Your Privacy is Important to Us

At Saskatoon City Employees Credit Union we are committed to protecting your privacy and safeguarding your personal and financial information. While the Internet is revolutionizing the way we do business - providing convenient access to financial services from your home or office - we recognize that it also brings concerns about Privacy and Security.

This Privacy Statement describes how your personal information is collected, used and disclosed within our Internet banking site. The Internet banking portion of our site is the area of our website that requires you to use your Login ID and Personal Access Code (PAC) before entering. By accessing our Internet banking site, you agree to the collection, use and disclosure of your personal information for the purposes described in this Privacy Statement.

Please note that this Internet Banking privacy policy is intended to supplement, and not replace, our full set of Privacy Policies and Practices. For more information on all of our Privacy Policies and Practices please contact us.

Controlled Access to your Information

To ensure that you are the only person who accesses your personal information, we restrict access to the Member*Direct*® site by requiring you to enter your Login ID and PAC to login. Only you know your PAC. Our employees do not have access to your PAC, and they will not ask you to reveal it. If someone does ask you to provide your PAC to them, you should refuse to do so and contact us immediately.
You are responsible to ensure that your Login ID and PAC are not disclosed to any other person. If you disclose your Login ID or PAC to any other person or become aware of or suspect any unauthorized activity has occurred or that your PAC or PIN may have been compromised, you are responsible to notify Saskatoon City Employees Credit Union immediately by contacting us in person or by telephone.

The practice of accessing your account information through publicly accessible computers and public wireless networks is strongly discouraged. The use of computers at locations such as Internet cafes, public libraries, hotel lobbies and public wireless networks such as "hotspots" to name a few examples, greatly increases the risk of possible unauthorized access to your accounts. Use of these access points are to be avoided.

In the case of accessing Business Accounts and Services, by the act of designating a person as a Business User, the business is authorizing that person to view information about the Business and if online transactions are permitted through the service, also authorizing to carry out online transactions on behalf of the Business, the Business accepts the responsibility for all losses that may arise from a Business Users misusing his or her authority in any way, either purportedly on the Business' behalf or for personal or other purposes. The Business and individual Business User will ensure that the Business User meets any eligibility or other requirements for online access that are communicated by us as part of the application process. The Business is also responsible for ensuring that any changes with respect to who is the authorized or designated Business User are appropriately managed by the Business and that passwords and other applicable user id or access information is managed accordingly.

Transactional Services

By design, our Internet banking site has many transactional functions such as transfers between accounts and bill payment functions. These transactions are all logged to ensure that your accounts are debited or credited appropriately, and that a history of each transaction is available to verify your account. We store and use your transactional information in the same fashion as if you had performed the transaction at a branch or any other service channel.

We may also use transactional information for servicing your account - for example, we may bill you for the particular transactions that you perform, or for the services that you use.

Creating a Secure Channel

To create a secure channel between your browser and our server, we use 128-bit Secure Socket Layer (SSL) encryption, the highest level available. To learn more about 128-bit SSL encryption, and our security policies, please view the security link.

Website Usage Statistics

We may collect information about how our account holders are using our Internet banking site. These usage statistics are only viewed in the aggregate - and are never tied to an individual.

We use this information for purposes such as improving the pages where our account holders are having difficulties, and to ensure that we have the appropriate infrastructure in place to service future needs.

The information collected may include your IP address, your browser type and your operating system, as well as data that is passively generated as you browse our Internet banking site, such as the number and types of pages visited, and the length of time spent per page and on our Internet banking site overall.

Our use of Cookies

We also use a key web technology called cookies. A cookie is a small information token that sits on your computer. As you use our Internet banking site, cookies are passed back and forth between our server and your browser. While cookies can be used for a variety of reasons, we only use cookies where they are of benefit to our account holders.

Specifically, we use two kinds of cookies - session cookies and persistent cookies. A session cookie exists only for the length of your browsing session and is deleted when you close your browser. A persistent cookie is a cookie that stays on your computer after you close your browser. A persistent cookie may or may not expire on a given date.

We use a session cookie to maintain the integrity of your Internet banking session. With each page that you visit, the cookie is passed back and forth between our server and your browser. We use the cookie to distinguish your session from the many others that may be happening at the same time. Our session cookies never store any personal information, such as your name, or date of birth, or financial information, such as your accounts and balances.

Most recent browser versions allow the user to set some level of control over which cookies are accepted and how your browser uses them. Many browsers will allow you to accept cookies from only known, reliable sites that you select, such as our Internet banking site. If you are concerned about cookies, we encourage you to upgrade your browser to a recent version and review the Help section of your browser to learn more about its specific control features.

Memorized Accounts Feature

We use a persistent cookie to store information to help you personalize our Internet banking site and to make it easier to use. For example, we allow you to make the login easier by remembering your Login ID within our Memorized Accounts feature. Since the Memorized Accounts feature is optional, this cookie only contains information that you have entered into it. We recommend that you do not use the Memorize Accounts feature on publicly available computers (such as at Internet cafes, airports or public libraries, or a home or office computer if it is accessible by persons other than yourself) to access our Internet banking site.

Logout Button

To help ensure that someone cannot access your personal information, always exit our Internet banking site using the "log out" button located at the top of every page and close your browser if you step away from your computer (since your browser may retain information you entered in the login screen and elsewhere until you exit the browser). When you exit using the log out button, we delete your session cookie so that your session cannot be resumed unless your Login ID and PAC are re-entered.

Enhanced Security Feature

Our Enhanced Security feature provides you even greater control over your privacy.

The Enhanced Security Feature prevents your browser from caching (storing in the computer's memory) those pages that you have viewed. Should you click on the "Back" button to view a previous page during a session, the page will be recalled directly from our server. Therefore, when you log out, no one will be able to view your information by clicking on the Back button, or by viewing the browser's History.

Once again, it is important to remember to always exit our Internet banking site using the log out button and close your browser if you step away from your computer. Also, please note that the Enhanced Security Feature does not prevent the caching of .pdf files.

Automatic Session Time-outs

In the event that you leave your computer without logging out, our Internet banking site has been designed to end your session automatically if our system detects that you have not provided any instructions or used the browser buttons to navigate for several minutes. To restart the session, you will need to provide your PAC again.

Email

General email is not secure since it passes through many points on its route from you to us. If you are using general email to communicate with us, we strongly recommend that you do not include personal financial information (such as account numbers), your PAC or other sensitive information within the email as we cannot guarantee its confidentiality on route to us.

When you email us your comments, questions or instructions, you provide us your email address and we use it to correspond with you. We then store your email and our replies to you so that we can refer to them in future. By sending us information or material, you grant to us an unconditional, irrevocable license to use those materials or information and you acknowledge that we may use any ideas, concepts or techniques that you send to us for any purpose, without compensation to you.

We will not provide your email address to any third party without your consent. We may use your email address to send you information about financial products or services that we think may be of interest to you. If you do not want us to contact you with product information by email, you may tell us so at any time and we will discontinue the practice.

If you have asked us to provide you with information on a regular basis, or if we email you information about our products or services, you may ask us to remove you from the list at any time. We intend to include instructions to unsubscribe from the list in every mailing, and on the site where you originally subscribed to the list.

The easiest way to tell if an email is fraudulent is to bear in mind that we will never ask you for your personal passwords, personal information numbers or login information in an email.

Service Partners

In providing our complete Internet banking service, we often use external service partners and suppliers to assist us. In performing their duties, these service partners may handle components of your personal information on our behalf. We ensure through our contracts with these partners that they handle your information with the same standard of care that you have come to expect from us. Our suppliers, like our employees, are bound to maintain your confidentiality and may not use the information for unauthorized purposes.

Some of our partners require that you first register with their service to permit us to tie their functionality into our Internet banking site. Registration for these external services will always be at your discretion. We may append personally identifiable data to this registration for the Partner to use to compare and validate the registration. You will always be notified of such an action during the registration process.

Links to Other Sites

Our Internet banking site may also contain links to other websites or Internet resources. As an example, from time-to-time we may provide links to Microsoft or Netscape to assist you in upgrading your Internet browser. However, Saskatoon City Employees Credit Union has no responsibility or liability for or control over these other websites or Internet resources or their collection, use and disclosure of your personal information. Always review the privacy statements of the sites you are viewing.

In addition, when banking online, check the address of any pages that ask you to enter personal account information. In the toolbar at the top of the page, any legitimate internet banking web site will begin with "https" to indicate that the page is secure.

Another safety precaution for online banking is to look to the padlock on your screen. If the page 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.

Contact Us

Please contact us if you have any questions or concerns about our Internet Banking Privacy Statement, or the practices of this site.

Protecting Your Privacy-We're in it together

This Privacy Statement originally came into effective September 1, 2003, was amended effective June 9,2008 and further amended effective July 23, 2010. As we continue to expand our online banking service to serve you better, and as new Internet technologies become available, we will need to review and revise this Privacy Statement. Please check the Privacy Statement on our Internet banking site regularly for changes. Changes to this Privacy Statement will apply to information and data collected from the date of posting and will not be applied to existing information held by us without your consent.