CFPD - Technology Access Points

1. Internal network files

- These are files used for daily work – Microsoft Office Suite programs such as Word, Excel
- Files are saved on the Foundation's internal network and saved in One Drive/Microsoft 365 Cloud
- If files are deleted, they will go into a recycle bin. If deleted in error, these can be retrieved for a limited number of days. Otherwise, they are automatically deleted from the recycle bin to maximum storage space.

Risk Issue: Internal fraud – employee deleting files and action not discovered within time frame held in recycle bin.

Risk Mitigator: Employees terminated with cause are given pay in lieu of notice and do not have access to technology systems once action taken.

2. Web site

- Uses WIX program, self hosted by CFPD
- Used for public information, also has private portals to Board, Bursary and Grants

Risk Issue: Illegal entry into a private portal as passwords not difficult to break into for criminals or those who have this expertise. While information in the private portals may become public in future, there is internal information and discussion points CFPD would not want to be made public at the time. Dependent of use of information by an illegal entry, could erode CFPD's reputation and trust in organization.

Risk Mitigator: Change private portal passwords on an annual basis, when there is a staff, board or volunteer turnover. Users of portals sign confidentiality agreements annually baring users of providing password to others for illegal entry.

3. Payroll software

- CFPD is using QuickBooks software installed on the 2 workstations (Executive Director and Bookkeeper) in the office, not the on-line version
- Weekly, the current data from the software program is saved on an external drive and taken to the Bookkeeper's home for off site storage

Risk Issue: The QuickBooks software becomes corrupted on the Bookkeeper's workstation become inoperable making it difficult for the program to restored, especially if there is work in progress saved during the week and after the backup has been saved on the USB drive.

Risk Mitigator: While restoring the software on a new workstation for the Bookkeeper would take time, having it on another workstation would reduce the time needed to complete the payroll, especially if due in the same week. It is noted that QuickBooks software will be moving only to on-line access in January 2026. The software will complete to provide updates (example – CPP and EI changes). While there are risks in having a USB with payroll data in an employee's home, this is currently deemed to be the most cost effective and reasonably risk-free process for CFPD.

4. Email

- Solutions IT is currently our technology support provider. They provide hosting for our email server and used various spam and malware filters to provide email from being a portal in for criminals trying to gain access to our systems.
- They currently use Sentinel One as the software to detect threats to our systems. This software looks like patterns that could signal bogus emails and is also reputed to be a "strong AI-driven threat detection".
- Solutions IT tech staff investigate email system threats and will communicate with CFPD's Executive Director or staff, in their absence, to resolve issues needing to be escalated for correction

Risk Issue: Email use as an entry point for cyber threats to CFPD's systems is deemed higher risk due to users. Bogus, but looking credible, emails and attachments on emails are two common cyber threat examples.

Risk Mitigator: CFPD's cyber threat detection software is updated to a stronger threat detection software as of Fall 2025. Board established Incident Response Policy (1.11) to assist with responding and reporting Cyber threats and/or other technologically related incidents. Cyber Insurance is in place as of December 2025 and a related CFPD Cyber Incident Response Guide related directly to assistance through the insurance provider was created for ease of use. Employee education (phishing) programs on detecting cyber attacks through email are planned for all employees in 2026.

5. Endowment Funds

- CFPD has contracted with Cardinal Capital Management for investment and managing the largest asset of CFPD, its endowment funds.
- We rely on the cyber risk and security practices of Cardinal with investments directly invested with various companies, governments.
- Cardinal Capital Management was founded in 1992 and has managed charitable organization investments since 2009. CFPD has contracted with Cardinal since September 2020. Cardinal takes a conservative approach to investments which matches CFPD's investment goals.
- Cardinal is a Canadian privately owned independent investment firm whose Head Office is in Winnipeg and with branch offices in Toronto, Brandon, Calgary, Edmonton and Kelowna

"Cardinal Capital Management maintains policies and procedures regarding cybersecurity to promote a secure digital environment. These policies and procedures include best practices, risk mitigation strategies, staff training, user access controls, encryption, secured virtual private networks and Muti-Factor Authentication tools, amongst other preventative and proactive protocols. The firm has a documented response plan which details the appropriate individuals and actions to respond in the case of an adverse cyber security event. Additionally, Cardinal maintains a cyber security insurance policy which is disaggregated by possible first and third-party losses tied to a cyber breach." (directly from Cardinal Capital Management-provided at the request of CFPD)

Risk Issue: There is no cyber risk issue with our Endowment Funds for CFPD as the funds are held external to our organization and we rely on the security measures of Cardinal and firms our funds are directly invested with. Riak is related to investment return.

Risk Mitigator: NA

6. Passwords (all technology points)

- CFPD's Executive Director and administrative staff have been issued many passwords for access to technology. Board members and volunteers have also been issued password(s) for the board portal and may have password(s) for the grants and bursaries portal as related to their committee work in these areas.
- It is important that passwords are not saved on your workstation or not held in a secure manner.

Risk Issue: Passwords being saved on workstations, reusing of common passwords and written password lists available in the office.

Risk Mitigation: CFPD created a Cyber Security and Acceptable Use Policy which identifies appropriate use of technology, password and acceptable use of devices by staff, board members and volunteers. This policy adherence has been added into the Code of Conduct and Ethical Behaviour declaration and signed by all staff, board members and volunteers. Password lists are secured by a password; unique passwords are being implemented and password saving apps are being considered to ensure seamless work processes.

7. DonorPerfect Canada

- This is a cloud-based (internet access) software used by nonprofit organizations to transact donations, issue receipts, complete event registrations and reporting.
- This software is owned by Aplos, a CA-based company and the specific software used by CFPD is the Canadian version offered by this company
- CFPD pays a monthly fee for use of this software.
- We use multi-factor authentication to use this program

Risk Issue: None identified

Risk Mitigation: N/A

8. Financial Systems

- CFPD has financial accounts with 2 providers – Stride Credit Union and Royal Bank. The credit union is used for daily banking, payments (billings, payroll) and the Royal Bank provides securities conversion to cash for doners donating securities or otherwise non-negotiables securities (examples are publicly traded shares, stock investments)
- Each uses 2 signers required for payments – electronic and physical based (i.e. Cheques)
- CFPD now carries a Cyber Insurance Policy

Risk Issue: Limited due to 2 signers required and multi factor authentication

Risk Mitigation: Manual procedures followed consistently: presentation of source document such as invoice or billing to substantiate payment including scrutiny by signer