OTTAWA-CARLETON DISTRICT SCHOOL BOARD

Building Brighter Futures Together at the Ottawa-Carleton District School Board

Audit Committee **25 November 2019**

Report 19-117

Policy P.074.IT Computer Network Security

Key Contact: Shawn Lehman, Superintendent of Instruction, ext. 8391

PURPOSE:

1. This report provides the proposed revisions to Policy P.074.IT Computer Network Security (attached as Appendix A) for consideration by the Audit Committee. The Security Steering Committee recommended that the policy, which was last updated in 1999, be revised. A consultation plan (attached as Appendix B) outlines how the stakeholders will be consulted regarding the changes to the policy. A timeline with consultation with key stakeholders has been identified (attached as Appendix C).

CONTEXT:

2. The District last wrote and approved Policy P.074.IT Computer Network Security in January 1999. The digital security landscape has evolved considerably during the last 20 years. While technology has to continually evolve to mitigate the technological threats, there is a greater need for awareness for staff and students to be cognizant of threats via social engineering, phishing attacks, email spoofing, etc. The revisions to the computer network security policy will assist in raising District awareness of security threats to the organization.

   The recommended revisions to the policy also include a more comprehensive understanding of the terms associated with the complexities related to network security, as well as incident management, business continuity, monitoring and compliance.

   The draft policy outlines guiding principles that set the foundation for the policy. A policy is a statement of intent, governing principles or end result adopted by the Board intended to guide future actions. Policies are typically related to the principles, rules, and guidelines formulated or adopted by an organization to reach its long-term goals. They are designed to influence and determine all major decisions and actions.

A procedure refers to a document issued through the Director of Education, governing the implementation of a Board policy, or required to coordinate and control certain aspects of system operations. They are the detailed methods and specific strategies employed by the organization to support day-to-day operations of the District's policies.

KEY CONSIDERATIONS:

3. **Policy and Procedure Framework**

The District currently has a computer network policy which is fairly straightforward and dates back many years. Staff has drafted a new policy with a view to rescinding and replacing the existing policy. The draft new policy is attached as Appendix A.

The new policy is intended to be a high level policy which establishes key areas of control in the District's network security infrastructure, including (reference section titles of policy i.e., compliance management etc). The policy sets the parameters for a secure infrastructure; the specific protocols will be established in the companion procedure which is under development.

This policy is intentionally focused on computer network security. While information management security and privacy are an important part of a secure infrastructure, the District has an established privacy policy. Every effort has been made to align but avoid duplication of the privacy policy in this draft.

OCDSB policies related to Computer Network Security P.074.IT include:

- P 128 GOV - Privacy- MFIPPA (Privacy--Municipal Freedom of Information and Protection of Privacy [MFIPPA];
- P 100 IT - Appropriate Use of Technology;
- P 049 IT - Electronic Communications Systems; and
- PR 501 GOV - Policy And Procedure Co-Ordination And Management.

4. **Security Audits**

In 2015-2016 the Regional Internal Audit Team conducted a review of the District's Enterprise Resource Planning (ERP) systems. This review recommended a formalized patch management process to ensure security patches were installed in a timely manner. In December 2018, the District sought out and participated in the 10 Essential Security Practices Assessment through a third party provider. The findings from this assessment indicated that while the District had recognized the need for security, there were other areas of need. Four foundational projects were recommended to address these needs:

Project	Deliverables
Governance Framework	● Organizational structure ● Roles and Responsibilities Matrix (RACI –Responsible, Accountable, Consulted, Informed) ● Security Steering Committee
Policy Framework	● Security policy framework. ● List of policies, guidelines, standards, and processes to be developed. ● Formal policy review and approval process.
Security Metrics and Reporting	● Key performance, risk and security metrics. ● Data collection, analysis and reporting processes.
Security Awareness Program	● Online interactive training modules. ● Communication plan. ● Security awareness performance measurements

5. **Security Governance**
The Security Steering Committee was formed as a result of the recommendation in the 10 Essential Security Assessment. The first recommendation of the Security Steering Committee was to update the Computer Network Security policy and review the accompanying procedures.

6. **Awareness and Training**
One of the key changes to this policy is the commitment of the District to provide training to all staff. Security awareness training can occur in a variety of forms including online modules, simulated phishing attacks with responses to educate the user and face to face workshops. Baseline data will be gathered and used to assist with planning future training opportunities and monitoring the impact.

7. **Third Party Data Sharing**
With the increase of availability of third party applications for educational use, teachers are being asked to interpret privacy agreements and terms and conditions before sharing student data. This has been a challenge for educators and it is clear they are in need of guidance and support in this area. The District is moving forward with the creation of a software catalogue committee that will

curate, oversee and recommend applications in schools from a pedagogical, technological and privacy and security aspect.

8. **Consultation**

This policy deals with very important issues which may be of high interest to some stakeholders, but may be less likely to attract input from the broader community as a whole. Recognizing this, careful consideration was given to how to craft a meaningful consultation strategy.

As the District has several policies and procedures to be reviewed this year, staff developed a specific page on the District website which contains information about current policy consultations. There is a link to this page on school websites and it includes key background information, timelines for consultation and opportunities for providing feedback.

Information about this consultation has been sent to all school councils through the school council newsletter and to all parents through Keeping You Connected. Interested parents were invited to share feedback either electronically or at a planned policy discussion meeting held on November 12th, 2019.

In addition to the parent consultation, consultation includes targeted outreach to the federations, the Audit Committee, principals, vice-principals and managers, students and staff in Business and Learning Technologies.

The attached consultation plan proposes a series of questions which will guide the consultation with all groups, including:

- Does the draft policy establish an effective framework for network security?
- What specific computer security protocols or best practices would you like to see documented in the accompanying procedures?
- Are there gaps or opportunities to enhance our computer and information management security practices?
- What resources or supports do you believe are necessary to support effective implementation of this policy?

A third party consultation firm has been hired to review the policy and provide input around potential changes. Persons interested in participating may provide comments until November 27th which will allow a revised draft to come forward to COW for January.

RESOURCE IMPLICATIONS:

9. The resources required to carry out this work will be part of the B&LT department budget.

COMMUNICATION/CONSULTATION ISSUES:

10. A consultation plan has been developed in consultation with Board Services. It is located as Appendix B in the package.

STRATEGIC LINKS:

11. This policy revision is aligned with a Culture of Caring through championing and nurturing a safe, caring and respectful workplace.

GUIDING QUESTIONS:

12. The following questions are provided to support the discussion of this item by the Committee.
    - What would the Audit Committee like to see in an annual security report?
    - What needs to be adjusted to the draft policy to increase the security of the computer network? and
    - What additional questions should we be asking about the computer network security policy?

Shawn Lehman
Superintendent of Instruction

Camille Williams-Taylor
Director of Education
Secretary to the Board

APPENDICES
Appendix A - Policy P.074.IT
Appendix B - Consultation Plan
Appendix C- Computer Network Security (Policy P.074.IT) Consultation Plan Timeline