NETWORK SECURITY

Background

Procedures and standards have been established to ensure the appropriate protection of the Division's information/data systems. The Division has in its possession confidential information/data that must be protected. This Administrative Procedure addresses the need for integrity of data throughout the Division's information system. This procedure supports Administrative Procedure 140 – Responsible Network Use and Administrative Procedure 141 – Information Security.

Procedures

1. All users of the Division's computer systems and network resources have the responsibility to ensure its overall security and to behave in a manner consistent with this security Administrative Procedure. Each user is responsible for understanding and complying with Administrative Procedure 140 – Responsible Network Use and Administrative Procedure 141 – Information Security.

2. The Director of Technology Services shall be responsible for establishing, maintaining, implementing, administering and interpreting network systems security procedures and standards. While responsibility for security of network systems on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for network systems security is centralized for all of the Division through the Director of Technology Services.

3. The Director of Technology Services shall:

   3.1 Provide backup services of all data systems;

   3.2 Ensure all Division owned computer systems have antivirus software installed, updated and enabled (if applicable).

4. Staff or students shall not:

   4.1 Establish network services onto any existing Division networks (e.g. personal web servers, FTP servers, news servers, electronic bulletin boards, RRS feeds, local area networks or Ethernet connections of any kind).

   4.2 Make any configuration changes or install any network devices that may have a negative impact on network performance/security.

5. Any Division owned technology that has been deemed surplus is to be decommissioned and properly disposed of by the Director of Technology Services.

6. Only personnel authorized by the Director of Technology Services shall install applications on servers or workstation.

7. Each user must have a unique network account with an encrypted password.

8. Network accounts may not be shared among multiple users without prior approval from the Director of Technology Services

9. Wireless Networks

   9.1 Shall have all wireless access points apply the latest security protocols;

   9.2 Shall utilize the latest encryption protocols; and

   9.3 Shall be administered by the Director of Technology Services.

10. Personally owned technology shall not be permitted onto the internal network unless approved by the Director of Technology Services. They are permitted on a separate wireless WiFi network provided to support personally owned devices.

Adopted/Revised: JUN 2016/NOV 2019/JAN 2023

Reference: Section 11, 31, 33, 52, 53, 196, 197, 222 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education
ATA Code of Professional Conduct