Security in StoryChief

Security & Access Controls

- **Authentication Options:**
  - Classic email + password login secured with bcrypt hashing
  - Two-Factor Authentication (2FA) enabled by default
  - Password-less login via Single Sign-On (SSO)
  - SAML2-based SSO (Okta, Microsoft Entra ID, etc.) available upon request
  - Google Sign-In supported out-of-the-box
  - Brute-force protection implemented for all authentication flows
- **Access Management:**

  All access is role-based (RBAC), ensuring users only access data relevant to their permissions.

  Internal audit logs are maintained for each feature and user interaction.
- **Infrastructure Protection:**

  We use Aikido to continuously monitor our infrastructure and codebase for vulnerabilities and misconfigurations.

  Our team follows secure development best practices and actively mitigates OWASP Top 10 risks by design.

  All access and permissions follow the principle of least privilege.

Data Security & Privacy

- **Data Storage:**

  All StoryChief data is stored within the EU — specifically in data centers located in Ireland (AWS) and Belgium (GCP).

  These providers are fully compliant with European GDPR regulations.

Read more on what personal data is saved.

- **Data Encryption:** Data in transit is encrypted using TLS (HTTPS).
- **Payment Security:**

  We do not store or process any payment data directly. All billing is handled securely through our payment partner **Stripe**, which is PCI-DSS compliant.
- **Backups:**

  All data is automatically backed up and stored redundantly. Backup systems are tested and monitored regularly to ensure recoverability.
- **Data Retention & Deletion:**
  - Customer data is retained for the duration of the subscription
  - Upon termination or request, all data is securely deleted within a defined timeframe in accordance with GDPR

Reliability & Availability

- **Cloud Infrastructure:**

  StoryChief runs on a hybrid cloud setup utilizing **Amazon Web Services (AWS)** and **Google Cloud Platform (GCP)** to ensure speed, resilience, and scalability.
- **Uptime Guarantee:**

  We offer a 99.9% uptime SLA, and our server architecture ensures continued availability even in the event of hardware failures.
- **Global Accessibility:**

  The platform is available globally on all modern devices and browsers (excluding Internet Explorer 11 and earlier for security reasons). Microsoft Edge is fully supported.
- **Monitoring & Health Checks:**

We use continuous health checks and pings to monitor service status and platform performance.

Testing & Vulnerability Management

- **Automated CI/CD pipelines** run integration and end-to-end tests to prevent regressions
- Regular internal code reviews and security scanning (via Aikido)
- Penetration testing is planned and scoped with external partners on a recurring basis

Vendor & Third-Party Risk Management

- All third-party tools and services go through a security and privacy evaluation
- We ensure our vendors follow strong security practices and maintain compliance

Disaster Recovery & Incident Response

StoryChief is committed to ensuring uninterrupted service and rapid response in the event of unexpected disruptions or security threats.

- We maintain a documented **Disaster Recovery Plan** to address infrastructure failures, data loss, and operational downtime.
- Our systems are designed for high availability and rapid failover to minimize service disruption.
- A formal **Incident Response Plan** is in place to detect, assess, contain, and resolve any security incidents.
- In the event of a breach or critical incident, we promptly assess the scope and impact, and notify affected customers in accordance with regulatory and

contractual obligations.

Release Process

- Code changes are automatically tested and reviewed before deployment
- Customer Success is kept informed about upcoming changes
- In-app notifications are used to communicate relevant updates to end-users
- Test environments can be spun up upon request for custom QA or demo purposes

Responsible Disclosure

We actively encourage security researchers and partners to report vulnerabilities.

You can find our **Responsible Disclosure Policy** here.