Income Cliniflex Website/Mobile App – Security and Privacy Policy

Security and Privacy Policy

We are committed to protect the security of our customers' transactions and the privacy of their personal information. We truly understand your concerns about transmitting and receiving confidential information online. We employ a wide range of methods to ensure this security.

The following are the security measures implemented.

- Physical security of our facilities and information stored in those facilities.
- Information obtained is stored on a secured server.
- Secure Socket Layer (SSL) is the encryption technology used in transmitting confidential and personal information between "income.com.sg" and its users.
- User passwords are encrypted in our database.
- Backup systems to ensure the security of critical data even in the case of a disaster.
- Additional verification procedures and second level password are implemented to protect more confidential information.
- Multiple levels of firewall between our internal computer systems and the Internet.
- Only valid username and password which identify each unique user will be allowed to log in to our secure web site(s). This ensures that only authorised users are admitted into our secure site(s).
- As an additional security measure, we log users out the session if there is no activity after a specific period.

Security Guidelines

Your Role In Safeguarding Your Personal Data And Account Information

Please ensure that your online password is kept confidential. Failure to do so exposes you to the risks of fraud and loss. We will not be responsible for losses suffered by customers as a result of:

- input errors or misuse of its Internet services;
- negligent handling or sharing of password;
- leaving a computer unattended during an online session;
- failure to report known incidents of unauthorised account access immediately.

The following are some security precautions that you should undertake when accessing the website/mobile app.

Checking For Authenticity And Security Of Website/Mobile App

Having both the username and password will help ensure that only permitted users can gain entry into online systems but there is also a need to check for authenticity and security of the website/mobile app.

- You should always check to ensure that the website address changes from http:// to https:// and, look out for a security icon in the form of a yellow lock when authentication and encryption is expected.
- You should also ensure that the website you are visiting belongs to NTUC Income ("Income") appointed vendor Adept Health Pte Ltd ("Adept"). Adept uses digital certificate and this can be found by clicking on the yellow lock icon.
- If you notice any discrepancy in the SSL certificate or there is a SSL server certificate warning, please terminate your login session and notify us.

Managing Your Username and Password

Your username and password identify you when you use our services. This also includes your One-Time Password (OTP) which is sent to your mobile phone via a SMS text message or your registered email address when you submit your username and password.

Following are some of the guidelines on managing your username, password and OTP.

- Ensure that your password and OTP are not exposed when you log in to our system/mobile app.
- Keep your password and OTP confidential at all times and do not divulge them to anyone.
- Do not allow anyone to use your username and password, as you are responsible for all transactions undertaken with your username and password.
- Do not use common or easy-to-guess passwords like your username, personal telephone number, birth date or other personal information.
- Memorise your password and do not write or record it anywhere.
- Do not select the option on browsers for storing or retaining username and password.
- Change your password regularly.
- Change your password immediately if you suspect that it has been disclosed to others.
- Never use the same password for other web-based services such as for email or online services, particularly when they are related to different websites/mobile apps.
- Do not use shared, public or Internet cafe computers to access our online portals.

Note:
No staff member or vendor should ever ask you for your password for whatsoever reasons. You must not reveal your password under any circumstances.

Take Precautions Against Virus, Trojan Horse, Worms and Spyware

Viruses and malicious software can capture password keystrokes and other personal information.

The following are some security precautions you should undertake.

- Do not use a computer or a device which cannot be trusted.
- Install anti-virus, anti-spyware and firewall software in your personal computers especially when you are using broadband connections, digital subscriber lines or cable modems.
- All the anti-virus, anti-spyware and firewall software products should be updated with security patches or newer versions on a regular basis.
- Do not install software or run programs of unknown origin.
- Do not open any email or attachment that is from an unknown source.
- Delete junk or chain emails.
- Update your operating system patches and service packs.
- Make regular backup of critical data.
- Consider the use of encryption technology to protect highly-sensitive data.
- Remove file and printer sharing in your PCs, especially when they have internet access via cable modems, broadband connections or similar set-ups.
- Do not disclose personal, financial or credit card information to little-known or suspected websites.

Remember To Log Out

Always remember to log out from your session when you have completed your transactions. Do not leave your computer unattended while Internet transactions are being processed.

Clear Your Browser's Cache

It is strongly advised that you clear your browser's disk cache after each session for both website/mobile app. Default files on a computer, called 'cache' files, can retain images of data sent or received over the Internet, making them a potential target for a system intruder.

Disclaimer

We shall in no event be liable to you, our customers or any other party for any damages, loss or expense including without limitation, direct, indirect, special, consequential or punitive damages, or economic loss, loss of profits, loss of opportunity, loss of business or goodwill as a result of, arising from or in connection with the following:

- any breach in security measures that are undertaken by us;
- any system, server or connection failure, modification, suspension, discontinuance, error, omission, interruption, delay in transmission, or computer virus;
- your omission or failure to observe the terms and conditions set out in this Security Policy; or
- your negligence or fault.

Privacy Statement

1. This private policy is to explain to you our information practices, where information is collected and used by Adept.
2. If you are only browsing this website/mobile app or using the Search function, we do not capture data that allows us to identify you individually. This site automatically receives and records information on our server logs from your browser, including your IP address, and the page(s) requested. Although user sessions are tracked, the users remain anonymous.
3. If you choose to send an application or an e-mail that contains personally identifiable data, for us to process the application or to render you a service, we may share the relevant data within the organisation, or if necessary, with relevant third party, who have direct support or business relationship with us, so as to serve you efficiently and effectively.
4. For your convenience, when you are carrying out a transaction using your personally identifiable data, we may also display to you data that you had previously supplied to us. This will speed up the transaction and save you the trouble of repeating previous submissions. Should the data be out-of-date, please supply us with the latest data. We will retain your personal data only as necessary for the effective delivery of our services to you.
5. We may be required to disclose personal data as required by law or a court order.
6. Personally identifiable data may be used for statistical, marketing and research purposes. Many times, these data are aggregated and the individuals are remained anonymous.
7. Some of our sites contain links to other sites whose information practices may be different than ours. You should consult the other sites' privacy notices, as we have no control over information that is submitted to, or collected by, these third parties.
8. We have put in place appropriate physical, electronic and managerial procedures to safeguard and help prevent unauthorized access, maintain data security and correctly use the information we collect.
9. Adept reserves the right to modify this privacy policy statement at any time. Continued use of this website/mobile app or any of our service provided herein signifies acceptance of any of such modification.