EDMONTON PUBLIC SCHOOLS

Administrative Regulation

CODE: CNA.AR

TOPIC: Security of Personal and Division Information

EFFECTIVE DATE: (03-05-2007)

ISSUE DATE: (12-09-2021)

REVIEW YEAR: (2028)

OBJECTIVE

To endeavour to ensure that the legitimate use and flow of information for educational and business purposes is balanced with adequate protection of information and information systems against damage, loss and unauthorized use, disclosure or modification.

To establish roles and responsibilities and define expected cybersecurity outcomes.

DEFINITIONS

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

The **Cybersecurity Services Program** is a Division initiative that coordinates the effort to protect the Division's information systems. The Cybersecurity Services Program will work with all departments who manage information systems to address the following security pillars:

- Strengthening and continuously hardening the Division's cybersecurity posture.
- Increasing information stakeholder awareness.
- Shifting security posture from reactive to proactive.

A **Cybersecurity Incident** is an event which could or did expose Division information or information systems to unauthorized access, damage, loss or theft.

Information Controller is the role assigned to those responsible for granting staff access to Enterprise information systems such as PeopleSoft, Finance Live, Powerschool.

RESPONSIBILITY

1. Technology and Information Management will manage the Cybersecurity Services Program, and endeavour to ensure broad participation in the program from all areas of the Division.
2. Decision Unit Administrators will assume or delegate the role of Information Controller for their respective enterprise information systems.
3. Information Controllers will review and approve information shared with third parties and will endeavour to ensure employees have authorized access to only the information and information systems that are required in order to fulfill their duties, in accordance with provincial standards.
4. Division employees who access Division information and IT systems shall take the responsibility to protect Division information and technology assets.

REGULATION

1. The Cybersecurity Services Program will:
   a. Develop and maintain an awareness and training program to endeavour to ensure that all staff are knowledgeable and engaged to protect Division information and networks.
   b. Assess and monitor the information system security vulnerabilities and threats to the Division on an ongoing basis and determine appropriate controls to mitigate the risks in consultation with relevant stakeholders.
   c. Develop and implement Division standards with respect to passwords, multi-factor authentication, access controls, encryption, confidentiality agreements, audit logs, privileged access and other relevant cybersecurity topics.
   d. Manage an incident response team, ensuring that appropriate stakeholders respond to cybersecurity incidents in a timely manner.
   e. Develop and maintain a reporting structure to endeavour to ensure that cybersecurity incidents, data breaches or possible risk of information disclosure are reported to the Division FOIP office on a priority basis and report relevant incidents to senior administration.
   f. Create a yearly report for the Board of Trustees based on an internal audit of Division information systems. The report will include physical security, network and application security and privacy incidents and an overview of the findings of the audit. Every fourth year the audit will be conducted in collaboration with an external auditor.

2. Information controllers will endeavour to ensure that information systems that they manage follow Division cybersecurity standards.

REFERENCES

CN.BP Managing Division Information
CN.AR Creation, Use and Maintenance of Division Information
CNA.BP Information Security
DK.BP Division Technology
DK.AR Division Technology Standards
DKB.AR Appropriate use of Division Technology
Provincial Approach to Student Information (PASI) Usage Agreement
Freedom of Information and Protection of Privacy Act
Education Act