data.

3.3.2. The recovery process includes: assessing the damage, activating the backup system, retrieving backup data, recovering or replacing damaged systems, and testing the functionality of the restored systems.

3.4 Communications

3.4.1. The Disaster Recovery Team will communicate the status of the recovery efforts to relevant stakeholders, including employees, school board management, and parents, as necessary.

3.4.2. All communication should be clear, accurate, and timely to manage expectations and reduce confusion or panic.

4.0 TESTING AND MAINTENANCE

The DRP will be tested at least annually to ensure its effectiveness. The plan should also be reviewed and updated regularly, or whenever there are significant changes to the IT infrastructure.

Part I – INCIDENT RESPONSE PROCEDURE

1.0 PURPOSE

The purpose of the Incident Response Policy is to ensure a coordinated response to information security incidents, protecting the Moosonee District School Area Board (MDSAB) assets and reputation.

2.0 SCOPE

This policy applies to all MDSAB systems, networks, and data, and to all employees, contractors, and third parties who interact with these resources.

3.0 PROCEDURE

3.1 Incident Reporting

3.1.1. Any security incident or suspected security incident must be reported immediately to the MDSAB IT department.

3.2 Incident Response Team

3.2.1. The Incident Response Team, led by the IT Manager, is responsible for responding to all reported security incidents.

3.2.2. The school board's designated cybersecurity partner, will provide an Incident Response Team and act according to their internal procedures.

3.3 Incident Response Process

3.3.1. Upon receiving a report of a security incident, the authorized cybersecurity partner will initiate the following process:

Identification - Confirm whether an incident has occurred and identify its nature and scope.

Containment - Take immediate steps to prevent further damage or loss, which may include isolating affected systems or networks.

Eradication - Identify and eliminate the cause of the incident, such as removing malware or correcting vulnerabilities.

Recovery - Restore affected systems and networks to normal operations, ensuring they are no longer compromised before reconnecting them.

Lessons Learned - Analyze the incident and the response to identify lessons learned and make improvements to prevent or better respond to future incidents.

4.0 COMPLIANCE

Failure to comply with this procedure may result in disciplinary action, up to and including termination of employment for staff, and termination of contracts for third parties. Any exceptions to this policy must be approved by the MDSAB Board of Trustees.

Part J – DEVICE SECURE CONFIGURATION PROCEDURE

1.0 PURPOSE

The Device Secure Configuration Procedure's primary purpose is to establish the standard practices for configuring and managing all computing devices used by Moosonee District School Area Board (MDSAB) to ensure that the data, networks, and systems remain secure and protected.

2.0 SCOPE

This procedure applies to all MDSAB owned and controlled devices including but not limited to computers, laptops, tablets, mobile phones, printers, and network equipment.

3.0 PROCEDURE

3.1 Device Configuration

3.1.1. All devices should be set up according to industry-accepted system hardening standards.

3.1.2. Default passwords must be changed before any device is deployed on the network.

3.1.3. Devices must be configured to automatically lock when left unattended for a period of 15 minutes.

3.2 Software and Updates

3.2.1. All software must be legally licensed and purchased from reputable vendors.

3.2.2. The IT department will regularly apply system and software updates to ensure that devices have the latest security patches.

3.3 User Access

3.3.1. Administrative privileges on devices should be limited to IT staff only.

3.3.2. User access to devices should be controlled via unique usernames and strong passwords.

3.4 Network and Internet Access

3.4.1. All devices should be configured to connect to the designated secure school network.

3.4.2. Firewalls must be enabled on all devices to block unauthorized access.

3.5 Anti-Malware

3.5.1. All devices should have anti-malware software installed, which should be updated regularly by the IT department.

3.6 Mobile and Portable Devices

3.6.1. Mobile and portable devices that store sensitive data must be encrypted.

3.6.2. Remote wipe capabilities should be enabled where possible to protect data in case of loss or theft.

Part K – 3RD PARTY VENDOR SECURITY PROCEDURE

1.0 PURPOSE

The purpose of this Third-Party Vendor Security Procedure is to ensure that all third-party vendors employed by Moosonee District School Area Board (MDSAB) align with our established information security and confidentiality standards. This policy outlines guidelines and procedures that must be followed by vendors to protect sensitive data and information related to our students, staff, and operations.

2.0 SCOPE

This procedure applies to all vendors, contractors, suppliers, or any other external entities who have access to MDSAB's information systems, networks, or data, and it is inclusive of all products, services, or solutions provided.

3.0 PROCEDURE

3.1 Pre-Engagement

3.1.1. All vendors must undergo due diligence which includes a review of their security policies, procedures, and controls.

3.2 Data Protection

3.2.1. Vendors must comply with applicable laws and regulations regarding data privacy and protection.

3.2.2. Data sharing with vendors should be limited to what is necessary for them to perform their agreed-upon service.

3.2.3. Vendors should use industry-standard encryption methods for data in transit and at rest.

3.3 Access Controls

3.3.1. Vendors should only have access to the data and systems necessary to perform their service.

3.3.2. Multi-factor authentication (MFA) is required for any remote access to MDSAB systems or data.

3.3.3. Vendor access rights will be terminated immediately upon the end of the contract or if a security risk is identified.

3.4 Incident Management

3.4.1. Vendors must report any incidents or suspected incidents that could impact MDSAB within 24 hours.

3.4.2. Vendors are required to have an Incident Response Plan and must coordinate with MDSAB's Incident Response Team in case of a security incident.

3.5 Audit and Compliance

3.5.1. Vendors should be reviewed annually to ensure that they are in compliance with the latest version of this procedure.

4.0 Policy Compliance

Failure to comply with this procedure by a vendor could result in contract termination.

Part L – MOBILE DEVICE SECURITY PROCEDURE (BYOD)

1.0 PURPOSE

The purpose of the Mobile Device Security Procedure (BYOD) is to establish procedures to secure any Bring Your Own Device (BYOD) equipment that accesses Moosonee District School Area Board (MDSAB) systems, networks, or data to maintain confidentiality, integrity, and availability of information.

2.0 SCOPE

This procedure applies to all employees, contractors, and third parties who use their personal mobile devices to access MDSAB systems, networks, or data.

3.0 PROCEDURE

3.1 Device Registration

3.1.1. The IT department must be able to document all connected devices.

3.2 Device Security

3.2.1. All BYOD devices must have the latest operating system and application updates.

3.2.2. All BYOD devices must be password protected and configured to auto-lock after a period of inactivity.

3.2.3. All BYOD devices must have remote wiping capabilities in case of device loss or theft.

3.3 Network Access

3.3.1. BYOD devices must only connect to the school board systems via secure and authorized methods.

3.3.2. All network connections made by BYOD devices should be encrypted, using technologies such as VPN, to protect information in transit.

3.4 Data Management

3.4.1. Sensitive data should not be stored permanently on BYOD devices.

3.4.2. Any sensitive data temporarily stored on a BYOD device must be encrypted.

3.5 Compliance

3.5.1. Users are expected to immediately report any suspected or actual breach of this procedure to the IT department.

3.5.2. Non-compliance with this procedure may result in the temporary or permanent disconnection of the device from school board systems.

REFERENCE DOCUMENTS

Legal:
Education Act, Section 169.1 Positive School Climate
Education Act, Section 265 Duties of Principal: Discipline and Care of Pupils and Property
Education Act, Part XIII Behaviour, Discipline and Safety
Ontario Regulation 298 Operation of Schools, section 11: Duties of Principals
Ontario Regulation 298 Operation of Schools, section 20: Duties of Teachers
Ontario Regulation 298 Operation of Schools, Section 23 Requirements for Pupils
Policy/Program Memorandum No. 128 The Provincial Code of Conduct and School Board Codes of Conduct
PPM No. 144 Bullying Prevention and Intervention
PPM No. 145 Progressive Discipline and Promoting Positive Student Behaviour
Ontario Human Rights Code
Criminal Code
Copyright Act
Municipal Freedom of Information and Protection of Privacy Act
Personal Health Information Protection Act

Board:
Board Policy GOV-01 Philosophy, Goals, and Values
Board Policy GOV-03 Role of the Corporate Board: Fiscal Responsibility
Board Policy GOV-04 Role of the Supervisory Officer
Board Policy GOV-08 Safe Schools
Board Policy GOV-13 Equity and Inclusion
Administrative Procedure 190 Information Security
Administrative Procedure 245 Effective Use of Technology
Administrative Procedure 376 Progressive Discipline: Students
Administrative Procedure 378 Suspension
Administrative Procedure 382 Expulsion
Administrative Procedure 480 Progressive Discipline: Employees