Powell River Action Centre Society – Food Bank
Data Protection & Cyber Security Policy
Anti-Fraud & Anti-Spam Legislation - 2024

The Society IT person is a paid position, under the policy of staff compensation. The IT person will sit on any Tech or IT Committees that are struck by the board of directors. The committee will report to the board. If no committee exists, the IT tech person will report to the board of directors on a quarterly basis. The following 24 points will be the minimum of cyber security, anti-spam, and anti-fraud.

1. 3rd party independent review
    a. Once annually the Society will engage the services of an individual or entity experienced in assessing and reporting on cyber security maturity.
    b. The management will ensure that the Society regularly works with a reputable third party to review the security program.
    c. The Society will periodically assess risks related to the use of third-party IT.

2. Documented hardware inventory
    a. The Society will keep a detailed and up to date record of the network connected devices.
    b. All devices containing sensitive material will be maintained and secured.

3. Data asset inventory
    a. The Society shall maintain a data asset inventory list of important data stored. This will include where sensitive data is stored, who has access and to identify any risks to the data and to properly protect it.

4. Mobile device access
    a. The Society shall maintain controls to prevent users from collecting data on personal devices.
    b. The Society policy is to maintain separate login information for staff and clients and others to access the network.

5. Management of information security
    a. The Chief Staff Person and IT Tech person will work with a formally assigned person to manage the information and security.

6. Cyber security insurance coverage
    a. The Society will maintain the insurance policy and annually review if coverage is adequate.

7. Unique accounts for users and permissions
    a. The Society will periodically review accounts ensuring that all access and privileges are appropriate.

8. Password control
    a. The Society will enforce strong password controls and ensure that passwords are frequently changed.
    b. The password list will be kept at the main desk and not copied or shared.

9. Remote access
    a. The Society does not currently allow remote access.
    b. If there is no other way to provide services, multi-factor authorization will be required to set up remote access.

10. Security awareness training
    a. Security awareness training will be periodically provided to prevent and mitigate user risk.

11. Background checks
    a. Staff are required to complete a positive criminal record check prior to employment. This check is for working with vulnerable population. It is presumed that this check would suffice as vetting.

12. Data classification
    a. The Society shall maintain a data classification that will identify what data is sensitive and it should be handled based on the classification assigned to it.

13. Disposal and reuse of media and/or devices
    a. The policy will account for the destruction of devices only after a third party has wiped clean any information on the hard drive.
    b. Data destruction will be properly carried out through a secure deletion procedure and shredding of hard copy associated with it.

14. Sensitive material encryption
    a. Sensitive information should be encrypted using current best practices.
    b. The third-party IT person/people will periodically update and maintain.

15. Back-up and Test back-up
    a. Sensitive data will be routinely backed up as part of a formal process.
    b. Back-up systems will be tested at least annually to ensure they are reliable and not subject to attack by ransomware.

16. Restricting Physical access
    a. Only vetted staff persons will have access to sensitive information.

17. Identifying and Blocking Malicious email

a. Train those employees who have access to identify and delete any email that looks like phishing.
b. Contract with third party IT to reduce the risk involved with malicious email.

18. Vulnerability Scans
    a. The IT professional will conduct these scans as frequently as necessary.

19. Formal IT change control
    a. If/when a formal IT change is required the professionals will work with the Chief Staff Person of the Society for a smooth and safe transition.

20. Anti-virus and endpoint protection against malware
    a. The Chief Staff Person will work with the IT professional to ensure the system is protected against malware.
    b. If malware of other virus is detected, the IT professional will be contacted immediately to attend to the Centre and work on the issue.

21. Separate guest users from corporate network
    a. There will be a separate log in for guest users.
    b. The Society network will remain secure with a separate log in for staff only.

22. Monitor security logs
    a. Twice annually the IT professional will send a security log report to the Chief Staff Person who will present any issues to the Board. If no issues arise, the board will not be notified. This does not conflict or compete with the IT quarterly report to the board on regular issues.

23. Security incident response plan
    a. The staff of the Society will abide by the incident plan created by the IT Professional.

24. Who are the key individuals needed to be contacted in the event of an incident
    a. The Staff will have access to the IT Professional contact information and will contact IT as soon as an issue is detected.

Anti-Fraud:

The Powell River Action Centre Society – Food Bank will follow the Signatory section of the Bylaws concerning who can sign documents on behalf of the Society.

Canada Anti-Spam Legislation:

The Powell River Action Centre Society will follow all protocols associated with the sending and receiving of spam email as legislated by the Canada Anti-Spam Legislation.