Security Policy

November 17th 2017, rev 1.

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 service 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.
5. Papyrs servers are protected by firewalls.
6. System software on the Papyrs servers is kept up-to-date. Security advisories are read and applied.
7. A virus scanner monitors the integrity of the system software on the Papyrs servers.
8. Credit card information is processed and stored by Fastspring or Stripe, PCI compliant e-commerce providers. We do not store or process any credit card data.
9. The Papyrs servers are physically secured and monitored 24/7. Security Brochure (pdf)
10. Papyrs adheres to the European Union's **General Data Protection Regulation (GDPR)**, which takes effect in May 2018.

General Data Protection Regulation – GDPR

1. Papyrs distinguishes between data stored by our customers on our platform and data stored by us about our customers.
2. The only Personally Identifiable Information (PII) Papyrs collects from its customers is what we need for invoicing purposes. Papyrs does not share PII data with third parties, except to provide our service (e.g. credit card information is sent to the credit card company for processing).
3. All data stored on our platform by our customers is treated as though it contains PII because all data *might* be sensitive and we don't know what our customers store on our platform (privacy).
4. When customers close their account all data they have stored on their Papyrs site will be destroyed. This happens in three phases: first the Papyrs site is deleted, then the local backups are deleted, finally the data from offline backups gets deleted (*right to erasure*). Pseudonymous data contained in system log files will be deleted as well.
5. Customers can download a backup of their Papyrs site that contains the content of the Pages, Attachments, Discussions, and Form Records in a portable format (*right to data portability*).

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. In addition, user data is continuously mirrored to multiple (physical) servers.

We reserve the right to update and change the Security Policy without notice. The latest version of the the Security Policy is available at https://accounts.papyrs.com/accounts/security/.

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