Sarcophagus Limited

GDPR Statement

Shared responsibility:

Working together to keep

your data secure

Shared responsibility:
Working together to keep your data secure

Sarcophagus Limited works with its business customers to keep their data secure. We take comprehensive measures to protect our infrastructure, network, and applications; train employees in security and privacy practices; build a culture where being worthy of trust is the highest priority; and put our systems and practices through rigorous testing and auditing.

While the Sarcophagus Limited development team is responsible for securing each aspect of the service that's under our control, customers play a key role in ensuring their teams and data are protected and secure. As the admin of a Sarcophagus Limited project team, you have the ability to configure, use, and monitor your account in ways that meet your organisation's security, privacy, and compliance needs.

We've put together this guide to help you understand what Sarcophagus Limited does to keep your account safe, and what you can do to maintain visibility and control over your team's data.

We hold data about you such as your name, email address, computer browser version, work address, telephone numbers, IP address, hardware information, auditing data, file transaction history. We can send you a full list of metadata that we hold about you on request. Should you leave your company, please let us know and we will remove you from the company and project channel. This will not remove the auditing and transaction records which will remain for legal purposes, however your personal name and contact information will not be available to third parties using the system.

Build security into our architecture

Thousands of businesses around the world trust us to protect their most important work. To earn that trust, we work hard to build secure products that admins like you can rely on. Here are some of the ways that we secure our architecture and networks.

Distributed architecture

The-project's architecture distributes your information, so it is difficult to access all your project specific data. This enhances security and makes processes faster and more reliable.

Secure networks

Strict procedures are maintained between the internal Sarcophagus Limited network and the public internet. Internet-bound traffic to and from the production network is carefully controlled through a dedicated, protected firewall with restrictive rules. Access to the production environment is restricted to only authorised IP addresses and requires authentication on all endpoints.

Encrypt user data

Sarcophagus Limited business customers interact with our systems through our mobile, desktop, and web applications, and APIs. Regardless of which app you're using, we protect your file data both in transit and at rest.

Data in transit

To protect data in transit between Sarcophagus Limited apps and our servers, Sarcophagus Limited uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a Sarcophagus Limited client (currently desktop, mobile, API, or web) and the hosted service is encrypted via SSL/TLS. For endpoints we control (desktop and mobile) and modern browsers, we use strong ciphers and support perfect forward secrecy and certificate pinning.

To prevent man-in-the-middle attacks, authentication of Sarcophagus Limited front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the transfer of any files and ensures secure delivery to Sarcophagus front-end servers.

Data at rest

Sarcophagus Limited passwords at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Files are stored in multiple data centres, one of which is a third-party hosting centre. Each file is renamed with a unique but random sequence of letters and not related to a client or specific project.

Maintain a reliable service

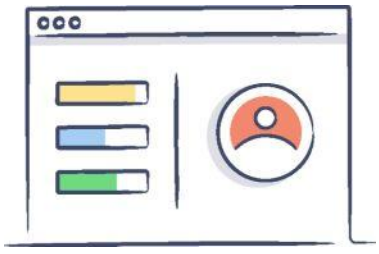
A storage system must be reliable, so we've developed Sarcophagus Limited with multiple layers of redundancy to guard against data loss and ensure availability. Redundant copies of metadata are distributed across independent devices within two data centres. Backups of files and metadata are as a single image backup of all the system and data disks. Data and metadata is replicated every hour to our own data centre.

In the rare event of a service availability outage, Sarcophagus Limited users should retain the original copies of their files on their local computers. Sarcophagus Limited files should be treated as a copy for dissemination to others rather than the original single copy.

We use SSL for all our pages and SFTP for management and users do not require any client software other than a browser (normally IE).

Limit employee access to backend systems

We are responsible stewards of your data so we ensure that Sarcophagus Limited employee access to our internal systems is strictly controlled. To start, access between our corporate and production networks is strictly limited. For example, production network access is SSH key-based and restricted to engineering teams requiring access as part of their duties.
Firewall configuration is tightly controlled and limited to a small number of administrators. Access to other resources, including data centers, server configuration utilities, production servers, and source code development utilities are granted through explicit approval by appropriate management.
Code is audited using the proprietary Vault software and this records the access and rollout of new code. Employee development changes and data cleansing requests, justifications, and approvals are recorded by management, and access is granted by appropriate individuals.



Maintain employee security and privacy awareness

Part of keeping our service secure is making sure that people who work at Sarcophagus Limited understand how to be security conscious and recognise suspicious activity. To that end, Sarcophagus Limited employees are required to acknowledge security policies prior to being granted systems access. Employees also agree to an internet acceptable use policy. They sign an employment contract to keep all data confidential and limit exposure to that data.

Validate our practices

To help us make sure that our security practices are working as intended, we use third parties to assess their effectiveness. Specialists perform periodic penetration and vulnerability tests on the Sarcophagus Limited corporate and production environments. Identified issues are prioritised and remediated by our security engineering team.

Communicate issues to you

Status of the service

Sarcophagus Limited makes available a standalone site to communicate the status of our service to The-project. As a current customer, you can visit the-project.com at any time to view the current site status, as well as past disruptions and maintenance.

Breach notification

Sarcophagus Limited will notify you in the event of a data breach, as required by applicable law. We maintain incident response policies and procedures, including a breach notification process, which enables us to notify affected customers as needed. If you've entered into a HIPAA Business Associate Agreement or an EU Data Processing Agreement, you will be notified as detailed in those agreements.

Give you the tools you need to be secure

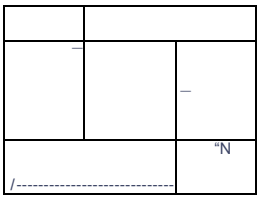
We want you and other Sarcophagus Limited admins to have the tools you need to make responsible, informed decisions about your team's security. To help you configure, use, and monitor your account in a way that meets your needs, your Admin Console comes equipped with security features for you to enable on behalf of your team. Through guides like our Support Centre, and our support team, we provide information to help you understand how these settings can help you responsibly configure your account.

Customer responsibilities

Learn about our practices

Determining if Sarcophagus Limited is the right fit for your company's needs is an important process. We encourage you to take the time to validate our practices, as you would with any other application. We can provide access to additional documentation such as our Business Continuity Plan and more detailed specifications under a non-disclosure agreement to help you make an informed decision. Our Terms of Service are available online for you to review and make sure that Sarcophagus Limited is a good fit for your team. Training is strongly recommended to ensure you fully understand how to implement and keep the system secure. For example, users sharing passwords will significantly reduce the effectiveness of our security and auditing and should be actively policed by each customer and company.

Configure sharing and viewing permissions



Sarcophagus Limited gives you flexibility to configure your account to support your security, collaboration, and privacy needs. Admins can review and modify these settings through the Admin Console to reflect their sharing or regulatory environment. For example, accounts can be configured so folders such as document classes etc. can't be shared with people outside of your team. When team members create shared folders for Sarcophagus Limited files, they can further customize the folders' settings and choose the appropriate level of access - edit or view-only.

Strengthen authentication

Strong authentication practices help keep your team's data safe. Sarcophagus Limited account authentication is used:

New user accounts

Team admins add a new user to a project by defining a name, email address and company they belong to. This process results in the system sending out an email to the new user with a one-time use password and unique username. The user must change the password in order to sign on to their account. Should the user forget their username or password, they can contact the support team for assistance who will carry out a diligent manual check to authenticate they are who they say they are.

Reset passwords

The password retention time is 180 days by default, but each customer can request a different retention time to suit their company practices and this can be applied to a customer template to provide standardization across all of the customer's project folders.
We have a strict password renewal and naming policy.

Conduct regular access reviews

Access to your team's account should evolve as your team membership, internal roles, and devices change. You should frequently check to make sure that only appropriate people, devices, and apps have access to your account to help keep your information in the right hands. Modifying or removing access is simple through the Admin Console.

Team members

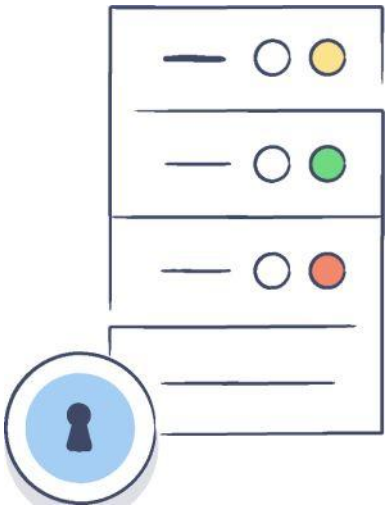
Team members can be easily added, removed, and reviewed from the Admin Console. To ensure sensitive data in your Sarcophagus Limited account can only be accessed by the right people, we recommend frequently reviewing this list. You can then remove access when someone leaves your organisation or no longer requires access due to a change in job role. Similarly, you can modify team members' roles in the Admin Console so that each user account has the appropriate level of access.

Devices

You and your team members should frequently review devices linked to your account and remove unused or unauthorised devices. Devices can be unlinked by both team members and team admins. You and your team members also have the option to remotely wipe Sarcophagus Limited content from you device when unlinking. Unlinking and wiping devices can keep your data secure in the event of loss or theft, or if someone is leaving your team.

Monitor for unusual activity

As a team admin, you can view reports that detail your teams file events, sharing, authentication, and administrator activities. Admins should regularly review these activity reports to keep an eye out for any unusual activity and help keep your team secure. You may also want to consider using a third-party SIEM or other monitoring integration to enhance your capabilities.



Determine encryption needs

Sarcophagus Limited original files should be kept on the originating company servers or computers and backed up as they are your legal records. To help keep them secure, we recommend that you enable disk encryption on your devices whenever possible, and require a strong and unique password to access your laptop, phone, tablets, server or any device that provides access to your Sarcophagus Limited account. Using strong and unique passwords on your devices will also protect access to your files.

Sarcophagus Limited protects files you upload in transit via 256-bit SSL encryption.

Sarcophagus Limited members may choose to also encrypt files before uploading them to Sarcophagus Limited on their own or through a third-party integration. However, users encrypting data before uploading it to Sarcophagus Limited are responsible for managing those encryption keys. Encrypting files before uploading them to Sarcophagus Limited may also reduce the functionality of some features.