Chinook's Edge School Division - Administrative Procedures

AP 1-29 Information Systems Security Management - NEW

Related Polices:	**Initial Approval:** 2014 January 14
Related Procedures:	**Last Amended:** 2021 September 21
Exhibits:	**Last Reviewed:** 2021 September 21

OVERVIEW

Chinook's Edge School Division (the Division) recognizes that technology systems and information are valuable assets which are essential in supporting its strategic objectives. The Division accepts its obligations to protect information from all threats and that effective information security is critical in ensuring the successful enablement of learning and delivery of business functions and services. The division is committed to an Information Security Management administrative procedure that not only preserves the confidentiality, integrity and availability of all physical and electronic assets but attempts to minimize distractions to learning.

Chinook's Edge School Division is committed to the Information Security Management System, and shall ensure that this administrative procedure is communicated, understood, implemented and maintained at all levels of the organization and regularly reviewed for continual suitability.

PURPOSE

This administrative procedure details the division's approach to Information Systems Security Management. The approach is based upon recommendations contained within ISO27001 (a code of practice for information security management) and the Government of Alberta School Technology Framework.

Information security management procedures focus on continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorized access or manipulation and is vital for the protection of information, staff, students and the division's reputation.

SCOPE

The ISMS Security Administrative Procedure applies to:

1. Information systems owned by, or under control of, Chinook's Edge School Division;
2. Information in storage, in use or at rest on Division information systems;
3. Information in transit across the Division's digital networks;
4. Control of information leaving the Division;
5. Information access control;
6. All parties using the Division's information systems and, information belonging to, or under the control of the Division including:
    - Superintendent
    - Board of Trustees
    - Senior Administration Team
    - Division employees
    - Contractors
    - Partner organizations
    - Parents
    - Students

- Volunteers

Application of the administrative procedure applies throughout the lifecycle of the information from creation/acquisition, utilization, transit, storage and disposal.

RISKS

Failure to adhere to this administrative procedure can result in the following:

1. Loss of Confidentiality of information;
2. Loss of information Integrity;
3. Risk to Student Safety;
4. Loss of Reputation.

Any of these outcomes can compromise Staff and Student safety and the Division's reputation. Additionally the Division may be exposed to fiscal loss.

PROCEDURES

The Superintendent, Board of Education, Senior Administration Team and all employees are committed to an effective Information Security Management System in accordance with its strategic organizational objectives and based on the principles of the School Technology Framework and ISO 27001.

To that end, the Superintendent shall ensure:

- Development and implementation of appropriate, practicable, measurable procedures and guidelines to protect the organization's information assets from all threats both internal and external.
- Direction and support for information security.
- Definition and designation of responsibilities to all users of the Division's information systems.
- Fostering stakeholder confidence by acting in accordance with security standards.
- Continual improvement of the Information Security Management System through the establishment and regular review of measurable security objectives at relevant functions and levels of the organization.
- Commitment to comply with business and legal regulatory requirements and contractual security obligations.
- Systems for protection against unauthorized access.
- Confidentiality of data.
- Development, implementation, and testing a Business Continuity Plan
- Creation of mechanisms to identify and review the risk and impact of breaches in protected information versus the needs of staff and student learning.
- Communication of all pertinent security policies to students, employees and other interested parties as applicable through the Division ISMS procedures documents.

<u>Security Awareness</u>

The division is committed to promoting safe working practices. All employees will be made aware of the need for security to a level commensurate with their role. Relevant ISMS procedures and guidelines will be accessible to all users. It remains the employee's responsibility to ensure they are adequately informed of ISMS procedures and policy changes.

<u>Business Continuity</u>

The Division will develop and maintain a Business Continuity Strategy based on specific Risk Assessment to maintain critical learning and business functions in the event of any significant disruption to critical services, systems or facilities.

Monitoring and reporting

The Division reserves the right to monitor the use of its information systems including email and Internet usage to protect the confidentiality, integrity and availability of the Division's information assets, ensure compliance with legal requirements and ensure student safety.

Risk Assessment

The Division will develop a Risk Management Strategy and the risk to the Divisions systems and information will be managed with reference to the Government of Alberta School Technology Framework.

Compliance

Chinook's Edge School Division will adhere to all legislation pertaining to information storage and processing including:

Alberta Freedom of Information and Privacy Act.
Alberta Human Rights Act.

Development of Procedures

Information Governance, development of specific administrative procedure and guidelines will be coordinated by the Technology Advisory Group and chaired by the Associate Superintendent, System Services.

Incident Reporting

All stakeholders are responsible for reporting any breach of administrative procedure or security incident to the Director of Technology. Details on reporting procedures are contained in the "Responsibilities and Procedures Security Incidents" Procedure.

POLICY GOVERNANCE

The following table identifies who within CESD is Accountable, Responsible, Informed or Consulted in regards to this administrative procedure. The following definitions apply:

- **Responsible** - the person(s) responsible for developing and implementing the Policy.
- **Accountable** - the person who has ultimate accountability and authority for the Policy.
- **Consulted** - the person(s) or groups to be consulted prior to final Policy implementation or amendment.
- **Informed** - the person(s) or groups to be informed after Policy implementation or amendment.

Responsible	Associate Superintendent, System Services
Accountable	Superintendent, Board of Trustees
Consulted	Technology Committee, Director Technology Services
Informed	All Employees, Contractors, Board, Parent, Students, Partner Organizations, Volunteers

REFERENCES

Alberta Freedom of Information and Privacy Act
Personal Information Protection Act
Alberta Human Rights Act

HISTORY

Approved:	2014 Jan 07
Reviewed:	2018 July 03
Reviewed:	2019 Nov 25