POLICY: Incident Response Policy	
POLICY NUMBER	**1.11**
ISSUING AUTHORITY:	**Community Foundation of Portage and District Inc.**
APPROVED:	**Date**
LAST REVIEWED:	**Date**
NEXT REVIEW:	**2028**

Purpose:

The purpose of this policy is to ensure a coordinated, timely, and effective response to incidents that threaten the safety of staff, data, and organizational operations. This includes data breaches, IT security threats, and physical emergencies at the CFPD office location, at CFPD events off-site, or when utilizing CFPD devices off-site.

Scope:

This policy applies to all staff, contractors, volunteers, and visitors at the CFPD office, in attendance at any CFPD events and to all users, donors and benefactors of the organization's systems, data, and networks.

1. Types of Incidents Covered:

A) Data Security Incidents

- Data breach (unauthorized access, loss, theft, or disclosure of sensitive data)
- Malware, ransomware, or virus attacks
- Unauthorized system access, loss of device or credential compromise

B) Physical & Staff-Related Incidents

- Medical event involving staff, volunteers or visitors
- Fire, flood, gas leak, or natural disaster at the office
- Building lockdown, security threat, or evacuation situations

2. Response Procedures:

All incidents require a completed incident response form to be completed. This document is attached as Appendix A. Once completed, this document is to remain a confidential report of CFPD and can be shared with emergency personnel, insurance agents etc. at CFPD di

A. Data Security Incidents

1. Identify & Report — All suspected or confirmed data breaches must be reported immediately to the IT service provider, the organization's designated IT and cybersecurity contact. Any loss of device must be reported to the IT service provider, Executive Director and Board of Directors Executive Committee. If unauthorized access is suspected, users must inform the IT service provider immediately and take subsequent action as dictated by the IT service provider.
2. Contain & Investigate — The IT service provider will take appropriate steps to isolate and/or lock the affected systems and assess the scope of the incident. The theft of devices is to be reported to the appropriate authorities. If devices are compromised, staff will need to utilize alternative devices to continue operating as determined/approved by the IT service provider.
3. Notify — If required, the IT service provider will assist in identifying affected individuals and notifying internal leadership, and regulatory bodies in accordance with applicable laws.
4. Remediate — Secure systems, update credentials, and patch vulnerabilities as necessary. Staff will be required to update passwords and credentials as needed to ensure confidentiality of data.
5. Review — Conduct a post-incident review with The IT service provider to document lessons learned and prevent future recurrence.

B. Emergency at Office Location

1. Assess & Notify — Call 911 if needed, emergency contact information for staff and volunteers is maintained and available on the Board Portal.
2. Evacuate or Shelter in Place — Evacuation routes include the main front door or the back door (exiting into Mayfair) of the office. If sheltering in place, the main front door is to be locked, and shades drawn. The best shelter location on-site is the boardroom and/or storage room. If evacuating, all staff are to evacuate simultaneously, locking the premises before departing. Staff are to follow local authorities' direction when evacuating or sheltering in place.
3. Account for Staff/Volunteers/Visitors/Attendees —At larger off-site location events, one master sheet of attendees should be kept by the event coordinator in the case of evacuation. All volunteers assisting with off-site events must attend a safety meeting at the location, detailing emergency exits, muster locations etc.

4. Document Incident — ED or attending Admin will record details and coordinate follow-up. Incident Report Form to be completed by relevant staff, CFPD board members or volunteers present at time of emergency.
5. Restore Operations — Evaluate office safety before resuming work; inform Board or Directors of any disruptions and/or further action because of the emergency.

   If the office is closed for extended period (greater than 1 operational week), an alternative location and/or work from home option will be pursued, in order to maintain as close to regular business operations as possible. Mail will be forwarded to an alternative location, and laptops will be utilized by staff to ensure continuity of processes.

3. Communication Plan

- Use internal emergency contact lists for urgent updates. Phone numbers for all staff, board members and volunteers are available on the board portal and are kept up to date. Members listed on the contact document are responsible for ensuring that their information is current, including an alternative emergency contact.
- Send real-time alerts via phone and email and/or via social media if required (i.e. office is temporarily closed)
- Assign a spokesperson for external communications if required

4. Training & Review

- All staff and board members must receive annual training on incident response procedures.

5. Responsibilities:

- **Incident Coordinator / Safety Officer/ED**: Leads incident response efforts (ED/On-site staff or BOD Chairperson)
- **IT/Security Team**: Manages digital threats and breach containment (The IT service provider)
- **Designated Admin**: Manages staff communication and documentation during emergencies (Administrative staff or designate)
- **All Staff/Volunteers**: Must report incidents immediately and follow emergency protocols

Responsibility:

Review and revision of this policy annually and/or following major incidents, with subsequent recommendation of the Board for approval.