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 vulnerability, we would like to know about it so we can take steps to address it as quickly as possible.

Focus Areas

- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Authentication or authorization flaws
- Server-side code execution bugs
- Sensitive data exposure
- Particularly clever vulnerabilities or unique issues that do not fall into explicit categories

In case you've found a security vulnerability, please do the following:

- Please submit your findings to responsible-disclosure [at] storychief [dot] io instead.
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data.
- Do not disclose your finding to others until it is resolved.
- Do not use attacks on physical security, social engineering, distributed denial of service, spam, malware/hacking tools or vulnerability scanners.
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

The Ground Rules

- Do not attempt to gain access to another user’s account or data.
- Do not perform any attack that could harm the reliability/integrity of our services or data. DDoS/spam attacks are not allowed.
- Do not publicly disclose a bug before it has been fixed.
- Only test for vulnerabilities on sites you know to be operated by StoryChief. Excluded subdomains, e.g. blog.storychief.io, should not be tested.
- Do not impact other users with your testing, this includes testing for vulnerabilities in workspaces you do not own.
- Automated scanners or automated tools to find vulnerabilities may be blocked.
- Never attempt non-technical attacks such as social engineering, phishing, or physical attacks against our employees, users, or infrastructure.

What we promise you:

- If you have followed the instructions above, we will not take any legal action against you in regard to the report.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission.
- Once the vulnerability is resolved, we'll coordinate with you if and how details of your finding could be publicly disclosed.
- We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date.
- We will keep you informed of the progress towards resolving the problem.

> 💡 Please note that we can't currently provide compensation for any found issues. Plans for a bug bounty program do exists but are not concrete yet.

Thank you for your contribution to StoryChief's security! We greatly appreciate the effort you put into improving security at StoryChief.