LUCA

Security / Compliance / Privacy

Security

User Authentication

All Luca accounts are protected with a strong password enforced and two-factor authentication (2FA). 2FA can be implemented and configured to remain within the existing environment of your organisation, protected by current sign-on credentials.

Encryption

To ensure the confidentiality and integrity of your files, all content is encrypted in transit and at rest with world-class encryption and key management techniques. Encryption for data at rest is automated using encrypted storage volumes.

Restricted Network Access

Firewalls are utilised to restrict access to systems from external networks and between systems internally. All network traffic is encrypted using Transport layer Security (TLS), with flexibility to configure the minimum TLS protocol version.

Audit Trail

Luca creates a comprehensive and immutable audit trail between all parties that includes hash of data, timestamp, IP address and end-user information. All these are recorded to decentralised and distributed ledger that cannot be modified / changed once been created.

Key elements of the audit trail are appended to all executed signature requests and include an identifier that can be used as a proof to lookup the corresponding transaction log if required.

Banking Security

Luca bank reconciliation feature uses the same security measures required of banks and other financial institutions when transmitting data. The Luca client authorises data supplier to provide Luca with transaction data relating to the client’s nominated account through a secure, integrated software linkage, direct between data supplier and Luca.

Development Practices

Our development follows industry-standard secure coding guidelines, such as those recommended by OWASP.

Cloud Platform

Luca partners with world class suppliers who provide key infrastructure and services, such as monitoring for suspicious activity, physical security, server and power redundancy, and built-in firewalls:

- Microsoft Azure platform hosted in Australia
    - For details about Security, Privacy, and Compliance in Microsoft Azure, please visit here.
    - Microsoft Azure audits are performed as per http://azure.microsoft.com/en-us/support/trust-center/compliance/
- Amazon Web Services platform hosted in Australia
    - For details about Security, Privacy, and Compliance in Amazon Web Services, please visit here.
    - Amazon Web Services audits are performed as per https://aws.amazon.com/compliance/
- Google Cloud platform hosted in Australia
    - For details about Security, Privacy, and Compliance in Google Cloud, please visit here.
    - Google Cloud audits are performed as per https://cloud.google.com/security/compliance/

Service Partner

Luca integrates with leading service partners that provide transaction data. The Luca clients authorises service partners to provide Luca with transaction data relating to the client's nominated account through a secure, integrated software linkage, direct between data supplier and Luca.

- Xero - Security, Privacy and Compliance detail
- myob - Security, Privacy Policy
- Basiq - Privacy & Terms

Compliance

Information Security Management System

Luca is working towards certifying for ISO 27001, which is globally recognised as the premier information security management system (ISMS) standard. Luca is achieving certification by developing and implementing a robust security management program, including a comprehensive Information Security Management System (ISMS).

Luca is working towards Service Organisation Control (SOC 1). System and Organisation Controls (SOC) is a suite of service offerings CPAs may provide in connection with system-level controls of a service organisation or entity-level control of other organisations.

Auditing Standards

Luca complies with Standards on Auditing in Australia for External confirmation requests. (Auditing Standard ASA 230, 500, 505).

- Responses are direct from the confirming party, either through the Luca Platform or the evidence providers existing channel.
- The auditor maintains control at all times within the Luca Platform.
- Address validation is performed by Luca during any on-boarding process. For requests being fulfilled by providers setup by the audit firm, the validation process remains their own responsibility.
- The identity management, encryption and the secure environment provided by Luca mitigates against any risk of using the service over the paper based process.

E-Invoicing

Luca is working towards complying E-Invoicing framework when it’s finalised. E-invoicing relies on open standards and technology solutions to exchange invoices seamlessly, without manual input. It removes the need to create paper-based or PDF invoices, scan, post or email them, or manually enter them.

Privacy

Protecting your privacy and keeping your personal information confidential is very important to us. We're bound by the Privacy Act 1988, including the Australian Privacy Principles (APPs) set out in the Act, when we handle your personal information.

The Block Ledger Pty Ltd Privacy Policy (Policy) outlines how we maintain your privacy when handling your personal information if you're a client, a visitor to one of our websites or a member of the public, in Australia.

By using or accessing the Service in any manner, you acknowledge that you accept and agree to the terms, practices and policies outlined in this Privacy Policy, and you hereby consent that we may collect, use, and share your information as set forth below.
This policy does not apply to any website, product or service of any third-party company even if the website or application links to (or from) the Service. Luca does not operate those websites, products, or services - please always review the privacy practices of a company before deciding whether to provide any information to them.

Information we collect

In general, we collect information in a number of ways, including (i) when a client or end-user provides it directly to us via the Website and/or Service, (ii) when we obtain end-user information through trusted third parties including financial institutions, (iii) through your continued access of the Service, including data passively collected through technology such as "cookies". The types of information we collect and our use of that information will depend on whether you are a Website Visitor, Client, or End-User.

By signing up for the Service, whether directly on our site, with one of the third-party applications that uses our software, or by any other means, you consent to these terms. Some features of the Service allow you to provide content, including financial credentials and information, to the Service. All content submitted by you to the Service or collected on your behalf from a third-party (e.g., client) application or a financial institution (e.g., a bank) may be retained by us indefinitely, even after you terminate your account. We may continue to disclose such content to third parties in a manner that does not reveal Personal Information, as described in this Privacy Policy.

Cookies and IP Addresses

We automatically receive and record information from your web browser when you interact with the Service, including your IP address and cookie information. This information is used for fighting spam/malware and also to facilitate the collection of data concerning your interaction with the Service (e.g., what links you have clicked on). Generally, the Service automatically collect usage information, such as the number and frequency of visitors to the Site. We may use this data in aggregate form, that is, as a statistical measure, but not in a manner that would identify you personally. This type of aggregate data enables us and third parties authorised by us to figure out how often individuals use parts of the Service so that we can analyse and improve them. We may also receive a confirmation when you open an email from us. We use this confirmation to improve our customer service.

Cookies are pieces of text that may be provided to your computer through your web browser when you access a website. Your browser stores cookies in a manner associated with each website you visit. We use cookies to enable our servers to recognise your web browser and tell us how and when you visit the Site and otherwise use the Service through the Internet. Our cookies do not, by themselves, contain Personal Information, and we do not combine the general information collected through cookies with other Personal Information to tell us who you are. As noted, however, we do use cookies to identify that your web browser has accessed aspects of the Service and may associate that information with your Account if you have one. This Privacy Policy covers our use of cookies only and does not cover the use of cookies by third parties. We do not control when or how third parties place cookies on your computer. For example, third party websites to which a link points may set cookies on your computer.

Website visitors

To simply browse our Website, you are not required to provide any Personal Information. However, we may gather non-personally-identifiable information, as described directly above, just for the purposes of monitoring and improving our Website and the Service. We will not share this information with third parties except as a necessary part of providing our Website and the Service, nor will we use it to target any advertisements to you. Of course, if you sign up with or use any of our services, more information is shared.

Clients

When you use Luca services as a client, whether paid or unpaid, we will gather and store your name, company name, email address, phone number, billing address, and any other relevant information that you provide directly to us. Any and all test and/or live users that sign up as an end-user of your services fall under the end-user category. If you sign up for a paid account, we will also store the relevant data required to complete your transaction, including but not limited to your financial information, bank account numbers, routing numbers, billing address and company name. We may also rely on a third-party payment processor to complete transactions, and all data shared with them falls under their own privacy policies. Further, we will collect and associate all relevant end-user data with your client account, including but limited to end-user names, email addresses, billing addresses and financial information. We may additionally collect information on the IP addresses, devices, and locations used to access Luca, which may be linked to your account for fraud detection and prevention purposes. Finally, we may collect additional data for identity verification on an as-needed based determined at our own sole discretion.

End-Users

As an end-user of any application that utilises the Service, whether via a client or other third-party, directly via use of our API or other services, or through an application built by us directly, you are agreeing to share financial information with us, including, but not limited to, your account credentials, transactional histories, account numbers, and balances/limits as well as general identity data including names and addresses of all account holders. You are enabling us to interact with and through your financial institutions on your behalf and with your consent. We may also retrieve information pertaining to usage of our client applications and other general activity that comes through the use of the Service.
We collect statistical information about how both unregistered and registered users, collectively, use the Service ("Aggregate Information"). Some of this information is derived from Personal Information. This statistical information is not Personal Information and cannot be tied back to you, your Account or your web browser.

How We Use Personal Information

Luca uses your Personal Information as follows:

- To operate and maintain the Service (such as, overall operating and maintenance, providing customer service, fixing malfunctions, testing our security systems, etc.).
- To provide you with the features, functions and benefits of the Service (such as, displaying to information regarding your financial accounts).
- To enhance, improve, add to and further develop the Service (such as, creating new features or functions, refining or personalising the user experience, increasing Service technical performance, etc.).
- We will use your contact information (such as your email address or phone number) to provide you with Service notifications.
- To help personalise the Service experience for you (such as, remembering your information so you will not have to enter it each time you use the Service or providing you with offers, advertisements or features you may like).
- And for the other purposes referenced in the "Sharing and Disclosure" section below (such as, for the purposes of legal compliance).

Sharing and disclosure of your Personal Information

Luca does not sell or rent any personal information to marketers or third parties that have not been explicitly authorised (e.g., in the case of a client).

We may share your Personal Information with trusted third parties who are integral to the operation of our Website and the Service, including but not limited to financial institutions, payment processors, verification services and credit bureaus, as well as any third parties that you have directly authorised to receive your Personal Information.

We may store your Personal Information in locations outside the direct control of Luca, for instance, on servers or databases co-located with hosting providers.

If you authorise an application to access your Luca account, you acknowledge that we may share financial information with the third party that provides the authorised application. The use of your information by such third party will be subject to their applicable privacy policy, which you should carefully review.

We may also disclose your Personal Information to law enforcement, government officials, or other third parties if required by law or we believe in good faith that the disclosure is necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of our Terms of Service.

We may occasionally email you with information about offers or new services. You can opt out of these email communications by replying with unsubscribe in the subject line, or via an unsubscribe link included in such communications. However, you will continue to receive certain email communications related to your account including information regarding transactions and your relationship with Luca.

Protection of information

We take all reasonable steps to ensure that the personal information we collect, use or disclose is accurate, complete, up-to-date and relevant and stored securely.

Although no data transmission can be guaranteed to be 100% secure, we take reasonable steps to ensure that your Personal Information is accurate, complete, up-to-date, relevant and stored securely. We also take all reasonable steps to ensure that the personal information we hold is protected from misuse, interference and loss and unauthorised access, modification or disclosure by use of various methods including access limitation, and Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information.

Changes to this policy

We reserve the right to make changes to this Policy from time to time. Please review this Policy periodically to check for updates. If any changes are material and/or retroactive, we may provide additional notice and/or an opportunity to “opt-in,” as appropriate under the circumstances. We may also advise you of changes to this policy by emailing and/or mailing the revised policy to the address you provide us.

Contact Us

Email: security@theblockledger.net
Post: Ground Level East, 65 Southbank Boulevard, Southbank, VIC 3006, Australia