Committee of the Whole (Public) **1 October 2019**

Report 19-092

Policy P.074.IT Computer Network Security

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

PURPOSE:

1. To seek approval of a consultation plan regarding revisions to Policy P.074.IT, Computer Network Security as recommended by the Security Steering Committee.

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 draft recommendations to the policy (attached as Appendix A) also includes 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.

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 new policy is intended to be a high level policy which establishes key areas of control in the district's network security infrastructure, including Incident Management, Business Continuity, Monitoring and Compliance. 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 .

4. Security Audits

In 2015-16 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 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 per the recommendation of the 10 Essential Security Assessment. The first recommendation of the Security Steering Committee was to up date 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.

RESOURCE IMPLICATIONS:

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

COMMUNICATION/CONSULTATION ISSUES:

9. 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 has been given to how to craft a meaningful consultation strategy.

Recognizing that the district has several policies and procedures to be reviewed this year, staff is developing a specific page on the district website which will contain information about current policy consultations. There will be a link to this page on school websites. This page will include key background information, timelines for consultation and opportunities for providing feedback.

Information about this consultation will be sent to all school councils through the school council newsletter and to all parents through Keeping You Connected.

Interested parents will be invited to share feedback either electronically or at a planned Policy Discussion meeting.

In addition to the parent consultation, the 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?

Persons interested in participating may provide comments until November 20th which will allow a revised draft to come forward to COW for December.

STRATEGIC LINKS:

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

RECOMMENDATION:

THAT the consultation plan outlining revisions to Policy P.074.IT - Computer Network Security, attached as Appendix B to Report 19-092 be approved.

Shawn Lehman Superintendent of Instruction Ext.8391	Camille Williams-Taylor Director of Education and Secretary to the Board

APPENDICES
Appendix A - Policy P.074.IT
Appendix B - Consultation Plan