Powershop Responsible Disclosure Statement

Statement

We're stoked you're helping us keep Powershop secure. If you've spotted a security issue in our systems, we're all ears. We're dead serious about protecting your info and our services, and we're always looking for ways to level up our security game. In this document, when we say "Powershop," "we," "us," or "our," we're referring to Powershop Limited and our related companies.

How you can help

We love your feedback! If you think you've found a security issue, letting us know is a huge help in keeping our systems secure and your info private. We'll work with you to understand and fix the issue ASAP. Just remember to stay within the lines outlined in this document. Please act only in the scope of this document.

Note: Powershop doesn't offer pay bug bounties or rewards for reported security issues.

Acting responsibly

To keep things safe for our customers and stakeholders, here's what we need from you when testing or reporting security issues:

- **Protect Privacy:** We're all about keeping things confidential. You must protect people's privacy and not access, use, copy, store, or share personal information, in line with the Privacy Act 2020.
- **Protect Data Integrity:** Only view the minimum info needed to confirm the security issue and leave all our data unchanged - we're all about keeping things intact.
- **Prevent Disruption:** Do your testing in a way that doesn't impact, degrade, or disrupt our systems - we want to keep things running smoothly.
- **Maintain Confidentiality:** Keep all details of the security issue confidential and only share them with Powershop through our approved reporting channels. Don't spill the beans about any security issues you've found until we've had a chance to fix them and agree on coordinated disclosure.

Our commitment to you

If you act in accordance with this Responsible Disclosure Statement and act in good faith, we commit to:

- **No action:** Not take action if in our reasonable opinion you have done good-faith security research and have acted in accordance with this statement.
- **Communication:** Keep you in the loop and communicate clearly, including an initial confirmation within 7 days.
- **Protect confidentiality:** Treating the information you share with us as confidential; between us and our suppliers, except with those who need to know to investigate and fix the issues, unless we have to act under the Privacy Act 2020.
- **Give you a shoutout:** Consider giving you a shoutout with a letter of acknowledgement if you're the first to report the issue and we make changes based on it.

Scope

In-scope:

- Online services operated under powershop.nz domains.
- Other domains and online services Powershop or our related companies own or operate.
- If you do not know if a service is within scope, please email us at ResponsibleDisclosure@powershop.co.nz.

Reporting Active Threats:

We encourage you to report any active or imminent threats to Powershop you may have observed or know of. If you've got intel on an ongoing attack, phishing campaign targeting Powershop or our customers, or leaked Powershop data, please let us know immediately at: ResponsibleDisclosure@powershop.co.nz.

Out of scope (prohibited testing):

The following test types and findings are excluded from the scope:

- Network level Denial of Service (DoS/DDoS) attacks.
- Social engineering, for example, phishing, spear phishing, whaling.
- Physical testing such as office access, tailgating.
- UI and UX bugs and spelling mistakes.

How to report a security issue

If you believe you've found a security issue in one of systems, please let us know by emailing: ResponsibleDisclosure@powershop.co.nz.

Include the following details:

- The type and location of security issue.
- How you found the security issue.
- Whether the security issue has been published or shared with others.
- Affected configurations.
- Potential exposure of any personal information.
- A detailed description of the steps required to reproduce the issue or risk, for example, proof of concept scripts, screenshots, and compressed screen captures are all helpful to us.
- Your name and contact details.

How to remain anonymous

The National Cyber Security Centre (NCSC) operate a coordinated vulnerability disclosure process where the finder of a security issue can use NCSC to notify affected vendors: https://www.ncsc.govt.nz/report/how-to-report-a-vulnerability/