Security Statement

Collabria Financial Services Inc. (Collabria) adheres to very strict and rigorous security standards in order to ensure that information concerning you and transmitted to us whenever you use secured areas on the Collabria Websites (such as transactional services and online application forms) is protected against error, loss or unauthorized access.

Despite these precautions, you must implement the personal security measures recommended in this Security Statement in order to maintain optimal protection when you visit the Collabria Websites.

The Collabria Websites (including those hosted by third parties) are:

collabriafinancial.ca

collabriacreditcards.ca

www.mycardinfo.com

Make sure you review the terms and conditions that apply to each Collabria Website as they may contain variances to what is provided in this Security Statement and create additional obligations for you.

Online transactional services

The rules governing our online transactional services reflect the highest standards of the financial industry and comply with laws regarding the protection of personal information.

To find out more about the protection of personal information on the Collabria Websites, please refer to Collabria's Privacy Policy – www.collabriafinancial.ca/privacypolicy.

All transactions conducted as part of our online transactional services are encrypted during secure-environment sessions to protect the confidentiality of data exchanged between the Collabria Websites and the browser used with your computer or mobile device. Web services are only accessible if you use the most recent versions of Internet Explorer, Mozilla Firefox, Google Chrome and Safari that support the SSL2, 128-bit protocol.

Find out how to update your browsers.

SSL is an acronym that refers to Secure Sockets Layer, the protocol that permits authentication and data encryption between a Web server and browser. It provides a secure channel for the exchange of data that can only be decoded by authorized persons.

Firewall

Access to the Collabria Websites is controlled by a firewall, among other security measures. A firewall is a security mechanism that filters attempts to access a secure system or network in order to head off any unauthorized attempts or intrusions.

Online requests

Once completed, the online forms you submit to obtain a financial product or are securely stored at Collabria or Collabria's third party site. This means the forms are secure and no data they contain can be intercepted by a third party

Personal security measures

I - General precautions

Security icon

Be sure you always navigate in a secure environment when transmitting confidential data. When you do not see a security icon (closed padlock) displayed on your PC or mobile device (if the latter offers this functionality), or when you notice an open padlock, this means the security of any Internet transaction or data transmission cannot be guaranteed and could be intercepted by a third party.

The location of the security icon varies according to the browser.

Once you've located the padlock, click on it to display the certificate attesting to the site's security. On it you should be able to find the site's owner as well as the certificate validity period.

Email

The email you send is not guaranteed secure during transmission. It is therefore important not to include any personal or confidential information in such messages. For this reason, Collabria cannot be held liable for any damages resulting from the interception, loss or modification of any email message you send.

II - Specific security precautions when using Collabria services

Passwords

- The first time you use a Collabria Website service that requires a password, choose a password to replace the one you were assigned initially. You will therefore be the only one to know this password.
- Select a password that is easy to remember. The password should contain between 6 and 12 characters, the first three of which must be numbers. The remaining characters must include at least one letter.
- Avoid passwords based on personal data as it could be discovered by ill-intentioned users and never use part of your credit card PIN number.
- Never disclose your password to anyone else.
- Do not save your password in your computer's memory.
- Do not write your password down on a piece of paper.
- Finally, to ensure maximum security, change your password on a regular basis. Recommended is every 60 days.

Terminating a session

It is important to terminate your session once you've finished using a Collabria Website, whenever you must momentarily step away from your computer workstation, or when you leave your mobile device unattended.

For added security, clear your cache memory and close your browser.

This security procedure is particularly important if the computer from which you conduct your transactions is shared with other users.

Clear cache memory

Cache memory is a temporary memory store in your desktop computer or mobile device used to locally retain browsing history from a session. When you need to retrieve this information, your computer or mobile device gets it from the cache memory rather than from main memory where it was originally stored. Cache memory thus speeds up the retrieval and display time for information you consult while browsing.

At the end of your session on a Collabria Website, you could therefore have personal financial data in your computer or mobile device cache memory. To protect the confidentiality of such information, make sure that you clear the cache memory at the end of each session. Please refer to your browser instructions if you need assistance clearing your cache.

Close browser

Closing the browser is the simplest and most secure way of terminating your session as it deletes stored information, which ensures that your data cannot be accessed.