Vulnerability Disclosure

Note: we do not offer monetary rewards for vulnerability disclosures

Promise: (In development)

Scope: (In development)

"Safe Harbor": (In development)

Process: (borrowed from https://www.cpacanada.ca/en/vulnerability-disclosure-policy while we develop our own policy)

> ### *You must NOT:*
>
> - *Break any applicable law or regulations.*
> - *Access unnecessary, excessive or significant amounts of data.*
> - *Modify data in the Organization's systems or services.*
> - *Use high-intensity invasive or destructive scanning tools to find vulnerabilities.*
> - *Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.*
> - *Disrupt the Organization's services or systems.*
> - *Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example, missing security headers.*
> - *Submit reports detailing TLS configuration weaknesses, for example, “weak” cipher suite support or the presence of TLS1.0 support.*
> - *Communicate any vulnerabilities or associated details other than by means described in the published security.txt.*
> - *Social engineer, ‘phish’ or physically attack the Organization's staff or infrastructure.*
> - *Demand financial compensation in order to disclose any vulnerabilities.*
>
> ### *You must:*
>
> > - *Always comply with data protection rules and must not violate the privacy of the Organization’s users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to secure data retrieved from the systems or services adequately.*
> >
> > - *Securely delete all data retrieved during your research as soon as it is no longer required or within one month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).*

Preferences: (In Development)