Papyrs

Security Policy

May 31st 2018, rev 3.

This document describes the security policy for Papyrs. We believe that security is of paramount importance, and we have gone to great lengths to make sure the data of our customers is safe (i.e. no data loss) and secure (i.e. no unauthorized access).

General

1. All traffic between the Papyrs servers, and between Papyrs servers and end users is protected by strong SSL/TLS encryption.
2. Encryption Certificates are created and signed by GANDI, a certificate authority.
3. User passwords are hashed and salted. Passwords are never logged or stored in log files.
4. Administrative access to the Papyrs servers is restricted to key personnel with IP-filters and strong passwords/keys.
5. All key personnel understands computer security best practices and is required to treat all data as confidential.
6. All our servers are monitored for unusual software/network activity.
7. Suspicious or automated connection attempts (other than allowed according to our API policy) are blocked automatically.
8. Hard drives of staff workstations are encrypted at rest (full disk encryption).
9. All customer data is encrypted at rest (full disk encryption).
10. We keep (audit) logs of access to internal documents and servers.
11. Papyrs servers are protected by firewalls.
12. System software on the Papyrs servers is kept up-to-date. Security advisories are read and applied.
13. A virus scanner monitors the integrity of the system software on the Papyrs servers.
14. Credit card information is processed and stored by Stripe, a PCI compliant payment processor. We do not store or process your credit card number.
15. The Papyrs servers are physically secured and monitored 24/7. Datacenter details: Hetzner, TransIP, AWS.
16. Papyrs adheres to the European Union's **General Data Protection Regulation (GDPR)**, which took effect in May 2018. See our Privacy & GDPR section on our Terms of Service page.

Backups and redundancy

1. Backups are made of all client data every night.
2. Multiple sets of backups are kept in multiple locations.
3. Backups are transferred over an encrypted connection.
4. Backups are encrypted at rest.
5. In addition, user data is continuously mirrored to multiple (physical) servers.

We reserve the right to update and change the Security Policy without notice, provided that such updates and modifications do not result in the degradation of the overall security. The latest version of the Security Policy is available at https://a.papyrs.com/accounts/security/.

If you have any questions, concerns, or need to report an incident, please contact us at **team@papyrs.com**.