INFORMATION SECURITY

Purpose

The purpose of this Administrative Procedure is to define standards for protecting the Division's information, especially sensitive and personal information, from unauthorized collection, use, disclosure, retention or destruction.

This Administrative Procedure applies to all the Division's employees, contractors, vendors and agents with a Division-owned or personally-owned computer workstation or mobile device used to connect to the Division network. This Administrative Procedure applies to remote access connections used to do work on behalf of the Division, including reading or sending email and viewing intranet web resources.

This procedure applies to anyone using Livingstone Range School Division information including, but not limited to, employees, agents, appointees, consultants, contractors, persons on secondment, volunteers, practicum students, student teachers, exchange teachers and students.

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

Definitions

"Division" means Livingstone Range School Division.

“Information” means all information in the custody or under the control of the Division, whether in electronic or other recorded format, and includes administrative, financial, personal and student information, and information about those who interact or communicate with the Division;

“Digital Resources” are educational documents, content and processes that are in digital formats.

“Personal Information” means recorded information about an identifiable individual, including but not limited to:

1) the individual's name, home or business address or home or business telephone number;
2) the individual's race, national or ethnic origin, religious or political beliefs, or personal associations;
3) the individual's age, sex, marital status or family status;
4) an identifying number, symbol or other particular assigned to the individual;
5) the individual's fingerprints, blood type or inheritable characteristics;
6) information about the individual's health and health care history, including information about a physical or mental disability;
7) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;

8) anyone else's opinions about the individual;
9) the individual's personal views or opinions, except if they are about someone else; and
10) student records.

"Employee" has the meaning given in the Freedom of Information and Protection of Privacy Act and includes employees, contractors, volunteers, and others providing services to, or on behalf of, the Division.

"Student information" means personal information about a student, whether enrolled with the Division or not, including information about any student contained in PASI.

"PASI" means the Provincial Approach to Student Information database and application maintained by Alberta Education.

"Risk" means any factor that could be detrimental to the confidentiality, availability, integrity or privacy of information in the custody or control of Livingstone Range School Division.

Information Security Principles

1) Only authorized persons may have access to information.
2) All information must be maintained in confidence and disclosed only if authorized by regulation or law including, but not limited to, the Education Act, the Freedom of Information and Protection of Privacy Act, the Child Welfare Act, and the Income Tax Act.
3) Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and Division records management standards, procedures, and practices.
4) Each person using the Division's information is responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.
5) The nature of security measures must be adequate and appropriate for the sensitivity of the information to be protected.
6) Employees will be provided with training and awareness materials as necessary to ensure that they understand their security obligations.

Cellular Telephones, E-Mails

Caution must be used when conveying confidential information over insecure technologies such as cellular phones, e-mail. Division owned or personal smartphones accessing divisional email must have passwords/code.

Secure Storage of Information

1) Sensitive or confidential information must be stored in a secure location with restricted access, such as secure electronic storage, a locked room, or a locked filing cabinet. Security measures must be appropriate for the sensitivity of the information being stored regardless of the physical or electronic medium on which it is stored.
2) Diligence must be taken when transporting or transferring sensitive or confidential information so that it reaches its intended destination intact and without unauthorized access or disclosure.

Disposal of Information

Any information that is no longer required for either administrative, educational, financial, legal or historical purposes, and the retention of which is not regulated by any provincial or Federal law may only be destroyed in accordance with records management procedures and practices as determined by the Division.

Remote Access

1) It is the responsibility of each of the Division's employees, contractors, vendors and agents with remote access privileges to the Division's corporate network to ensure that their remote access connection is as secure as the user's on-site connection to the Division.
2) All hosts that are connected to Division internal networks via remote access technologies must use the most up-to-date anti-virus software, including personal computers.
3) Personal equipment that is used to connect to the Division's networks must meet the security requirements of Livingstone Range School Division. Personal equipment cannot be used to access SIS and or PASI services external to the LRSD network. (As per Schedule "A" Pasi Security controls for School Authorities.)
4) Organizations or individuals who wish to implement Remote Access solutions to Livingstone Range School Division production network must obtain prior approval from the Division.

Email Use

1) The Division email system shall not be used for the creation or distribution of any disruptive or offensive messages. Employees who receive any emails with this content from any Division employee should report the matter to their supervisor immediately.
2) All email that is sent or received via Division email systems, whether personal or work-related, is in the custody or under the control of the Division for records management, security and Freedom of Information and Protection of Privacy Act purposes. Personal email messages may be included in Division responses to FOIP access requests or privacy complaints. Within the parameters of FOIP, and any other relevant legislation, the Technical Services Department may review files and communications to ensure system integrity and responsible use of resources.

Mobile Employee Endpoint Responsibility

1) This policy applies to any mobile device, or endpoint computer either issued by the Division or owned personally by an employee used for Division business which contains stored data owned by the Division. This includes Livingstone Range School Division email.
2) All employees shall assist in protecting devices issued by the Division or storing Division data. Mobile devices are defined to include but not limited to desktop systems in a telework environment, laptops, tablets, external hard drives, memory sticks and cell phones.
3) Portable computing devices and portable electronic storage media that contain data owned by the Division must use password protection or encryption or equally strong measures to protect the data while it is being stored.
4) Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall be made aware and confirm awareness that

compliance with the all applicable policies, procedures, and standards related to mobile and personal computing devices is mandatory.

Workstation Security

1) Workstations include: laptops, desktops, tablets and other computer based equipment containing or accessing Division information, including authorized home workstations accessing the Division's network.
2) Appropriate data security measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including personal information as defined in the Freedom of Information and Protection of Privacy Act, health information as defined in the Health Information Act and student information as defined in the Student Records Regulation, as well as any other information of a sensitive or confidential nature.
3) Employees using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.
4) The Division will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures may include but are not restricted to:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen with a timeout period to ensure that workstations that were left unsecured will be protected.
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including all personal information, on network servers, not local drives or cloud storage, whenever possible.
- Complying with all applicable encryption requirements.
- Ensuring that anti-virus programs are running and up to date.
- Ensuring that monitors are positioned away from public view.
- If wireless network access is used, ensuring that access is secured using appropriate security measures and standards.

Passwords

1) All system-level passwords (e.g., root, AD admin, application administration accounts, etc.) must be changed when any member of the Technology Services Department leaves the employ of Livingstone Range School Division.
2) All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed at least every 12 months.
3) Staff Passwords must not be inserted into email messages or other forms of electronic communication.
4) All school Administration Staff (including administration assistants) passwords shall have the following characteristics:

   - Contain both upper and lower case characters (e.g., a-z, A-Z)
   - Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Use at least 8 alphanumeric characters
- Should not be written down or stored on-line unencrypted

Unacceptable Use

The following activities are strictly prohibited, with no exceptions:

1) Violations of the rights of any person or the Division that are protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Division.
2) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Division or the end user does not have an active license is strictly prohibited.
3) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs...).
4) Revealing your account password to others or allowing use of your account by others. This includes family and substitute employees.
5) Using a Division computing asset to actively engage in any activity that is prohibited by law or Division policy.
6) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
7) Circumventing user authentication or security of any host, network or account.
8) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
9) Providing personal information to any third party without express authorization to do so, either as part of employment responsibilities or as authorized on a case-by-case basis.
10) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
11) Any form of harassment via email, text, or telephone, whether through language, frequency, or size of messages.
12) Unauthorized use, or forging, of email header information.
13) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
14) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Application Service Providers (ASPs)

Any business process, system or application that is proposed to be outsourced to an ASP must be evaluated against the following:

1) In the event that Division data or applications are to be hosted or affected by an ASP, a binding contract with the ASP should fully specify the privacy and security measures to be employed to ensure that ASP services provide an acceptable level of data protection.
2) If the ASP provides confidential information to the Division, the Division is responsible for ensuring that any obligations of confidentiality are satisfied. This includes

information contained in the ASP's application. The Division's legal services department should be contacted for further guidance if questions about third-party data arise.

Application Service Provider (ASP) Security Standards

This defines the minimum security criteria that an Application Service Provider (ASP) should meet in order to be considered for use by the Division. As part of the ASP security compliance process, the ASP Vendor must demonstrate compliance with the Standards listed below. These Standards are subject to additions and changes by the Division.

1) Scope

   This document can be provided to ASPs that are either being considered for use by the Division, or have already been selected for use.

2) Responding to These Standards

   The Division can request from an ASP detailed, technical responses to the following statements and questions. In addition, ASP should include any security white papers, technical documents, or policies that may be relevant.

   Responses to the Division information requests for the following sections should be specific and sufficiently detailed. Where appropriate, the ASP's written agreement with the security statement contained in the section may be deemed a sufficient response by the Division.

3) General Security

   The Division reserves the right to periodically audit the Division application infrastructure to ensure compliance with the Division's ASP Policy and Standards. Non-intrusive network audits (basic portscans, etc.) may be done randomly and without prior notice.

   The ASP on request must provide an architecture document that includes a network diagram of the Division Application Environment, illustrating the relationship between the Environment and any other relevant networks that details where the Division data resides, the applications that manipulate it, and the security thereof.

   The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

4) Physical Security

   The equipment hosting the application for the Division must be located in a physically secure facility.

   The infrastructure (hosts, network equipment, etc.) hosting the Division application must be located in a locked environment.

   The ASP must on request disclose who amongst their personnel will have access to the environment hosting the application for the Division.

   The Division requires that on request the ASP disclose their ASP personnel background check procedures.

5) Network Security

If the data to be transmitted between the Division and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between the Division and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

6) Host Security
The ASP must disclose on request how and to what extent the hosts comprising the ASP's application infrastructure have been hardened against attack.

The ASP must provide on request a listing of current patches on hosts, including host operating system patches, web servers, databases, and any other material application.

Information on how and when security patches are applied shall be provided to the Division on request including the ASP’s policy for applying security patches?

The ASP must describe their processes for monitoring the integrity and availability of those hosts.

The ASP must provide information on their password policy for Division application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

7) Cryptography
Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, and/or PGP.

December, 2012

References

Freedom of Information and Protection of Privacy Act (FOIPP)
Education Act Section 56
Cloud Computing and Privacy Toolkit -Alberta Education May, 2016
PASIprep Security Overview

Updates: July 2013; December 2017, January 2020