Security Policy

January 25th 2012, 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 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)

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**.