channable

RESPONSIBLE DISCLOSURE OF SECURITY VULNERABILITIES

We appreciate responsible disclosure of security vulnerabilities. This document details our stance on reported security problems. No matter how much effort we put into system security, bugs and accidents can happen and security vulnerabilities can be present.

If you discover a vulnerability, we would very much like to know about it so we can take steps to address this as quickly as possible. In such circumstances, we would like you to inform us so we can take appropriate action.

PLEASE:

- Email your findings to security@channable.com. Encrypt the contents of your emails using this GPG key.
- 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 reveal the problem to others until it has been resolved. We take any reports extremely seriously and will get back to you as soon as possible.
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties.
- Provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible.

WE PROMISE:

- To respond to your report within 3 business days with our evaluation and an expected resolution date.
- If you followed the instructions above, we will not take legal action against you in regards to your report.
- We will handle your report with strict confidentiality and will not pass on your personal details to third parties without your permission.
- We will keep you informed of the progress towards resolving the problem.

This policy was adapted from Floor Terra's example policy from
https://responsibledisclosure.nl