MERIDIAN PRIVACY & SECURITY NOTICE

Meridian Credit Union's ("Meridian") Privacy and Security Notice together with any privacy related provisions included in the agreements you have with us form our privacy policy. This policy applies to the collection, use, or sharing of any personal information collected by Meridian in the course of conducting its business and will continue to apply for so long as we may hold your information (including for a reasonable time after the termination of your relationship with us.) By providing us with information, you are consenting to the collection, use or sharing of your information as set out in our privacy policy.

Meridian is dedicated to protecting your privacy and your personal, business and financial information. We carefully follow privacy policies and security practices in everything we do, to support our commitment to you.

What We Collect and How We May Use or Disclose Your Information

When you apply for or open an account with us and through the course of our relationship we may collect, use and disclose certain information obtained from or about you to. Generally, we use this information to communicate with you, confirm your identify, satisfy legal or regulatory requirements, prevent fraud, maintain security, administer your accounts, offer to you and ensure your suitability and eligibility for products or services and to collect debts owed to us. Examples of how we collect, use or disclose your information include:

- Contact information, such as your name, address, email address, social media or other electronic addresses and telephone numbers, which we may use to communicate with you;
- Identity information, such as date of birth, nature of business or occupation. This information may be used to protect against fraud, money laundering or may be required by law for us to collect. As well we may collect identification documents such as a driver's license or other documents such as a utility bill. We use these items to verify your identity;
- Financial information, such as income, assets, liabilities, transaction history, payment history, credit history, and account activity. We may use this information to understand your needs, determine appropriateness, suitability or eligibility for certain products and services;
- Credit Bureau Information and other information about you, that we may use, disclose and collect from credit bureaus, credit reporting agencies or other financial services databases. We may do this to prevent against fraud or to ensure your suitability and eligibility for certain products, including pre-approved products.
- Social Insurance Number (SIN), which we use for tax reporting purposes when requesting interest generating products or other investment income generating products or to verify and report credit or other information with the credit bureaus and credit reporting agencies. Also we may use your SIN to confirm your identity as it allows us to keep your information separate from others, such as those with similar names. You may refuse to consent to the use of your SIN or its disclosure, except for purposes required by law, such as tax reporting.
- Health Information, for the purposes of providing optional insurance products or services. We may use a third party to provide credit insurance products or services, as such you consent for us to exchange information including health information with the third party insurance provider.
- Other individuals' information, such as names and contact information of beneficiaries, your spouse, dependents or references. This information may be required by law, or to provide certain protection to you or in the case of references to verify information you have provided.
- Recordings of telephone calls or other electronic communication. This is used to establish a record of the information provided to you by us and a record of your information and instructions to us and to maintain quality of the services we provide. We may also use video recording in and around our physical premises and ATMs to ensure your safety and ours and to prevent against fraud and other illegal activity.
- Electronic or computer information, such as IP addresses, information about your operating system, web-browser or internet connection. We may use this information for the reasons described within the notice, particularly for security purposes or to enhance your digital experience.
- Other information, that may help us to confirm your identify, satisfy legal or regulatory authority, collect a debt to us, prevent fraud, maintain security, administer your accounts or ensure your suitability and eligibility for products

or services.

We strongly encourage you to read this entire document together with your account agreements as other means of collecting, using and disclosing your personal information may be described within.

Our Canadian Privacy Principles

We are committed to protecting your privacy and your right to control the collection, use and disclosure of your personal information, whether it is under Meridian's control, or information that has been transferred to a third party for processing, in accordance with *Canada's Personal Information Protection and Electronic Documents Act (2000)*.

- **Accountability:** We have designated a Privacy Officer who is responsible for overall privacy governance and all employees are accountable for compliance to these principles. The contact information for our Privacy Officer can be found within this notice.

- **Identifying Purposes:** Before or at the time we ask you for personal information, we will identify the purposes for which it will be used or disclosed. We may ask for information about your identity, transactions, your application, financial behaviour, or other details particular to the product or service.

- **Consent:** You are always in control of your personal information. We require your knowledge and consent for the collection, use, or disclosure of personal information (except when specific legislative or circumstances apply) and we will explain how your information will be used and with whom it will be shared, in a clear, comprehensive and easy to find manner. We will make it easy to withdraw your consent at any time; however this may affect our ability to provide products and services, or fulfill our commitments to you. We will not collect, use or disclose your personal information without your consent, except where required by law, or sell your personal information to third parties.

- **Limiting Collection:** We only collect information needed for the purposes we have identified, or the products and services you have requested, and we only collect information by fair and lawful means. We keep this information only for as long as it is needed for the purposes described above, even if you cease to be a Member.

- **Limiting Use, Disclosure and Retention:** Unless you consent otherwise or it is required by law, your personal information will only be used or disclosed for the purposes it was collected. We retain your documentation for the longer of: (a) the duration required to provide products, services or commitments to you; and (b) our legal and regulatory requirements This may require us to retain your information beyond the end of your relationship with us, however we will securely dispose of your personal information when we no longer need to retain it. You acknowledge that we may use third party service providers that operate outside of Canada, as a result, your information may be securely used, stored or accessed in other countries and be subject to the laws of those countries. For example, information may be shared in response to valid demands or requests from government authorities, courts and law enforcement officials in those countries.

- **Accuracy:** To ensure we are able to satisfy the purposes for which you have provided your personal information, we will list specific items of personal information. If you believe you the personal information we have retained about you is inaccurate, you may request that we review and correct any errors.

- **Safeguards:** We will protect your personal information with appropriate physical, technological and organizational safeguards relative to the sensitivity to the information, regardless of the format in which we hold it (physical or electronic) and even when it is being disposed. We regularly train our employees on the importance of maintaining the confidentiality of your information. Please note your information may processed by our service providers in other country By using our products or services, you consent to the transfer of information to countries outside of Canada — including the United States — which may provide for different data protection rules.

- **Openness:** We will make clear, easy to read and consistent information about our policies and practices relating to the management of personal information readily available in writing, by telephone, in publications and on Meridian's website. We will include details of who is accountable for these policies and practices; to whom access requests may be sent; and to whom concerns may be addressed. We will also describe what personal information (if any) is made available to other (including subsidiaries or parents) and why. We will not sell your personal information.

- **Individual Access:** Upon request, we will inform you as to the existence, use, and disclosure of your personal information and be given access to that information. You are entitled to question the accuracy and completeness of the information and have it amended as appropriate. We will endeavour to provide this information to you within 30 calendar days, however occasionally we may need additional time and we will communicate these reasons to you. You may access the information we have retained about you by contacting our Privacy Officer.

- **Challenging Compliance:** You are able to challenge our compliance with the above Privacy Principles. We have simple and easily accessible complaint procedures and we will take appropriate measures to correct information handling practices and policies, where deficiencies are identified. We will notify you of the outcome of investigations.

  For further information on PIPEDA, please visit: https://www.priv.gc.ca/en/privacy-topics/

Privacy Preferences

To manage your privacy preferences including marketing preferences or to refuse or withdraw consent, please contact or visit your local branch or contact our Contact Centre:

Meridian Contact Centre, Toll Free:
1-866-592-2226 (request your Branch Manager)
Email: MeridianContactCentre@meridiancu.ca

You may also contact us by mail or online:

Meridian,
Attention: Privacy Officer

3280 Bloor Street West Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Email us: privacyofficer@meridiancu.ca

Have a Concern About Privacy?

Meridian™ is committed to providing you with the best Member experience that we can.

If you have a concern about privacy, please follow our easy 3-step Member Concern Handling Procedures ("MCHP").

Step 1: Talk to your Branch, Wealth or Business Banking Representative
How to contact your Branch, Wealth, or Business Banking representative
Call your home branch directly. You can find branch contact information with our Branch Locator.

Get in touch with your branch through our Contact Centre
Call Toll Free: 1-866-592-2226. Select option 1 (request your Home Branch)
Call International Collect: 1-416-597-0165
Email: MeridianContactCentre@meridiancu.ca

Step 2: Contact your Branch Manager

How to contact your Branch Manager
Call your home branch directly. You can find branch contact information with our Branch Locator.

Get in touch with your branch through our Contact Centre
Call Toll Free: 1-866-592-2226. Select option 1 (request your Home Branch)
Call International Collect: 1-416-597-0165
Email: MeridianContactCentre@meridiancu.ca

Step 3: Contact the Privacy Officer

How to contact Meridian's Privacy Officer
Email: privacyofficer@meridiancu.ca

Mail:
Privacy Officer
75 Corporate Park Drive
St. Catharines, ON L2S 3W3

Note: If corresponding by email, please do not include any confidential information as email correspondence is not guaranteed to be secure.

If you want more information or are still not satisfied after contacting Meridian's Privacy Officer, the following external agencies can provide you with information and a further review of your concern:

Office of the Privacy Commissioner of Canada (OPC)

The OPC oversees compliance with Canada's privacy laws, and you can contact them at any time with a privacy complaint.

Toll-free: 1-800-282-1376
Online Form: On the OPC website

Mail:
Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Note: If corresponding by email, please do not include any confidential information as email correspondence is not guaranteed to be secure.

Our European Privacy Principles

While Meridian Credit Union does not have operations in Europe, we are committed to ensuring to full transparency to our Members residing in the European Union under the European Union's General Data Protection Regulation (2017) ('GDPR'), to ensure they are aware of all of the personal data we handle; specify how we protect their personal data; and provide greater control over how we use their personal information.

For further information on GDPR, please visit: http://www.knowyourprivacyrights.org

Meridian Contact Centre, Toll Free:
1-866-592-2226 (request your Branch Manager)

Your Online Privacy

Meridian offers you a variety of ways to bank and interact with us online. Our digital channels offer you control and convenience as well as access to our digital services.

Digital banking provides convenient access to information and the ability to perform transactions from home, work or other locations. It is important to be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or a virus in a very short period of time.

What we are doing to protect your security

Meridian Online Banking offers you the best security currently available in a commercial environment so that your personal and financial information is protected while in transit between your computer and our server. This is done through the use of industry standard security techniques:

- In addition to encrypted passwords, Meridian's Online Banking services offer enhanced security features, including the use of challenge questions, to help you identify that you are accessing Meridian's Online Banking site (and not a fraudulent site masked to appear as the legitimate online banking site). You will be asked to answer one of your personal challenge questions if you sign in to Meridian's Online Banking or Mobile Banking App from a computer or mobile device that you have not previously registered as 'trusted'.

- Encryption ensures that information cannot be read in transit or changed by scrambling the data using a complex mathematical formula. Some browsers can create a more secure channel than others, owing to the 'strength' of their encryption. Meridian uses the strongest channel available - referred to as 128-bit SSL (Secure Socket Layer). If you have a browser that only supports 'weaker' encryption such as 40-bit or 56- bit SSL, you will need to upgrade your browser before using our site. The longer and more complex the 'key' is, the stronger the encryption. The 40 and 128 refer to the length of the key. Since 128 is longer, than 40, it is more secure.

- Use of robust and multi-layered security of servers and applications, multiple layers of internal and external firewalls which protect Meridian's online environments.

- Regular reviews of our security practices and technology updates as well as regular reviews to ensure our security and privacy policies and standards reflect our industry leading position.

- Access to our databases is strictly managed and systems are in place to ensure security is not breached, including the physical security of our computer hardware and communications.

- Automatic session terminations - To help you protect your information, if there has been no activity for 15 minutes, you will be prompted that your session will be terminated and have the option to continue with your session, if not replied to within 5 minutes; your online banking session will end automatically.

What you need to do to protect your computer and password

Protecting your password and answers to your secondary challenge questions.

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected. In order for us to ensure that only you are accessing your accounts, we need a unique way of knowing that it's you. Just as the key to your home protects unwanted entry, the online banking 'key' - your password and your secondary challenge questions - ensures that only you can access your accounts.

It is your responsibility to ensure that your 'key' to Meridian Online Banking is protected. Please observe the following security practices:

- Select a password that is easy for you to remember but difficult for others to guess.
- Select your security questions that only you know the answer to.
- Select your security image and phrase that is easy to remember and meaningful.
- Do not select a part of your PIN (your ABM 'key') or another password.
- Keep your password and secondary challenge answers confidential - do not share.
- Do not write your password down or store it in a file on your computer.
- Never disclose your password to anyone for any reason. Ensure no one watches you type in your password.
- Change your password regularly. We suggest every 90-120 days.
- Members are reminded that any password that has been in use prior to March 2012 will be required to follow new requirements the next time their password is reset.

Protecting your computer

- Never leave your computer unattended while using banking services.
- Always exit the Meridian Online Banking using the logout button and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- Prevention of Browser Caching (storing of pages) is enabled by default when using Meridian Online Banking. This prevents secure pages and page information from being stored on your personal computer. It is also a beneficial security feature if you are accessing the site from a shared computer, such as at a friend's house or through a publicly-accessible computer, such as at a library or airport.
- Secure or erase files stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to "empty" the cache.
- Disable automatic password-save features in the browsers and software you use to access the Internet.
- Install and use a quality anti-virus program. As new viruses are created each and every day, be sure to update your anti-virus program often. It is recommended you update anti-virus definitions automatically. Scan all download files, programs, disks and attachments and only accept files and programs from a trusted source.
- Install and configure a personal firewall on your computer to ensure others cannot access your computer through the Internet.
- Install new security patches as soon as your operating system and Internet browser manufacturers make them available.

Protecting your information when using a public computer

You should be extra vigilant when using publicly available computers. Even if you adopt the tips above to protect your information, you need to bear in mind that even benign programs, like popular desktop search programs, can pose a security risk. Certain programs, such as Google Desktop, cache items that you have viewed so an unwelcome third party can easily search and find those pages again later.

To ensure a safe and secure Internet session, only visit reputable sites. If you visit any questionable web site before Meridian Online Banking, we recommend you close your browser and restart it before proceeding to Meridian Online Banking.

Fraud: Recognize it. Report it. Stop it.

Electronic identity theft can occur when you respond to a fraudulent email that asks for your personal banking information (This is called Phishing). Armed with this information, a person may be able to access your accounts or establish credit, pay for items or borrow money using your name. For this reason, Meridian uses different methods to help you confirm the Meridian Online Banking site is legitimate and secure. These include the selection of a unique personal image, challenge questions and answers and a unique personal code.

Safety precautions for online banking

We will never ask you for your personal passwords, personal information numbers or login information in an email. If you receive such an email:

- Do not click on any links contained in the email or reply to it;
- Immediately forward the e-mail to onlinebankingsecurity@meridiancu.ca.
- Delete the email once reported.
- Check the address of any webpages that ask you to enter personal account information. In the toolbar at the top of the page any legitimate banking web site will begin with 'https' to indicate that the page is secure.
- Look for the padlock found in the lower right corner of your screen. If the is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.
- Type in our web address yourself to ensure you are transacting with our server.
- Check your bank and credit card statements regularly to ensure that all transactions are legitimate.

By working together, we can defend potential online information security threats.

Contact Meridian at 1-866-592-2226 immediately if you suspect someone has gained knowledge of your password or if you suspect any loss, theft or unauthorized use of your account.

Our Cookie Policy

We use "cookies" as a fundamental part of our interaction with your web browser

A "cookie" is a small text file that's stored on your computer, smartphone, tablet, or other device when you visit a website or use an app. Some cookies are deleted when you close down your browser. These are known as **session cookies**. Others remain on your device until they expire or you delete them from your cache. These are known as **persistent cookies** and enable us to remember things about you as a returning visitor.

Our website **www.meridiancu.ca** ("our site") uses session and persistent cookies to distinguish you from other users of our site. This helps us to give you the best possible experience when you browse our site, and also allows us to improve our site. By using or browsing our websites, you're agreeing to our use of cookies.

All of this helps us to make our site better for you. For example, it means we can ensure you find what you're looking for easily and speed up your searches.

Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies. We have no control over these. Third party cookies are likely to be analytical/performance cookies or targeting cookies.

You can block cookies within your browser, by activating its setting that allows you to refuse all or some cookies. Please keep in mind that if you use your browser settings to block all cookies (including essential cookies), you may not be able to access all or parts of our site.

To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit **www.allaboutcookies.org**. Alternatively, you can search the internet for other independent information on cookies.

100%. Guaranteed.

Security is an integral part of everything we do.

Strong security is our digital backbone. We're committed to keeping your accounts and personal information safe and secure. In fact, we're so confident in our online security that in the unlikely event that *unauthorized transactions occur, we will reimburse you 100%. GUARANTEED.

Our commitment to you

We protect your online and mobile transactions and make sure they are as safe as possible. To protect the privacy and integrity of your information during transactions, our security safeguards include:

- **Strong encryption** technology to make sure that data passing between your PC and our web server is secure
- Digital certificates issued by trusted third-party companies to let you know that our **website is secure** and genuine
- **Automatic log out** after 20 minutes of inactivity
- Firewalls to **protect your information** with us
- **Immediate investigation** into any suspicious activity identified on your account

Your commitment to us

We can't do it all alone. We need you to do your part to help keep your information safe. This means that you'll need to follow the terms in your account agreements and the protection guidelines outlined under Your Online Privacy.

To receive reimbursement under this guarantee, you need to:

- Keep software up to date, including updated anti-virus and firewalls
- Always log out of your online banking sessions
- Keep your password confidential and secure and do not disclose it to any person
- Review your bank statements for suspicious activity as soon as you get them
- Do your own due diligence on all transactions
- Let us know about any **suspicious activity** right away. (If you think you are a victim of fraud, please call us immediately at 1-866-592-2226)
- Remember that email messages are not encrypted and they could be intercepted and read by third parties. Please don't send us any personal information by email
- Keep your Challenge Questions unique and hard to guess
- Take steps to protect yourself against *phishing and think twice before clicking on links embedded in emails asking you to log into your account
- Check the URL in your browser to make sure the website is authentic and look for the locked padlock icon. You can confirm a valid certificate by double-clicking on the locked padlock icon
- Don't use a public wireless network to log into your Meridian online banking or mobile application

Making these commitments to each other will keep your financial and personal information well protected and safe.

Remember, we'll **never** send you emails or text messages asking for personal information, your ABM PIN, your Challenge Question answers, or online banking password.

We always have your back.

We're always here for you and if you have any questions or concerns about the security of your Meridian accounts or Meridian's mobile services, please contact us at MeridianContactCentre@meridiancu.ca

*__Unauthorized Transactions__ means a transaction made on a Card or Account by any person or entity other than an Account User.
*__Phishing__ is a type of online fraud that asks you to disclose private information