Halton District School Board

Cyber Security and Data Protection

Administrative Procedure

Topic:	**Cyber Security and Data Protection**
Status:	**Active**
Effective:	January 2024
Revision Date:	New
Review Date:	January 2025
Responsibility:	Superintendent of Information Services

Intended Purpose

1. Information and information systems, like physical infrastructure and financial resources, are critical Halton District School Board (HDSB) assets, and shall be safeguarded deliberately, appropriately, and consistently throughout their life cycles.
2. Cyber protection shall be provided in a manner that serves the security and safety of HDSB students and staff while adhering to legislative requirements.
3. Cyber risk management is a shared responsibility between HDSB officials, school administrators and Information Services. Accountability for cyber risks shall rest with the Director of Education and the Superintendent of Information Services.
4. Appropriate safeguards shall be in place to ensure the protection of students' and staff privacy and their safety online. The effort taken to apply these safeguards shall be proportionate to the possible harm or injury that could result if confidentiality, integrity and availability are not assured.
5. Per the Responsible Use of Information and Communication Technology (ICT), all students and staff shall be responsible for ensuring safe and ethical online behaviour and understand their accountability for the protection of information that is received, created, or maintained on behalf of the HDSB.
6. The HDSB, schools, and all staff have a duty of care to take reasonable steps to protect students from harm encountered within the online learning environment.

Halton
District
School
Board

Cyber Security and Data Protection

Administrative Procedure

Scope

1. This procedure applies to:
   - all HDSB departments, schools, staff, trustees, volunteers, and students that use HDSB Information and Information Technology (I&IT) resources including but not limited to HDSB devices, infrastructure, and applications;
   - HDSB visitors (including parents/guardians and rental parties) that have been authorized to use HDSB I&IT resources;
   - all vendors, contractors, and other third-party individuals and organizations that have been authorized by the HDSB to have access to HDSB I&IT resources; and
   - individuals and organizations that have been authorized by the HDSB to have access to the HDSB's network-connected Operational Technology (OT) resources.
2. The requirements of this administrative procedure also apply in situations where information is created, processed, transmitted, or stored by contracted third party service delivery partners and their subcontractors including but not limited to metadata and customer-derived data.
3. Contracts and service level agreements with third party service providers who have access to or share custody of HDSB information and/or information systems shall include the obligation to follow the requirements of this Administrative Procedure (AP) as applicable. This shall extend to any sub-contractors on whom the service providers rely to deliver services to the HDSB.
4. HDSB Information and Information Technology (I&IT) resources include but are not limited to HDSB information, HDSB devices (including but not limited to phones, laptops, tablets, and networked printers), HDSB servers, other HDSB infrastructure, and applications and contracted cloud services and applications.
5. HDSB Operational Technology (OT) resources is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. It includes building facilities automation equipment which are increasingly internet connected (e.g. Industrial Internet of Things (IIoT), building sensors, key scan cards, and both HVAC and HVAC control systems (Building Automation System (BAS)).

Halton
District
School
Board

Cyber Security and Data Protection

Administrative Procedure

Guiding Principles

Cyber Protection Standards

Cyber Protection is the term used to collectively describe the following three areas:

- **Cyber Security** which refers to the protection of information and information technology (I&IT) resources with respect to confidentiality, availability and integrity, and secure network-connected OT resources;
- **Cyber / Online Safety** which refers to the promotion of safe online practices and the mitigation of the risks associated with the inappropriate use of technology in accordance with the HDSB's Responsible Use of Information and Communication Technology (ICT) Administrative Procedure; and
- **Digital / Online Privacy** which refers to the protection of Personal Information (PI), Personal Health Information (PHI), and other HDSB sensitive information from unauthorized access and recognizes the importance of guarding personal and sensitive information when using technology.

To achieve these objectives, the HDSB is committed to each of the following principles as outlined below in this AP:

- **Cyber Protection Strategy / Roadmap** which defines the HDSB's plan to improve cyber protection in the HDSB and its overall approach to managing cyber risks to the HDSB's K-12 technology ecosystem and its users.
- **Cyber Protection Tools, Standards, Procedures and Guidelines** which defines specific mandatory or recommended measures (also commonly referred to as safeguards or "rails") to defend against cyber threats, producing a reliable foundation for cybersecurity, cyber safety, and privacy protection for the HDSB and its staff and students.
- **Cyber Protection Assurance** which refers to continually assessing the adequacy and efficacy of cyber protection measures in protecting the HDSB and its staff and students from current and evolving cyber threats.

Cyber Protection Strategy / Roadmap

1. The HDSB shall establish and maintain a multi-year cyber protection strategic plan for implementing and improving cyber security across the organization.
2. The HDSB shall ensure that:

a. appropriate technical and administrative safeguards are implemented to secure HDSB I&IT and network-connected OT resources to a degree that is consistent with the cyber protection requirements outlined in this Administrative Procedure and as may be outlined in other applicable HDSB policies, procedures, or legislation; and
b. users of HDSB provided technology are informed or trained on the HDSB's Responsible Use of Information and Communication Technology (ICT) Administrative Procedure and on safe and appropriate online practices

3. The HDSB is committed to adopting CIS Critical Security Controls (CIS Controls), adhering to the requirements of the provincial Cyber Security Wellness Architecture (CSWA) and meeting the standards set out in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 Core and Reference Architecture (RA) 3.0.
4. The HDSB is committed to a process of continuous monitoring, assessment, reflection, renewal, and improvement as Cyber Protection standards continue to evolve.

Cyber Protection Tools, Standards, Procedures and Guidelines

1. Cyber Risk Management

With increased reliance on technology, digital processes and the internet, the HDSB recognizes that cyber risks have the potential to affect all aspects of the HDSB, its staff and students, and its reputation.

The HDSB recognizes cyber risk management as an important practice that enables the HDSB to align cyber security, cyber safety, and digital privacy with HDSB strategic priorities and operational plan initiatives while effectively mitigating cyber risks to the HDSB's assets and operations. Cyber risk management follows the HDSB's risk management framework, which informs all strategic, operational, and budget decisions.

As an integral part of cyber risk management, Information Services shall classify I&IT and network-connected OT assets to determine the level of information sensitivity and risk to the assets and the appropriate levels of safeguards needed to protect them. The classification level shall be determined by assessing the requirement for confidentiality of information, integrity, and availability of information and systems.

Any new or renewed I&IT solutions and network-connected OT solutions in the HDSB shall undergo an assessment of cyber risks prior to entering into a contract or service agreement and prior to implementation and/or renewal.

For cloud services, the assessment may be of evidence in the form of an attestation providing reasonable assurance regarding the presence and correct operation of safeguards within a service.

Information Services shall do a re-assessment of cyber risks if there are any significant changes to the HDSB's I&IT posture, solution, network-connected OT solution, and/or the K-12 threat environment, and/or when deemed necessary.

All identified risks shall have a designation of who is responsible for their treatment, management and oversight with the Director of Education being ultimately accountable for all cyber risks in the HDSB.

Depending on the nature of the identified risk, responsibility for its risk treatment plan and its implementation or remediation may reside with Information Services, the business owner, the service owner, the service provider, and/or the vendor.

2. Onboarding, Offboarding, Device Recovery & Access Revocation

In collaboration with Human Resources, Information Services shall ensure new hires and those in new positions and/or new roles in the HDSB are assigned privileges, granted access and undertake security training commensurate with the duties they will perform prior to being granted access to HDSB sensitive information, information systems, and any HDSB owned and managed I&IT or network-connected OT resources.

In collaboration with Human Resources, Information Services shall ensure authorized users of HDSB I&IT and network connected OT resources:

1. are aware of their cyber protection responsibilities;
2. adhere to the HDSB's cyber protection standards, procedures and guidelines as applicable to their role(s); and
3. receive cyber protection awareness training commensurate with their role(s) and level(s) of access; and
4. receive privacy training commensurate with their role(s) and level(s) of access.

At the time of retirement, resignation, leave, or termination of employment, Human Resources will collaborate with Information Services to ensure timely processes are in place to retrieve HDSB devices as required and disable access to HDSB accounts and resources.

In the case of a leave or secondment of 12 months or less, employees may retain their HDSB assigned devices (including cell phones if applicable) and will maintain access to their HDSB Gmail account, Google Drive, and designated application(s) for training, pay and benefits.

In the case of a leave or secondment greater than 12 months in length, all HDSB assigned devices must be returned to Information Services. Employees will maintain access to their HDSB Gmail account, Google Drive, and designated application(s) for training, pay and benefits.

In the case of retirement, all access to HDSB accounts and resources will be terminated after 15 calendar days.

In all cases of resignation or termination of employment, access to any and all HDSB accounts and resources will cease with immediate effect.

Requests for exceptions to the requirements detailed above must be directed to and obtain the express written approval of the Superintendent of Information Services.

3. Cyber Awareness and Data Protection Training

Information Services shall conduct mandatory, regular and ongoing cyber awareness and data protection training (cyber security, cyber safety, and online privacy) for authorized users of the HDSB's I&IT resources and network-connected OT resources.

Education will include digital literacy and citizenship awareness training for both staff and students.

Training for staff shall be role-based and provide clarity on user responsibilities and expectations with respect to:

1. protecting HDSB I&IT and network connected OT resources;

2. protecting privacy and confidentiality, including complying with regulations and legislation;
3. adhering to the HDSB's Responsible Use of Information and Communication Technology (ICT) Administrative Procedure which includes expectations of appropriate online behaviour, expected practices with respect to physical security and the safe, responsible, and secure use of HDSB technology; and
4. adhering to the HDSB's cyber protection standards, procedures, and guidelines.

4. Identity and Access Management (IAM)

The HDSB will implement identity and access management (IAM) programs to ensure only authorized individuals are provided access to HDSB information, systems and networks. The following three steps will be required for an employee to access the HDSB's infrastructure:

1. identification (e.g. username, Employee ID);
2. two or more authentication factors (i.e. password and Multi Factor Authentication (MFA)); and
3. authorization / validation.

Single Sign On (SSO)

Information Services will facilitate and prioritize employee Single Sign On functionality wherever possible subject to security, software and operational limitations.

Account Monitoring

Information Services will conduct regular monitoring of employee accounts to identify and remediate (a) unauthorized access and/or (b) inaccurate permissions or privilege creep in violation of the Principle of Least Privilege.

Account reviews shall be conducted on a regular basis by Information Services under the direction of the Manager of Cyber Security and in collaboration with other departments as necessary.

5. Network and Cloud Security

Secure Access Service Edge (SASE)

The HDSB shall adopt and implement the principles of SASE as the core tenets of its security architecture framework in order to offer optimized and secure network services across individual users, premises, edge, remote and public/private cloud environments. SASE is comprised of five key networking and security technologies:

1. Software-defined Wide Area Network (SD-WAN);
2. Firewall as a Service (FWaaS);
3. Cloud Access Security Broker (CASB);
4. Secure Web Gateway; and
5. Zero Trust Network Access (ZTNA)

New programs, software, systems and other technology will not be considered for procurement and deployment in the HDSB if they are not compliant with SASE requirements and CIS Controls unless an exception is approved by the Superintendent of Information Services.

Zero Trust Network Access (ZTNA)

The HDSB shall operate in a “Zero Trust” environment and adopt a posture of “assume compromise” whereby all systems will deny access by default and eliminate implicit trust under the assumption that all accounts and devices are potentially compromised.

Only trusted individuals and devices will be permitted to access the HDSB network and other infrastructure.

Unauthorized Networks & Communication Tools

All HDSB wireless access points, network connected devices, network-connected OT resources and internally or externally hosted applications (including cloud services) shall conform with HDSB standards, procedures, and guidelines.

Unauthorized networks, rogue access points, and/or unapproved communication tools at local schools and other HDSB sites including but not limited to unapproved wireless access points, connected devices, equipment, and/or remote connections (e.g. VPN or SSH tunnels) are strictly prohibited.

Unauthorized wireless access points, connected devices, equipment, and/or remote connections (e.g. VPN or SSH tunnels) shall be the subject of site audits and scanned for and disabled upon discovery.

The HDSB shall not permit its networks to have open access except for managed guest networks that are isolated from the HDSB's other network segments by reliable means.

Access Control, Authentication & Authorization

HDSB staff and any other individual requiring access to sensitive HDSB information, IT systems and network-connected OT systems shall first be authorized through a HDSB approval process.

User access shall be granted and/or terminated immediately upon receipt of a documented access request/termination with the approval of the Superintendent of Information Services or designate.

Multi Factor Authentication

All staff users will be required to authenticate using an approved Multi Factor Authentication (MFA) application as the primary means of personal authentication.

The HDSB shall make available an alternative method of authentication for employees who require an alternate means of MFA.

Principle of Least Privilege (PoLP)

The Principle of Least Privilege (PoLP) shall be applied to all staff across the organization regardless of role. Access privileges shall be enough to enable an individual to perform their role but not permit them to exceed their authority.

HDSB user accounts with elevated privileges shall be subject to continuous account monitoring for inaccurate permissions, privilege creep, and/or unauthorized use of permissions. Super User access shall be tightly controlled and monitored and subject to regular and ongoing monitoring, assessment, and auditing.

Auditing of access and usage of users' accounts shall be conducted regularly and on an ongoing basis by the Manager of Cyber Security and Data Protection with the approval and under the supervision of the Superintendent of Information Services to prevent and detect/identify incidents of privilege abuse, unauthorized access, and/or privacy breaches.

Information Services has developed a Privileged Account Management (PAM) Protocol to establish guidelines and procedures for the secure management and control of privileged accounts within the HDSB.

<u>Network Segmentation / Microsegmentation</u>

The HDSB will implement network microsegmentation for staff, student, public, and vendor use as a critical element of its Zero Trust posture.

Networks may be further segmented by purpose, department, and/or user group for reasons of security.

<u>Approved Devices & Device Authentication</u>

Technology can be vulnerable to hacking and other cyber security threats if it is no longer supported by its vendor or updated by its owner/user with regular security updates.

Change and configuration management are critical elements of the HDSB's cyber security posture. Only devices configured and managed through Information Services will be permitted on any secured HDSB infrastructure. Devices that are not configured and managed through Information Services and/or meet a minimum security standard will not be permitted to operate on any secured HDSB infrastructure (including HDSB networks) and will not have access to sensitive data, applications, and systems.

Personal devices that do not meet minimum security standards including the latest updates and virus definitions and/or are unable to authenticate to the standard set by Information Services will only be permitted on the HDSB's public network.

6. Endpoint Detection & Response / Extended Detection and Response (EDR/XDR)

Effective EDR strategies enable Information Services to:

1. detect security incidents;
2. contain incidents that have been detected;
3. investigate and respond to incidents that have been detected; and
4. remediate endpoints to their state prior to compromise.

Information Services shall implement reliable, enterprise-grade controls for the HDSB network to regulate all traffic moving within the HDSB network and between the HDSB and external, untrusted (internet) entities (e.g. cloud service providers).

Information Services shall encrypt sensitive HDSB data at rest and/or in transit as an important measure to mitigate against unauthorized access to information.

Information Services shall implement protective measures and controls to procure, monitor, and secure endpoint devices and reduce the risk of cyber incidents and breaches from endpoint devices connected to the HDSB network.

Privacy and Data Protection

The HDSB recognizes the need to differentiate the data of children (minors) from that of adults and accepts that additional and/or different privacy safeguards may be needed for minors.

The HDSB shall take appropriate measures to ensure the confidentiality, integrity, and availability of sensitive information including but not limited to:

1. sensitive business information such as HDSB financials and contracts
2. personnel matters;
3. the Personal Information of students and staff; and
4. the Personal Health Information of students and staff.

The HDSB is committed to protecting the privacy of and safeguarding access to student and staff PI and PHI held by the HDSB and to following rules for collection, retention, use, and disclosure as required by legislation and detailed in the Records Management Administrative Procedure.

All individuals with access to student and staff PI, PHI and other HDSB sensitive information shall be required to comply with applicable HDSB policies, standards, procedures (see Records Management Administrative Procedure), and guidelines and abide by all applicable privacy laws and legislations.

Technology, software, and other applications unable to meet the HDSB's standards for privacy, security and/or data protection as determined by Information Services will not be authorized for use by students and/or staff and will not be permitted access to HDSB infrastructure (including HDSB networks), sensitive data, applications, and systems.

Data Loss Prevention (DLP)

Information Services shall implement Data Loss Prevention (DLP) capabilities to identify, monitor and protect data in use, in motion and at rest. DLP tracks data moving within the network, on employee devices, and when stored on corporate infrastructure.

To prevent end users from accidentally or maliciously sharing data that could put the organization at risk, DLP capabilities are designed to detect and prevent the unauthorized access, use and transmission of information by ensuring end-users do not send sensitive or confidential data outside the organization without proper authorization. DLP will send an alert, change permissions for the data or, in some cases, block the data when it is in danger of leaving the corporate network. Wherever possible, such measures will be automated.

Under no circumstances should an employee transfer and/or back up HDSB data from their HDSB account to a personal account without the express written approval of the Superintendent of Information Services.

Questions with respect to data loss prevention should be directed to Information Services.

Vulnerability & Patch Management

Information Services will create and maintain an asset inventory to track the HDSB's I&IT, infrastructure, applications, and network-connected OT assets in order to quickly identify, assess impacts, mitigate vulnerabilities, and promptly deploy patching and other security remediation.

Decisions as to the timing and implementation of patching and vulnerability mitigation shall rest with Information Services.

7. Physical Security & Cyber Hygiene

With respect to cyber security and risk management, Information Services will utilize a combination of audits, surveys, vulnerability assessments, and other industry practices to monitor, assess, test, and remediate matters pertaining to the physical security of HDSB workspaces, premises, infrastructure, and resources. Information Services will collaborate with other departments as necessary to assess and remediate security concerns.

Physical security is a shared responsibility among all stakeholders. The HDSB is committed to ensuring a safe working environment for all students and staff. With respect to cyber security and risk management, all employees are expected to operate in a physical Zero Trust environment and take precautions appropriate to their roles and functions. The protection of physical property encompasses both technical and nontechnical components.

All staff and students are expected to adhere to the physical and cyber security requirements as detailed in the Responsible Use of Information and Communication Technology (ICT) Administrative Procedure.

8. Working from Home / Remote Work

Employees working from home will comply with the HDSB Working From Home (WFH) Administrative Procedure, the Records Management Administrative Procedure, the Responsible Use of Information and Communication Technology (ICT) and the procedures detailed in this AP.

Sensitive data, applications and systems must be treated as confidential and not be exposed to unauthorized parties, including family members or other individuals in the same WFH location.

Staff working from home shall continue to operate in a Zero Trust environment, requiring all staff users to:

1. authenticate using multi-factor authentication (MFA) as the primary means of device authentication;
2. ensure the security of their home network; and

3. install on their device(s) all the required certificates, updates and other security requirements in order to access the HDSB's infrastructure (including staff networks) and sensitive data, applications and systems until such time as SASE is fully implemented as determined by Information Services.

Devices unable to authenticate to the HDSB's security standard will have restricted access to the HDSB's infrastructure (including staff networks), sensitive data, applications, and systems.

Systems unable to adapt to SASE requirements may not be available to users on personal devices.

9. Supply Chain, Cloud & Third Party Service Providers

The HDSB recognizes that cyber risks associated with a vendor's supply chain, third-party service providers, contractor, and cloud providers are important areas requiring coordinated risk mitigation efforts. Areas of third-party cyber risk include but may not be limited to:

- access by third-party service providers or vendors - virtual or physical access to HDSB technology, IT system, and sensitive information;
- suppliers;
- software, hardware, and cloud services with vulnerabilities, compromised systems, or embedded malware;
- cyber security vulnerabilities in supply chain management or supplier systems;
- third-party data storage or data aggregators; and
- contract terms and conditions, including provisions around data privacy, incident response, and the vendor's overall cyber security and privacy practices.

In collaboration with Information Services and other departments where applicable, Business Services shall include cyber security, cyber safety, and privacy requirements in new and renewed technology procurements to ensure appropriate levels of information and user protection are in place.

Information Services shall institute cyber risk assessment practices as a key step in the procurement of technology, cloud services, and IT services to ensure adequacy of cyber security, cyber safety, and privacy controls.

Contracts and service level agreements with third-party service providers (including any sub-contractors) who have access to or share custody of HDSB information, IT systems, and/or other HDSB technology shall include the obligation to follow the requirements of this administrative procedure and applicable HDSB standards, procedures and guidelines, or be subject to equivalent industry-based assurances.

10. Software and Technology Catalogue & Approved Applications

Information Services shall maintain and update its Software and Technology Catalogue to protect staff and student personal information and HDSB data. The Software and Technology Catalogue will detail software applications approved for use by staff and students, on the HDSB network and/or on HDSB devices.

Unless otherwise approved by Information Services, HDSB staff shall only use applications and software identified and approved in the Software and Technology Catalogue. Any applications or technology not approved for use in the Software and Catalogue must not be used by staff and students on HDSB devices and/or the HDSB infrastructure (including HDSB networks) and will not have access to sensitive data, applications, and systems.

To determine inclusion or exclusion from the Software and Technology Catalogue, all applications shall be subject to an application vetting process to assess need, pedagogical value, procurement requirements, technical compatibility, privacy risks, and data and/or operational security risks.

No piloting or use of software or programs, free or otherwise, may occur without the express written approval of Information Services.

Staff shall be held accountable when their actions contravene HDSB standards, procedures and guidelines.

11. Incident and Breach Response Planning, Management, Response and Recovery

The requirements of the NIST 2.0 Framework require organizations to include procedures, practices, and protocols to address the following with respect to threats to the HDSB:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Accordingly, Information Services shall develop and maintain playbooks, including but limited to Ransomware and Cyber Incident playbooks, which will include as applicable:

1. incident and breach response plan(s) including the activation of a Secure Operations Centre (SOC);
2. incident and breach management procedure(s) that include definitions for metrics (e.g. severity classification based on the NIST framework, response timelines, etc.), terms used, accountability, and the roles and responsibilities;
3. direction for the coordination of HDSB staff, the establishment of a Security Operations (SecOps) team comprised of both Information Technology Operations and Information Services Security staff and the inclusion of other HDSB departments as necessary (e.g., Facilities, HR, Business Services, Communications and Engagement);
4. protocols and the use of automated systems for detecting, containing, monitoring, eradicating, and recovering from cyber incidents and breaches;
5. escalation procedures and escalation contacts including legal and external forensic support; and
6. a comprehensive review of the lessons learned as a result of the incident.

The HDSB will employ automated detection and response capabilities to monitor, detect, and remediate potential or actualized cyber incidents and breaches on HDSB networks, devices/endpoints, systems/applications, network-connected equipment, and platforms. While every effort will be made to minimize impacts to users and, the priority of automated systems and the SecOps team will be to respond to and eradicate threats to the HDSB. Depending on the nature and severity of an identified threat, immediate action may be necessary or recommended.

Information Services shall ensure users of the HDSB’s I&IT and network-connected OT resources are made aware of how to identify and report a cyber incident or breach.

Any person who causes or contributes to cyber incidents or breaches shall be held accountable when their actions contravene HDSB standards, procedures, and guidelines.

12. Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

Information Services shall define, for all business and time critical IT systems, business requirements and metrics for availability, reliability, and continuity of service to inform business continuity and disaster recovery plans.

Information Services shall put in place, for all business and time critical IT systems, a Disaster Recovery Plan (DRP) to support continuity of business and timely recovery of IT systems in the event of a significant degradation of service or unplanned outage.

The DRP shall be the responsibility of Information Services and align with the Business Continuity Plan (BCP) as developed and owned by the business owners of the IT systems across the HDSB. The BCP will help define the business requirements for the DRP.

The DRP shall be subject to regular reviews to ensure the plan is up to date and can be successfully executed in the event of a disruptive event or major failure.

Information Services shall implement and regularly test backup and off-site storage procedures and capacities for all essential business information and critical IT systems no less than every 12 months, in the event data and IT systems need to be restored.

Cyber Protection Assurance: Monitoring, Assessing, and Auditing

Information Services shall monitor risk compliance for I&IT and network-connected OT resources deemed critical to the HDSB. This may be done in the form of cyber risk assessments, penetration tests, vulnerability assessments, privacy impact assessments (PIAs), phishing campaigns, tabletop exercises, audits (both remote and on site), and other industry established practices.

HDSB networks, devices/endpoints, systems/applications, network-connected equipment, and platforms shall be monitored to detect and prevent potential cyber incidents and breaches in accordance with legislation.

Monitoring and assessments including but not limited to cyber risk assessments, penetration testing, vulnerability assessments, PIAs, tabletop exercises, audits, and other industry established practices may be conducted centrally across the organization or locally at specific sites or with specific user or staff groups as approved by the Superintendent of Information Services in consultation with the Manager of Cyber Security and Data Protection.

Staff shall be held accountable when their actions contravene HDSB standards, procedures and guidelines including the direction detailed in this AP.

Access to and analysis of monitoring data shall be restricted to authorized personnel only as determined by the Superintendent of Information Services in consultation with the Manager of Cyber Security and Data Protection.

Exceptions

Information Services shall develop an exception request process that ensures any requested deviations to the policy and standards are remediated within an established timeframe.

Any requests for deviations from defined security configurations shall be directed to the Superintendent of Information Services.

Exceptions must be approved through a change management process and documented as follows:

1. standard/requirement/product that requires an exception;
2. reason(s) for noncompliance with the requirement;
3. business and/or technical justification for the exception;
4. scope and duration of the exception;
5. risks associated with the exception;
6. description of any compensating controls that mitigate risks associated with the exception;

7. identification of any unmitigated risks; and
8. detail a plan for achieving compliance.

The Superintendent of Information Services shall collaborate and coordinate with other departments as necessary when considering requests for exceptions.

Halton
District
School
Board

Cyber Security and Data Protection

Administrative Procedure

Reference number: Pending

Cross-Reference:

Board Policies, Procedures & Protocols

Board Assigned Mobile Cellular Device Administrative Procedure
Cyber Security and Data Protection Policy
Electronic Monitoring Administrative Procedure
Privacy and Information Management Policy
Privacy Breach Protocol Administrative Procedure
Records Management Administrative Procedure
Responsible Use of Information and Communication Technology (ICT) Administrative Procedure
Risk Management Administrative Procedure
Risk Management Policy
School, Staff and Student Websites Administrative Procedure

Industry Standards

Guide to the NIST Cybersecurity Framework: A K-12 Perspective
NIST K-12 Cybersecurity Self Assessment
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations