Responsible Disclosure Standard

The Network for Learning Limited ("N4L") takes the security and privacy of our information seriously. If you identify a security issue with our systems, please tell us so that we can get it fixed.

This Responsible Disclosure Standard is designed to help both you and N4L when you find a security issue with our systems.

We won't take legal action against you, or suspend or terminate your access to our services when you follow these guidelines when reporting the issue to us. We reserve all of our legal rights if you do not follow this Responsible Disclosure Standard.

1. Reporting a security issue or vulnerability

1.1 If you believe you have found a security issue or vulnerability in one of our products or platforms, please notify us as soon as possible by emailing security@n4l.co.nz.

1.2 Please provide a clear explanation of the issue, including the following details:

(a) the nature and type of security issue;

(b) how you found the security issue;

(c) whether the security issue has been published or shared with others;

(d) any exposure or potential exposure of any personal information;

(e) the location and potential impact of the security issue;

(f) a suggested patch or remediation if you are aware of how to fix the vulnerability; and

(g) a detailed description of the steps required to reproduce the security issue. (Proof of concept scripts, screenshots, and compressed screen captures are all helpful to us)

1.3 By submitting your report to N4L, you agree:

(a) not to disclose the security issue to anyone other than N4L;

(b) to keep all communication with us confidential, unless we agree otherwise in writing;

(c) that we may use, distribute or disclose information provided in your report; and

(d) to keep any data, code or exploit details secure until N4L asks for those details to be destroyed.

1.4 If you transfer data, code, or exploit details to N4L you must use a secure file transfer service (for example, PGP keys in a security.txt file).

2. Our commitment to you

If you have identified a security issue within our systems and notify us in accordance with this Responsible Disclosure Standard, we commit to:

(a) working with you in good faith to understand and resolve the security issue quickly;

(b) being as straightforward and communicative with you as we can;

(c) treating the information you share with us as confidential within N4L and our

suppliers, unless we must disclose it because:

    (i)   a third party discovers the security issue within our system before we have had the opportunity to resolve it; or

    (ii)   the information on the security issue is used to cause a privacy breach and N4L is required to handle the breach in accordance with the Privacy Act 2020;

(d)   not initiate legal action by way of a complaint to the New Zealand Police or any other relevant enforcement agency, provided you comply with this Responsible Disclosure Standard; and

(e)   In our discretion, recognise your contribution with a letter of acknowledgement if you report the issue and as a result we implement a corrective action based on the issue.

3. Scope of this Responsible Disclosure Standard

3.1   This Responsible Disclosure Standard only applies if you are doing security testing or research on:

(a)   online services operated under "n4l.co.nz" domains;

(b)   other domains and online services that are clearly identified as owned and/or operated by N4L; and

(c)   any other systems or services that N4L provides to its customers.

3.2   This Responsible Disclosure Standard does not apply to (and we strictly prohibit):

(a)   physical testing such as office access (e.g., open doors, tailgating);

(b)   social engineering (e.g., phishing, whaling);

(c)   research or testing of applications or systems not listed in clause 3.1 above;

(d)   UI and UX bugs and spelling mistakes;

(e)   network-level Denial of Service (DoS/DDoS) weaknesses;

(f)   destruction or corruption of (or attempts to destroy or corrupt) any data or information that belongs to N4L;

(g)   accessing, using, deleting, or disclosing any personal information or otherwise breaching the privacy of individuals;

(h)   anything that may disrupt our systems or slow our system down for users; and

(i)   any request for payment in connection with any identified or alleged security issue.

3.3   We reserve the right to commence legal action, including by way of a complaint to the New Zealand Police or other appropriate law enforcement agency, if you fail to act in accordance with this Responsible Disclosure Standard.

3.4   For issues that affect other providers, we suggest you contact CERTNZ who offer an anonymous reporting service for system security issues.

3.5   For issues that affect schools, please contact the Ministry of Education in accordance with its Responsible Disclosure Standard.

This Responsible Disclosure Standard was last updated with effect from 28 May 2024