Clearview Public Schools
We All Belong – We All Succeed

Administrative Procedure 141 - Network Security

Background

Procedures have been established to ensure the appropriate protection of the Division's information systems. The Division has in its possession confidential information that must be protected. This Administrative Procedure also addresses the need for the integrity of data throughout the Division's information system.

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.

2. The Director of Technology Services and the Systems Analysts (SAs) have the same responsibilities as users, plus the additional responsibilities and privileges outlined below due to their administrative positions. Systems Analysts are expected to:

    2.1. assess the security of Division servers, workstations, network systems/resources and data to define and promote best practices regarding the security of data and systems;

    2.2. conduct vulnerability scans on a regular basis to ensure the security of Division servers, workstations, network systems/resources and data, and if necessary, prescribe a course of action to mitigate any vulnerabilities;

    2.3. investigate, evaluate and implement security related technologies, such as authentication/authorization mechanisms, encryption, certificate services, antivirus software, network monitoring equipment, and firewalls;

    2.4. assist in the resolution of serious security compromises, which may include cooperation with law-enforcement agencies, and provide assistance for recovery and security;

    2.5. establish appropriate user privileges, monitor access control logs, and perform similar security actions for the systems they administer;

    2.6. be adequately trained to provide network services for the network operating environment;

    2.7. help develop, maintain and test security procedure(s);

    2.8. help develop, maintain and test access control, backup and disaster recovery plans;

    2.9. take reasonable precautions to safeguard against corruption, compromise or destruction of data, computer systems, and network resources;

2.10. ensure user information is treated as confidential. It is recognized that an SA may potentially have contact with a user's files, email, etc., in the course of his or her duties. The contents of such files must be kept confidential. Access to a user's files is only authorized in the event of a security investigation or at the written request of the user;

2.11. take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on all computer systems and network systems;

2.12. subscribe to and implement appropriate vulnerability lists based on the network operating system and services they support;

2.13. participate in security training approved by the Director of Technology;

2.14. participate freely, from a "technical perspective", on any committee(s) or discussions that may have an impact on the information technology system.

3. Principals/site managers are responsible for ensuring that appropriate computer and communication system security measures are observed in their departments/schools. Principals/site managers are also responsible for making sure that all users are aware of Division procedures related to computer and information system security.

4. General Administration

4.1. each user must be made aware of and have access to the applicable policies and administrative procedures.

4.2. any individual aware of any breach of information, the information system or network security, including the compromise of computer security safeguards, must report such situations to his/her supervisor. If it is determined that a security breach has occurred, it must be reported in writing to the Director of Technology;

4.3. an SA must acquire prior approval from the Director of Technology before making any configuration changes or installing any network devices that may have a negative impact on network performance/security;

4.4. staff or students shall not establish their own personal local or wireless network or services such as: web servers, FTP servers, news servers, electronic bulletin boards, RRS feeds, local area networks, chat servers, proxy servers, game servers, wireless access points or modem connections to any existing Division local area networks, without written approval by the Director of Technology and their supervisor;

4.5. enterprise services, such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), Windows Internet Naming Service (WINS), firewalls, routing, E-mail, E-mail relay services, and Directory services are to be run in cooperation with IT department procedures and guidelines;

4.6. Security protocols, such as Internet Protocol Security (IPsec) and Secure Socket Layer (SSL) must be used whenever deemed appropriate;

4.7. Port scanning and packet sniffing are strictly prohibited without senior executive approval;

5. Physical Security

5.1. computing equipment shall be placed in an environmentally controlled location (e.g., temperature control, humidity, exposure to moisture, etc.);

5.2. servers and networking equipment must be stored in secure locations (server room, wiring closets, etc.) with restricted access only to the IT and Facilities department personnel as well as the Principal/site manager;

5.3. magnetic media, such as hard drives, diskettes, or tapes, must be erased before disposal;

5.4. a shredder must be used for the disposal of sensitive documents;

5.5. all networking devices and servers are required to be connected to an Uninterrupted Power Supply (UPS);

5.6. where appropriate, security access and authorization documentation for visitors, must be retained for a minimum of three (3) months;

5.7. mission critical data, or copies of it, is not to be stored in an unsecured area. Unsecured areas include but are not limited to laptop, portable storage device or a handheld device or paper copy.

5.8. Back-up servers shall not be on the same network as the production servers.

6. System Security

6.1. only personnel authorized by the Director of Technology shall install applications on servers or workstations;

6.2. administrative access to systems will be determined by the Director of Technology;

6.3. system configuration must be done in a safe manner. The system must have an appropriate level of security at all times;

6.4. whenever system security has been compromised or convincing reason to believe it has been compromised, the SA involved must immediately:

6.4.1. reassign all relevant passwords;
6.4.2. force every password on the involved system to be changed at the time of the next log-in; and
6.4.3. communicate and document his/her actions to Technology department staff and any other person(s) affected by the change;

6.5. wherever possible, operating systems and applications must be kept current with the latest operating system and application patches applied;

6.6. applications must be configured with security in mind;

6.7. security, account, and system level logging must be turned on when any server is set up;

6.8. all unneeded services must be turned off for network devices and computer systems;

6.9. the use of fault tolerant systems, such as disk mirroring and RAID array, is mandatory for all servers that store mission or business critical data and highly recommended for all other servers;

6.10. where appropriate, maintenance and service agreements with vendors must be kept current.

7. User Account Security

7.1. each user must have a unique user ID. An SA must be able to uniquely identify all users, including name, user ID, association, and location;

7.2. All “administrator” accounts and any remote access must use 2FA/MFA, and all “administrator” passwords to mission critical systems must be recorded, kept up to date and saved, both electronically and hardcopy, in a secure location for future reference;

7.3. each user’s profile must not be read, write or execute capable by other users. Permission to access shared resources is to be granted by site administrator only as needed;

7.4. accounts created for vendors to provide services must only be active during the time the service is carried out;

7.5. accounts must be reviewed annually to ensure that only valid accounts remain active;

7.6. if possible, failed login sessions must be terminated and the account locked after five (5) unsuccessful tries;

7.7. where possible, concurrent logins must be limited to one (1).

8. Terminations and Transfers

8.1. all significant changes in staff duties or employment status must promptly be reported to the Assistant Superintendent of Human Resources, who, in turn, will notify the Director of Technology to make the necessary changes to the user’s account;

8.2. computer access of terminated employees must be deactivated immediately upon notification from the Assistant Superintendent of Human Resources or the Superintendent.

9. Password Administration

9.1. all accounts must have assigned passwords;

9.2. users are never to reveal their password(s) to anyone else unless a school or Division authority asks for it.

9.3. an SA or any other staff member from the Technology department is prohibited from disclosing users' ID and/or passwords to anyone without appropriate authority;

9.4. a strong password is required, which could include alpha-numeric, capitalization and special characters. A minimum password length of 7 characters is required;

9.5. passwords are to be reset annually or more frequently if desired;

9.6. passwords must not be written down and left in a place where unauthorized persons might discover and use them;

9.7. all passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed, to anyone besides the authorized user;

9.8. all vendor-supplied default passwords must be changed before any computer or communications system is used;

9.9. user is never to use their network account password for access to other websites or programs.

10. Communications

10.1. encryption is to be used when a high degree of confidentiality is required for email communication;

10.2. any user requiring access to resources on the Division network from outside of the network must have approval from the Director of Technology.

11. Wireless Devices

11.1. a "wireless" connection is less secure and has less throughput than a "wired" connection; therefore, all wireless systems are to be viewed as a complement to a wired system and not as a replacement for a wired system;

11.2. it is mandatory for all wireless access points to apply the latest security protocols;

11.3. sensitive applications must not be hosted on wireless subnets or be transmitted over the wireless network;

11.4. no systems on wireless subnets are to store or transmit data of a sensitive nature such as credit card numbers, confidential student information, legal or attorney privileged data;

11.5. all users of wireless subnets must acknowledge these policies and agree to abide by them before access is granted to wireless subnets;

11.6. all wireless access points must be administered by Division Technology department personnel;

11.7. the Director of Technology and Superintendent must approve any exceptions to the above.

12. To assure continued uninterrupted service for both computers and the network, all computer systems must have Division approved antivirus software installed, updated and enabled at all times.

13. Backups

13.1. a SA, or backup administrator, must make sure that all scheduled backups are completed, monitored and tested for effectiveness. Systems are to be restorable after a failure due to loss of data or compromise within a reasonable period of time;

13.2. backups are to be stored in a secure environment;

13.3. critical operations data weekly backups must be stored in a secure environment offsite;

13.4. the number of sets and frequency of backups of a system are to be based on the risk analysis of the system, application, or data being backed up;

13.5. backup and restore procedures must be documented;

13.6. backup media must be tested periodically to determine its effectiveness.

14. Disaster Recovery

14.1. inventory of hardware, software, service agreements, vendor contacts, personnel information and responsibilities must be maintained;

14.2. the Disaster Recovery Plan (DRP) shall be reviewed annually by the Director of Technology;

14.3. The DRP manual will be located in the Division Office vault as well as a copy kept off site in a secure location.

15. This Administrative Procedure applies to all staff, students, consultants, temporaries, volunteers and any others who access the Division computer network. This Administrative Procedure also applies to all computer and data communication systems/equipment, whether owned and/or administered by the Division or not.

16. The Director of Technology shall, in conjunction with senior leadership, review this document on an annual basis.

Reference: Section 31, 32, 33, 52, 53, 196, 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

Effective: 2010-06-23
Amended: 2013-10-17; 2022-01-01