No. VI-[illegible]

Information Security	
Adopted: June 9, 2022	Last Reviewed/Revised: June 9, 2022
Next Scheduled Review: 2024-2025	
Associated Policies & Procedures: I-02 Records Information Management I-07 Protection of Privacy I-30 [illegible] I-43 Use of Technology and Digital Citizenship VI-51 Security Breach Procedure VI-62 Use of Technology and Digital Citizenship VI-63 Social Media VI-81 Privacy Procedure VI-83 [illegible]	

Purpose

The purpose of this procedure is to outline the requirements [illegible] Policy I-47 Information Security.

Application and Scope

Halton Catholic District School Board (HCDSB) will be risk-focused, comprehensive, and responsive in meeting its cyber and data security commitment. It applies to all employees, third-parties, and [illegible]

References

EC-Council Certified Chief Information Security Officer Program, Version 3

Gartner Glossary

Information Governance for Executives, Fundamentals and Strategies, Robert F. Smallwood

National Institute of Standards and Technology Resource Centre

Open Web Application Security Project

Phishing | What Is Phishing?

Share files from Google Drive to your Computer - Google Drive Help

Using a secure method to collect or receive electronic documents

14. Report all problems and concerns that relate to a possible or potential breach of information security to privacy@hcdsb.org and helpdesk@hcdsb.org. The latter if the incident involves technology. Refer to HCDSB procedure VI-51 Security Breach.

15. Apply a security classification to content (e.g., type confidential in email subject, insert confidential in the footer or header field in a document or in a text box widget on an internal site).

16. Ensure boundary and internal network protection controls are implemented and maintained in accordance with Municipal Freedom Information Protection Privacy Act requirements.

17. Account for ongoing and continuous changes to business operation, ongoing risks, and the external environment utilizing information risk management best practices.

18. Maintain practices to effectively identify relevant threats, protect information assets, detect security incidents, respond to security incidents, and recover from them.

19. Maintain an asset and data inventory (to prioritize information in accordance with sensitivity level) as well as a risk register (to document risk management decisions).

20. Ensure all third parties with access to confidential information agree to the provisions in HCDSB's third-party data sharing agreement.

APPROVED: Administrative Council

AUTHORIZED BY: ______________________________

(Director of Education and Secretary of the Board)