x-RD Vulnerability Disclosure Policy

x-RD Pty Ltd

06 February 2025

Document Information

Document Reference Information	
File Name	Vulnerability Disclosure Policy
Policy number	ISMS-DOC-A12-10
Classification	Approved for Public Release

Version Control

Version	Date	Author	Remarks
0.1	30/11/2022	Information Security Officer	First Draft
0.2	01/12/2022	Branding Partnerships Lead	Approved Public Release
0.3	06/02/2025	Marketing & Communications Lead	Branding Update

Document Approval

Title	Name	Signature	Date
Chief Operating Officer	Paul Smooker		03/03/23

Information Handling

The guidance, standard, policy or procedure information contained within this document is the property of x-RD Pty Ltd and is supplied without liability for errors or omissions. This information has been prepared for the staff of x-RD Pty Ltd who are authorised to use or copy the information only for the purposes for which it is intended, otherwise no other part may be reproduced, used or disclosed except as authorised in writing by the x-RD Pty Ltd Managing Director or an authorised delegate.

This document is classified as **APPROVED FOR PUBLIC RELEASE** and is to only be accessed by those with a requirement to do so.

This document is to be handled in accordance with the x-RD Pty Ltd Information Classification and Handling Standard

Table of Contents

Introduction

1. Background

The security of our systems and technology is a top priority to x-RD. We take every effort to keep our ICT systems secure. Despite our efforts, there may still be vulnerabilities.

This policy allows security researchers to share their findings with us. If you have found a potential vulnerability in one of our systems, services, or products, please tell us as quickly as possible. It is not x-RD's position to compensate you for finding potential or confirmed vulnerabilities.

2. What does x-RD's Vulnerability Disclosure Policy cover?

This policy covers:

- any product or service wholly owned by x-RD to which you have lawful access

This policy does **not** cover:

- clickjacking
- social engineering or phishing
- weak or insecure SSL ciphers and certificates
- denial of service (DoS)
- physical attacks
- attempts to modify or destroy data.

This policy does not authorise individuals or groups to undertake hacking or penetration testing against x-RD ICT systems.

This policy does not cover any other action that is unlawful or contrary to legally enforceable terms and conditions for using a product or service.

3. How to report a vulnerability to x-RD

- To report a vulnerability, email security@x-rd.com.au.

- Please include enough detail so we can reproduce your steps.

- If you report a vulnerability under this policy, you must keep it confidential. Do not make your research public until we have finished investigating and fixed or mitigated the vulnerability.

4. What happens next

We will:

- respond to your report within two (2) business days

- keep you informed of our progress

- agree upon a date for public disclosure