Security Disclosure

The Causeway Security Disclosure Policy

Causeway takes the protection of our customers' data very seriously and acknowledges the valuable role that well-intentioned independent security researchers play in internet security. As such, we welcome responsible reporting of any security vulnerabilities that may be found in our site or applications. A security vulnerability is something which impacts the confidentiality, integrity, or availability of Causeway data, its applications or its systems or its customers' data.

Causeway is committed to working with security researchers to verify and address any potential security vulnerabilities that are reported to us.

Causeway will not seek prosecution of any security researcher who reports any suspected security vulnerability in good faith and in accordance with this policy.

Please review these terms before you test and/or report a vulnerability.

Reporting a potential security vulnerability

Full details of the suspected security vulnerabilities should be privately reported by sending an email to security@causeway.com

Guidance

Whilst we welcome responsible reporting of security vulnerabilities,

You must NOT:

- Disrupt any Causeway or its customers' services or systems
- Perform actions that may negatively affect Causeway, its customers or its users (e.g. spamming denial of service attacks etc)
- Access, destroy or corrupt, or attempt to access, destroy or corrupt, data or information that does not belong to you
- Conduct any type of physical or electronic attack on Causeway personnel, property or its partners' data centres
- Social engineer or violate the privacy of any Causeway personnel
- Breach any laws or any agreements in order to discover security vulnerabilities

You must:

- Always comply with legislation/regulation rules and must not violate the privacy of any data Causeway hold. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by law).

This policy is designed to be compatible with common good practice among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Causeway to be in breach of any of its legal obligations, including but not limited to (as updated from time to time):

- The Computer Misuse Act (1990)
- The Data Protection Act 2018
- The UK General Data Protection Act 2021
- The General Data Protection Regulation 2016/679 (GDPR) The Copyright, Designs and Patents Act (1988)The Official Secrets Act (1989)

Causeway affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a Causeway service or system, where the researcher has acted in good faith and in accordance with this disclosure policy.

What you can expect from Causeway

Please do not share or publicise an unresolved security vulnerability with any third parties. If you responsibly submit a vulnerability report, the Causeway security team will use reasonable efforts to:

- Acknowledge receipt of your vulnerability report in a timely manner
- Try to validate and reproduce the issue and will prioritise through our internal process
- Notify when the vulnerability has been resolved
- Thank every individual who submits a vulnerability report helping us improve Causeway's security.

It is not currently possible for Causeway to offer a paid bug bounty programme at this time, however we will make every effort to give discovery credit to security researchers who take the time and effort to investigate and report security vulnerabilities to us according to this policy.

Feedback

For any feedback or queries relating to this policy, please email security@causeway.com

Document Control

Version	Version Date	Changes	Author
V1.0	Dec 2022	Live document	Hywel Evans
V2.0	Feb 2024	Amendments to provide further clarity on the process steps each party must take where a security vulnerability is reported	Hywel Evans