## CYBERSECURITY POLICY

[Organization Name]’s business is based on the ability to safely collect and assess the private information of our clients. We are aware financial businesses such as ours are a main target of cyber attacks. [Organization Name] is therefore vitally interested in protecting its client and company information from cyber attacks and is committed to using up-to-date and internationally recognized cyber security measures to do so.

DEFINITIONS

The following definitions have been sourced directly from the Canadian Centre for Cyber Security:

“Cyber attack” refers to the use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

“Cyber incident” means any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

“Cyber incident” means a threat actor, using the Internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

POLICY

The security and protection of information is of the utmost importance to [Organization Name]. We recognize that the information we collect is highly sensitive and if our systems are compromised, it could create serious injury to our customers and our business.

We will therefore implement proper planning and protection measures to reduce cyber security incidents and mitigate cyber threats. We will train our staff on cyber security awareness such as the controls we have in place and how to recognize any cyber threats that are occurring or may occur. All employees at [Organization Name] are to be on alert for possible or actual security breaches at all times, and must report any concerns to management immediately.

Employees must ensure that any software they are using or devices they are working on, including mobile devices, are securely configured. All devices must be set up and checked by (Insert who is responsible: the employee or if there is an IT department).

[Organization Name] will provide secure mobile devices to its employees to be used for conducting business securely. Employees may not use unsecured mobile devices at any time (Remove if this does not apply).

We have named (INSERT TITLE) as being responsible for our IT security.

At [Organization Name], the following security controls are in place. [Organization Name] will:

* Complete risk assessments on an ongoing basis of (Insert timeframe or if there is an accredited Canadian company that examines risk at [Organization Name] to determine any gaps every two years, and/or become certified itself, for example)
* Revise countermeasures as needed to fill in any gaps identified in the risk assessment
* Use multiple levels of security to protect information including top level SSL (website security), IP blocking, multiple authentication, cloud computing using SOC 2 audited compliance
* Ensure all data is encrypted and sent via a secure portal and never by through third party services or email
* Backup data to an external secure location and know how to recover this information if needed; make sure this data is also encrypted
* Utilize security software such as anti-virus and anti-malware software and activate firewalls
* Keep standalone devices, operating systems, applications, and security software up-to-date and free of known vulnerabilities
	+ Enable automatic software updates for all software so that security patches can be implemented immediately
	+ Replace any devices or software that no longer allow for automatic updates
* Only utilize external support services that are certified in Trust Service Principles compliance
* Properly control data placed on external portable media to protect it against loss and to remove data once transferred
* Follow cyber alerts and advisories available from the Government of Canada

Cyber Incident Response Plan

Do you have a specific procedure in place that you follow? IF so, add it here. We are happy to work with you on this if you provide some specifics of your procedure.