Information Technology (IT) Operating Procedures Update, PR573, Passwords for Network Access Security and PR725, Cyber Risk and Security

To: Governance and Policy Committee

Date: 11 September, 2019

Report No.: 09-19-3699

Strategic Directions

- Allocate Human and Financial Resources Strategically to Support Student Needs
- Transform Student Learning
- Create a Culture for Student and Staff Well-Being

Recommendation

It is recommended that the newly developed Cyber Risk and Security Procedure (PR725) and revised Passwords for Network Access Security Procedure (PR573), as presented in this report, be received for information.

Context

In April of 2015, the Board adopted the Acceptable Use of Information Technology Resource Policy (P088). Both the newly developed Cyber Risk and Security Procedure (PR725) and revised Passwords for Network Access Security Procedure (PR573) support implementation of the Acceptable Use of Information Technology Resource Policy (P088). As part of this process, the Procedures were reformatted in accordance with to the TDSB's Operational Procedure Template.

The Procedures (see Appendices A and B) are presented to the Governance and Policy Committee for information.

Action Plan and Associated Timeline

Subject to the Procedures being received at the Governance and Policy Committee, the Procedures will be presented to the Board of Trustees on September 25, 2019 for receipt.

Resource Implications

No additional resources will be required for the implementation of the Cyber Risk and Security Procedure (PR725) and Passwords for Network Access Security Procedure (PR573).

Communications Considerations

The Procedures will be communicated to the system and posted on the Board's internal and external website.

Board Policy and Procedure Reference(s)

Policies

- Acceptable Use of Information Technology Resources (P088)
- Freedom of Information and Protection of Privacy (P094)

Operational Procedures:

- Admission to Specialized Schools and Programs (PR612)

Appendices

- Appendix A: Cyber Risk and Security Procedure (PR725) - Newly Developed
- Appendix B: Passwords for Network Access Security Procedure (PR573) – Revised

From

Manon Gardner, Associate Director, School Operations and Service Excellence by email at Manon.Gardner@tdsb.on.ca or by phone at 416-394-2041

Peter Singh, Executive Officer, Information Technology/Information Management and Freedom of Information and Privacy by email at Peter.Singh@tdsb.on.ca or by phone at 416-396-5700

Appendix A

Toronto District School Board

Operational Procedure PR725

Title: **CYBER RISK AND SECURITY**

Adopted: July 11, 2019
Effected: July 11, 2019
Revised: NA
Reviewed: NA
Authorization: Executive Council

1.0 RATIONALE

This Cyber Risk and Security Procedure (the "Procedure") defines the approach by which the Board will manage its cyber risks in accordance with the Board's risk tolerance. The Procedure establishes a foundation for managing cyber risks and defines the boundaries for risk-based decisions within the Board.

This Procedure supports implementation of the Acceptable Use of Information Technology Resources Policy (P088) and the Freedom of Information and Protection of Privacy Policy (P094), and is aligned with TDSB's Cyber Security Strategy Framework and applicable legislation.

2.0 OBJECTIVE

The Procedure provides staff with a consistent cyber risk assessment process, for the purpose of determining areas of cyber risk, and appropriate cyber risk management controls;

The Procedure also determines the effectiveness of the implemented cyber risk management controls from the resulting cyber risk assessment.

3.0 DEFINITIONS

Board is the Toronto District School Board, which is also referred to as the "TDSB".

Cyber Risk is a negative event caused by a threat exploiting a weakness in underlying technology resource, process or people that will variably interfere or impede in achieving the goals or objectives of a given initiative.

Cyber Risk Assessment is a methodological assessment of the cyber risks for a digital initiative, in which recommendations are provided to manage such risks.
Cyber Risk Management Controls are a set of recommendations that are used to reduce cyber risk to an acceptable level.

Cyber Security Strategy Framework is a high level document outlining TDSB's information technology strategy for providing a safe and secure computing environment for our students and staff.

Data includes but is not limited to TDSB student records, employee records, confidential,
personal, or professional information and communications, or any other electronically
formatted information.

Digital Initiative is any TDSB sponsored project or initiative that involves the use of new (procured or developed) and/or enhancements to existing information technology.

Internet of Things (IoT) is any device that is connected to the Internet.

Information Technology Resources include but are not limited to computers, phones, tablets, cellular/mobile technology, applications, email, IoT, servers, networks, internet services, internet access, data, websites and any other electronic or communication technology provided by the TDSB or third party that exist today or may be developed in the future regardless of whether or not it may be used as a stand-alone device.

Information Technology Service Request (ITSR) is a formal information technology intake process in which new and/or enhancements to existing information technology initiatives are reviewed and assigned resources.

IT Liaison is a representative from TDSB's information technology team.

Program/Business Owner is the owner and/or sponsor for a TDSB digital initiative.

Personal Information is recorded information about an identifiable individual. As defined by the *MFIPPA* this may include, but is not limited to:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or

information relating to financial transactions in which the individual has been involved,

- Any identifying number, symbol or other particular assigned to the individual,
- The address, telephone number, fingerprints or blood type of the individual,
- The personal opinions or views of the individual except if they relate to another individual,
- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- The views or opinions of another individual about the individual, and
- The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Risk Register is a repository that is used to record and manage all of the identified cyber risks during the life cycle of a digital initiative.

TDSB is the Toronto District School Board, which is also referred to as the "Board".

User is any individual who accesses the TDSB's Information Technology Resources through any electronic or communication activity with any device (whether or not such device is a personally owned or has been provided by the TDSB) and regardless of the user's physical location. User's include but are not limited to employees, students, parents, volunteers, visitors, contractors, trustees, or any other authorized individuals.

4.0 RESPONSIBILITY

Associate Director, School Operations and Service Excellence and Executive Officer, Information Technology/Information Management and Freedom of Information and Privacy

5.0 APPLICATION AND SCOPE

This Procedure applies to all TDSB staff, including consultants, contractors or other persons who wish to initiate a digital initiative whether hosted by TDSB or third party.

This Procedure also applies to all of the Board's digital initiatives and stakeholders who are accountable and responsible for ensuring that a cyber risk assessment is performed at the start of a new digital initiative.

6.0 PROCEDURES

The following principles apply to the management of cyber risk:

- Support the Acceptable Use of Information Technology Resources Policy (P088), Freedom of Information and Protection of Privacy (P094) and other applicable TDSB policies, by ensuring a safe and secure computing environment for our students and staff.
- Align to TDSB's Cyber Security Strategy Framework.
- Adapt security and privacy by design1 to ensure effective cyber risk reduction.
- Ensure that cyber risk management is carried out as a consistent, holistic, organization wide activity that aligns and integrates with enterprise risk management.
- Comply with legislation such as MFIPPA for the protection of sensitive and personal information.

6.1. Cyber Risk Assessment Accountability & Responsibility

- A cyber risk assessment will be performed at the start of a digital initiative to ensure that cyber risk management controls are identified and considered at the start of all the Board's digital initiatives and continued through the life cycle of service delivery.
- The accountability to ensure that a cyber risk assessment is performed will remain with the IT Liaison, if one is assigned. Otherwise the accountability to ensure that a cyber risk assessment is performed will remain with the program/business owner. The IT Liaison and/or the program/business owner can delegate the responsibility of completing the cyber risk assessment form to a project or technical resource.
- The program/business owner will own the risks identified in the cyber risk assessment, its disposition, and agree to establish completion dates for accepted cyber risk management controls that are identified as part of the cyber risk assessment.

[1] *Privacy by Design* – a set of principles developed by Dr. Ann Cavoukian and adopted as an International Standard, including by General Data Protection Regulation (GDPR) to preserve privacy.

6.2. Cyber Risk Assessment Process & Form

IT Liaison will:

- Use the cyber risk assessment form and complete section 2 with relevant and detailed information before submitting the form to the Cyber Security and Risk Management team for review.

- Respond to requests from the Cyber Security and Risk Management team for additional details and/or clarity of any information provided in the cyber risk assessment form within mutually agreed upon timelines.

- If section 2 of the cyber risk assessment form does not contain sufficient detail after the initial follow up; the Cyber Security and Risk Management team will deem the form to be incomplete and reserve the right to assign a risk ranking of high if deemed appropriate.

- Agree to the recommendations provided in section 4 of the cyber risk assessment form, and provide a plan detailing the names and dates for the completion of the cyber risk management controls. Responsibility for accepting the cyber risks that are not reduced to an appropriate level will rest with the program/business owner.

- IT services reserves the right to reject any digital initiative if the risk is high, and/or if the program/business owner has not agreed to implement the appropriate cyber risk management controls within a reasonable timeframe.

6.3. Cyber Security and Risk Management team will:

- Provide guidance for users who request assistance completing the cyber risk assessment form.

- Review the completed cyber risk assessment form, and provide cyber risk management controls.

- Reach out to the IT Liaison (if necessary) for additional details and/or clarity on any information provided in the cyber risk assessment form.

- Submit the completed cyber risk assessment form with cyber risk management controls to the IT Liaison and/or program/business owner, as well as submit the cyber risk assessment form to the Senior IT Managers team when deemed necessary for internal review.

- Follow up with the IT Liaison and/or program/business owner for sign off on the cyber risk management controls for medium and high risk digital initiatives.

- Update the risk register

6.4. IT Senior Management Team will:

- Review the completed cyber risk assessment form provided by the Cyber Security and Risk Management team.

- When appropriate cyber risk assessment will be tabled at the BOAT (Business Operations and Administrative Technologies) and/ or EduTech (Education Technologies) Committees, Enterprise Risk Management for their reviews or information.

6.5. Compliance

- Users are expected to adhere to the guidelines provided in this Procedure and supporting policies. Cyber risks must be identified at the start of all digital initiatives through a cyber risk assessment. Cyber risk management controls must be provided and implemented following the completion of the assessment and within a reasonable and agreed upon time frame.

- Failure to do so may put the Board at risk for potential cyber security incidents and/or privacy breaches which can impact the safety and security of our students and staff.

- As a result the Board, including our students and staff, may face disciplinary action, in the form of significant negative impact to the finances, operations, and/or reputational standing in the community.

7.0 EVALUATION

This Procedure will be reviewed as required, but at a minimum every four (4) years after the effective date.

8.0 APPENDICES

Not Applicable

9.0 REFERENCE DOCUMENTS

Policies

- Acceptable Use of Information Technology Resources (P088)
- Freedom of Information and Protection of Privacy (P094)

Frameworks:

- TDSB Cyber Security Strategy Framework
- TDSB Cyber Security Charter

Legislative Acts and Regulations:

- *Education Act*
- *Municipal Freedom of Information and Protection of Privacy Act*

Other Documents:

- TDSB Cyber Security Strategy Framework
- TDSB Cyber Security Charter
- Cyber risk assessment form

Appendix B

Toronto District School Board

Operational Procedure PR573

Title: **PASSWORDS FOR NETWORK ACCESS SECURITY**

Adopted: November 13, 2000
Effected: November 13, 2000
Revised: October 28, 2010, December 6, 2011, September 6, 2016, **March 22, 2019**
Reviewed: December 2011, October 2012, April 2013, March 2019
Authorization: Executive Council

1.0 RATIONALE

This operational procedure supports the implementation of the Board's policy on Acceptable Use of Information Technology Resources (P088).

2.0 OBJECTIVE

To provide details about the creation and use of passwords for network access security. Passwords play a key role in preventing unauthorized access to resources. This procedure sets out different groups of network users to ensure that password strength matches the various user groups across the system.

3.0 DEFINITION

Password is a string of characters used by staff and students to log onto the network.

4.0 RESPONSIBILITY

Executive Officer, Information Technology and Information Management

5.0 APPLICATION AND SCOPE

This operational procedure applies to all users who access the Board's Information Technology Resources.

6.0 PROCEDURES

All Board employees and students with access to the computer network must follow the procedure outlined below to ensure maximum password security:

6.1 Students – Primary (Grades K - 3)

(a) Minimum Password Length - a minimum password length of four characters.

(b) Password Complexity – the complexity value is set to "Enabled" but it is not enforced.

(c) Password History - password histories are enforced to three revisions to prevent passwords from being recycled until three different passwords have been used, i.e. you have to use three different passwords before you can go back and reuse the first one.

(d) Minimum Password Age – the minimum password age is set to zero days, i.e. you can change your password twice in one day.

(e) Maximum Password Age – there is no maximum password age. This means that the password never expires and can be used until it has been changed.

(f) Account Lockout Threshold – the Account Lockout Duration and Account Lockout Threshold are defined in Windows Directory Services (Active Directory), but not disclosed in this procedure for security reasons.

6.2 Students – Junior and Intermediate (Grades 4 – 8)

(a) Minimum Password Length - a minimum password length of six characters.

(b) Password Complexity – the complexity value is set to "Enabled" but it is not enforced.

(c) Password History - password histories are enforced to five revisions to prevent passwords from being recycled until five different passwords have been used, i.e. you have to use five different passwords before you can go back and reuse the first one.

(d) Minimum Password Age – the minimum password age is set to zero days, i.e. you can change your password twice in one day.

(e) Maximum Password Age – there is no maximum password age. This means that the password never expires and can be used until it has been changed.

(f) Account Lockout Threshold – the Account Lockout Duration and Account Lockout Threshold are defined in Windows Directory Services (Active Directory), but not disclosed in this procedure for security reasons.

6.3 Students – Secondary (Grades 9 – 12)

(a) Minimum Password Length - a minimum password length of eight characters (there is a marked increase in computing power required by an intruder to hack passwords longer than seven characters in length).

(b) Password Complexity – the complexity value is set to “Enabled” but it is not enforced.

(c) Password History - password histories are enforced to five revisions to prevent passwords from being recycled until five different passwords have been used, i.e. you have to use five different passwords before you can go back and reuse the first one.

(d) Minimum Password Age – the minimum password age is set to zero days, i.e. you can change your password twice in one day.

(e) Maximum Password Age – there is no maximum password age. This means that the password never expires and can be used until it has been changed.

(f) Account Lockout Threshold – the Account Lockout Duration and Account Lockout Threshold are defined in Windows Directory Services (Active Directory), but not disclosed in this procedure for security reasons.

6.4 Staff (Except those staff identified in Section 6.5 and 6.6 below)

(a) Minimum Password Length - a minimum password length of eight characters (there is a marked increase in computing power required by an intruder to hack passwords longer than seven characters in length).

(b) Password Complexity – the complexity value is set to “Enabled” but not enforced.

(c) Password History - password histories are enforced to five revisions to prevent passwords from being recycled until five different passwords have been used, i.e. you have to use five different passwords before you can go back and reuse the first one.

(d) Minimum Password Age – the minimum password age is set to zero days, i.e. you can change your password twice in one day.

(e) Maximum Password Age – there is no maximum password age. This means that the password never expires and can be used until it has been changed.

(f) Account Lockout Threshold – the Account Lockout Duration and Account Lockout Threshold are defined in Windows Directory Services (Active Directory), but not disclosed in this procedure for security reasons.

6.5 High-Security Staff

High-Security Staff include staff in the following areas:
- Employee Services (Payroll)
- Senior Team
- All Assistants to Senior Team (**ALL Asst to Senior Team**)
- Trustees and Administrative Liaisons **(All Trustees & Assistants)**
- Finance
- Legal

(a) Minimum Password Length - a minimum password length of twelve characters (there is a marked increase in computing power required by an intruder to hack passwords longer than seven characters in length).

(b) Password Complexity – the complexity value is set to “Enabled” but not enforced.

(c) Password History - password histories are enforced to five revisions to prevent passwords from being recycled until five different passwords have been used, i.e. you have to use five different passwords before you can go back and reuse the first one.

(d) Minimum Password Age – the minimum password age is set to zero days, i.e. you can change your password twice in one day.

(e) Maximum Password Age – the maximum password age is 90 days. Users are required to change the password every 90 days and will be reminded of the change seven days ahead of expiry.

(f) Account Lockout Threshold – the Account Lockout Duration and Account Lockout Threshold are defined in Windows Directory Services (Active Directory), but not disclosed in this procedure for security reasons.

6.6 High-Security Information Technology Staff

High-Security Information Technology Staff include staff in the following areas:
- Information Technology Services
- Student Information Systems
- Research & Information Services

(a) Minimum Password Length - a minimum password length of 12 characters (there is a marked increase in computing power required by an intruder to hack passwords longer than seven characters in length).

(b) Password Complexity – the Complexity value is set to “Enabled” but not enforced.

(c) Password History - password histories are enforced to five revisions to prevent passwords from being recycled until five different passwords have been used, i.e. you have to use five different passwords before you can go back and reuse the first one.

(d) Minimum Password Age – the minimum password age is set to zero days, i.e. you can change your password twice in one day.

(e) Maximum Password Age – the maximum password age is 90 days. Users are required to change the password every 90 days and will be reminded of the change seven days ahead of expiry.

(f) Account Lockout Threshold – the Account Lockout Duration and Account Lockout Threshold are defined in Windows Directory Services (Active Directory), but not disclosed in this procedure for security reasons.

7.0 EVALUATION

This operational procedure will be reviewed as required, or every four (4) years, whichever occurs first.

8.0 APPENDICES

- Not Applicable

9.0 REFERENCE DOCUMENTS

Policies:

- Acceptable Use of Information Technology Resources (P088)