Responsible vulnerability disclosure statement

The Queensland University of Technology seeks to build a trusted environment for individuals to disclose vulnerabilities in our products and systems. We encourage responsible security research through online communication channels, websites and/or direct communication.

Our program is based on ISO/IEC 29147 Information Technology – Security Techniques – Vulnerability Disclosure.

Vulnerability disclosure is a process through which individuals, such as users, vendors or security researches work together to find solutions that reduce risks associated with a vulnerability. It encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution before public disclosure.

We will not take legal action against security researchers acting in good faith in relation to the discovery and reporting of a potential security vulnerability. This is provided that all such potential security vulnerabilities are discovered and reported strictly in accordance with this Responsible disclosure statement.

Please note that as a public education institute we do not compensate individuals or organisations for identifying potential or confirmed security vulnerabilities.

If in doubt, please contact the Queensland University of Technology, Information Security Team by sending an email to security@qut.edu.au.

The following types of research are strictly prohibited:

- Any attempt to modify or destroy any data
- Executing or attempting to execute a denial of service (DoS) attack
- Sending or attempting to send unsolicited or unauthorised email, spam or any other form of unsolicited messages
- Conducting social engineering (including phishing) of University employees, contractors or customers or any other party
- Accessing or attempting to access accounts or data that does not belong to you
- Testing third party websites, applications or services that integrate with our services or products
- Posting, transmitting, uploading, linking to, sending or storing malware, viruses or similar harmful software that could impact our services, products or customers or any other party
- Exfiltrating any data under any circumstances
- Any activity that violates any law.

Should you discover any personal, financial or proprietary information please do not proceed any further and contact us immediately.

In the interests of effective use of our limited cyber security resources we would ask that you refrain from reporting trivial issues that are very unlikely to pose a risk to our users, systems or data, or issues discovered by automated tools and not further verified.

Reporting potential security vulnerability instruction

You can disclose potential security vulnerabilities to the Queensland University of Technology, Information Security Team by emailing security@qut.edu.au.

When reporting a vulnerability, you are encouraged to provide:

- an explanation of the potential security vulnerability, including details of any exploit with enough information to enable the security team to reproduce it
- a list of products and services that may be affected
- proof-of-concept code, scripts and screenshots
- your contact details for further communication.

We will do the following:

- contact you within three working days
- notify you when the matter has been addressed
- keep reports confidential (subject to any regulatory and legal requirements)
- keep your identity confidential unless you choose otherwise.