Security in StoryChief

Reliability

StoryChief manages all data via Amazon Web Services (AWS). All data is automatically backed up and stored redundantly. Thanks to our server and network infrastructure, StoryChief remains accessible even when hardware problems occur. We guarantee an uptime of 99.9% to continuously our services up and running. All information about security measures taken by AWS can be found here.

Authentication and payment data

All payment information is handled by our billing partner Stripe. No payment information is ever touched by our application.

StoryChief offers a multitude of authentication options. For the classis email + password authentication passwords are saved in hashed format using the Bcrypt hashing algorithm. Support for 2 Factor Authentication is available by default. Password-less authentication is possible with SSO.

Data Security & Privacy

All data is stored within the borders of the European Union. The data centres of AWS are distributed all over the world, but as far as the data of StoryChief (including backups) is concerned, this only applies to data centers in Ireland. AWS is fully compliant with the European Data Security Regulations (GDPR). Read here more about which data StoryChief stores.

Availability

StoryChief is available on any device, worldwide, with the exception of Internet Explorer 11 and earlier versions for security reasons. IE edge however is supported. Health checks and simple pings of the components are used to check if the functions are operational.

Release process

The StoryChief development team has implemented a structured release process:

- Integration and automatic end-2-end testing in CI ensures that updates do not break any use cases required by users.
- Changes are communicated to the customer success team in a timely manner.
- Test environments can freely be created upon request.
- Changes are communicated to end users in-app.

Data management

- Internal audit logs exist for each feature.

Security by design

- The StoryChief development team checks for owasp's top 10 security risks by default.
- Sqreen advanced intrusion detection and RASP is active on the platform.
- All access is based on roles by default.
- 2FA Authentication is supported by default.
- Brute force protection for authentication is provided.

Responsible Disclosure Policy

At StoryChief, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present. If you discover a security vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. Please check out our Responsible Disclosure Policy for more information.

Identity and Access Management (IAM)

StoryChief offers the following SingleSign-on (SSO) capabilities:

- Authentication is possible via gmail/google by default.
- Multi-Factor Authentication can be enabled by default.
- Authentication by SAML2 can be provided on request (Okta, Microsoft AD, ...).