- The steps undertaken to ensure that all data is kept securely.

- Our security firm Provident Security is on call 24/7 and reports any suspicious movement inside the office during closed hours. If the alarms are set off, Provident will report to Mike Chutter, then through a contact tree if he does not answer (which includes Peter Chutter and Gail Howard.) Police will be notified.

We are working with our IT company, Netcetera to ensure our online activity and network are secure. A "Datto" device allows local backups of all data and systems on the premise as well as in the 2 secure data centers (Calgary and Toronto). All data in transit and at rest in the cloud is fully encrypted. In the event of a server failure, Netcetera can virtualize (bring up) the failed server on site within minutes if needed. In the event that we lose the building Netcetera can virtualize all servers in the cloud so that people can connect from home. This takes a little longer, but should be done the same day. They will monitor these backups 24/7 and take any corrective action needed. When they do periodic preventive maintenance checks they test that the file recovery and virtualization capability is working as expected.

From the antivirus, anti-ransomware, anti-phishing, anti-hacking etc. perspective we have never been better protected. The firewall is configured to protect the network with Secure VPN for remote access. We have premium antivirus with anti-ransomware protection on all endpoints and servers. In addition, we are monitored 24/7/365 by Sophos SOC which is staffed with highly trained security analysts and engineers who are ready at anytime day or night to neutralize and remove any attackers that may try to infiltrate our systems. In its entire history no company, whose security is monitored and managed by this SOC team has ever been compromised, taken down or suffered any data loss during an attack.

Netcetera has segmented our network to improve performance and security. This limits our exposure in the event of an attack. Netcetera and ourselves are always looking forward to ensure our network is robust and externally secure.

- Data Retention

Chutter UW collects only the personal information the organization needs to fulfill a legitimate identified purpose per PIPEDA regulation

Chutter UW will dispose of personal information that does not have a specific purpose or no longer fulfils its intended purpose (for purpose of UW files- 10-15 years). Dispose of information in a way that prevents a privacy breach, such as by securely shredding paper files or effectively deleting electronic records. If

information is to be retained purely for statistical purposes, (we) employ effective techniques that would render it anonymous.

- Breach Notification Procedures.

- report to the The Office of the Privacy Commissioner of Canada (OPC) any breaches of security safeguards that pose a real risk of significant harm;
- notify affected individuals and relevant third parties of any breaches with a real risk of significant harm; and
- keep records of all breaches, regardless of whether a breach presents a real risk of significant harm.

Notification to affected individuals needs to contain:
- a description of the circumstances of the breach and, if known, the cause;
- when the breach occurred;
- as much as possible, a description of the personal information that is the subject of the breach;
- what steps the organization has taken to reduce the risk of harm to affected individuals.
- name and coordinates of a contact person.
- the steps affected individuals can take to reduce the risk of harm, for example, changing their passwords or monitoring accounts.

- Governing the management of passwords

All staff members are required to set a password fitting the following specification:
Maximum Password Age: 42 days
Minimum Password Length: 7 characters