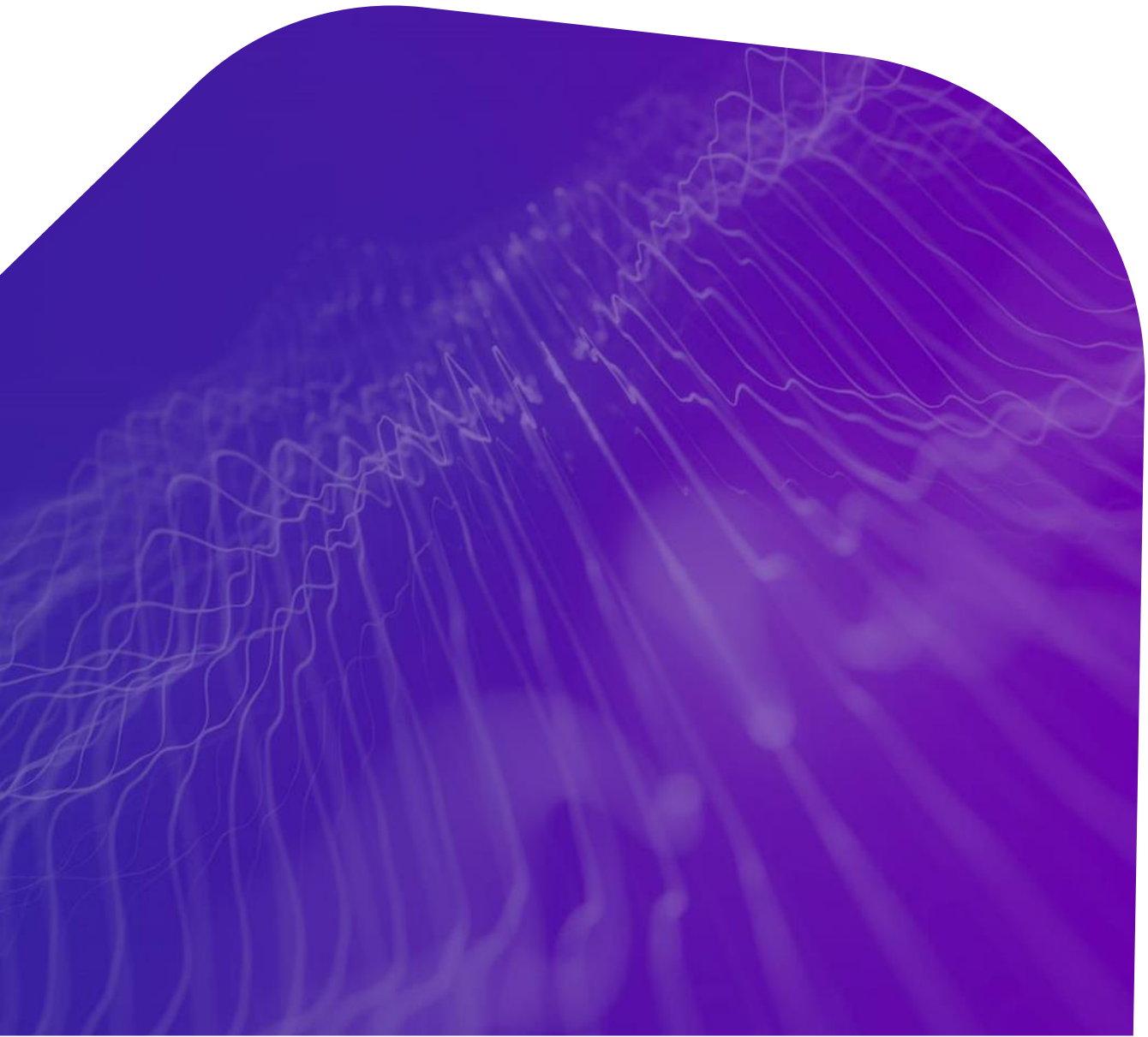
Vulnerability Disclosure Program (VDP)

MSP021



Securely Connected Everything™

Agenda

1. Document Control and Changes to this VDP

Version: 2.1
Effective date: 30 January 2025
Approved by: Chief Executive Officer
Next review: January 2027

Orro Group may update this VDP from time to time. Orro Group will publish the latest version of this Program on our website.

2. Classification

This document is classified as: Public.

3. Purpose

This Vulnerability Disclosure Program (**VDP, or Program**) applies to Orro Pty Ltd ABN 72 111 999 663 and its related bodies corporate (**Orro Group, we, us, our**). The purpose of the VDP is to provide a mechanism for external security researchers and members of the public (**Researcher, you, your**) to responsibly report potential security vulnerabilities or exploitation techniques which may affect the confidentiality, integrity and availability of Orro Group's systems, services or networks (**Reports**).

This VDP supports Orro Group's commitment to implementing appropriate security measures and risk management processes to endeavour to protect its systems and data, and efforts to continuously improve its cybersecurity posture, in alignment with the Australian Government Information Security Manual (**ISM**) and Infosec Registered Assessors Program (**IRAP**) expectations.

This VDP outlines permitted and non-permitted activities for Researchers, the procedure for making Reports, and how Orro Group will deal with any potential security vulnerabilities identified through the Program.

This VDP does not constitute an invitation or authorisation for Researchers to conduct security testing. Any testing outside the defined scope at clause 5 or without prior written consent from Orro Group is strictly prohibited.

4. Guiding Principles

Orro Group encourages responsible Reports and will endeavour to:

- Act in good faith when engaging with Researchers
- Investigate Reports in a timely and risk-based manner
- Communicate updates regarding the Report to the Researcher
- Support lawful and ethical security research that improves the security of Orro Group systems, services and networks

5. Scope

This VDP applies to:

- Externally accessible systems, services, applications and networks managed, operated, or hosted by Orro Group
- Internet-facing infrastructure, OneTouch Control (**OTC**), cloud services, web applications, Application Programming Interfaces (**APIs**), and supporting platforms managed, operated, or hosted by Orro Group

You are eligible to participate as a Researcher under this VDP if you meet all of the following criteria:

- You are 18 years of age or older
- You are an individual participating in your personal capacity, or you work for an organisation that permits you to participate (you are responsible for compliance with any policies of your organisation)
- You are not a resident of any country that is subject to any sanctions issued by the Australian Government

The following systems, services or networks are explicitly out of scope of this VDP:

- Internal Orro Group systems, services and networks not accessible from the internet
- Systems, services or networks owned and fully managed by third parties where Orro Group does not have administrative control
- Testing of any multi-tenant cloud resources, shared platforms, or services where Orro Group does not have exclusive administrative control

The following people are excluded from the scope of this VDP:

- Employees and officers of Orro Group (or individuals who were employees of officers of Orro Group within 6 months of the time they make a Report)
- Technology or security contractors engaged by Orro Group, their employees and any other individuals they directly or indirectly engage for work relating to Orro Group

6. Prohibited Testing Activities

To protect the confidentiality, integrity, and availability of Orro Group systems, services and networks, the following activities are strictly prohibited:

- Any action that may degrade, disrupt, or interrupt the performance of any of Orro Group systems, services or networks
- Denial-of-service (**DoS**) or distributed denial-of-service (**DDoS**) testing
- Data destruction or deletion, modification, damage to data integrity, or unauthorised exfiltration
- Accessing, downloading, using, altering, deleting or destroying personal information, customer information, or confidential information
- Any ransomware or related threats or activity
- Automated vulnerability scanning or fuzzing without prior written authorisation from Orro Group, regardless of performance impact
- Social engineering, phishing or other impersonation activities or attacks targeting Orro Group staff, customers, or partners
- Sending electronic messages to any person without their consent
- Posting any virus or malware on any system, service or network, or otherwise using, handling or deploying any virus or malware
- Breaching any applicable law

If you identify a security vulnerability you must not exploit it, including for any person's gain or for the detriment of Orro Group or any other person. Instead, you should describe in your Report the "proof of concept" as to how the vulnerability could be exploited by an attacker as set out in clause 7.2.

7. Reporting Vulnerabilities

You should submit a Report to Orro Group about potential or suspected security vulnerabilities or exploitation techniques as soon as they are identified as set out in clause 7.1.

7.1 Reporting Channel

All Reports must be submitted via:

- **Email:** isms@orro.group
- **URL:** https://orro.group/about/trust-security/ (Vulnerability Disclosure Form)

Orro Group will not accept Reports through other means.

Please do not direct other enquiries, such as enquires about our services or careers to the above channels.

7.2 Required Information

To assist timely investigation, Reports should include the following information:

- Name and contact information (email address or phone number) of the Researcher
- A clear description of the vulnerability, including evidence
- A list of affected systems, services, applications, networks, or URLs (as the case may be)
- Detailed steps taken to produce or verify the vulnerability, including relevant URLs, parameters and sample code
- Any suggestions you have about how to fix the vulnerability, such as any proof of concept, screenshots, or logs (where available)
- An assessment of potential impact (how an attacker could exploit it)
- Any other relevant information

Reports that lack sufficient detail may delay triage and remediation activities.

7.3 Post-Reporting

When you make a Report, Orro Group may, acting reasonably and in its sole discretion:

- Acknowledge receipt of your report
- Investigate and respond to your report, including to request further information
- Communicate status updates during triage and remediation of any vulnerability disclosed in a Report
- Undertake remediation planning and prioritisation, based on Orro Group's assessed risk, system criticality and business impact
- Disclose information from the Report and any Orro Group investigation to any regulators or law enforcement to comply with Orro Group's legal obligations (where required)

If the vulnerability in your Report may affect a third party, Orro Group may share non-identifying information from your Report with that affected third party but only after notifying you that we intend to notify the third party, and only after seeking that third party's confirmation that they will not pursue legal action against you (subject to the limitation in clause 0), unless it is reasonably suspected that you have breached the law in discovering the vulnerability.

Orro Group understands that the information in a Report may put a Researcher at risk. We will therefore limit what we may disclose to third parties to exclude any personal information about you without seeking your prior consent, unless we are required to disclose the information by a law or regulator as set out in this clause 7.3.

8. Safe Harbour

Orro Group supports responsible security research conducted in good faith and in accordance with this VDP. Safe harbour protections apply only where all of the following conditions are met:

- The researcher complies fully with this VDP and all applicable laws
- Testing is limited to systems, services and networks explicitly within the scope of the VDP as set out in clause 5
- Testing does not constitute any Prohibited Testing Activities as set out at clause 6
- There is no exploitation beyond what is necessary to demonstrate that the vulnerability occurs, without Orro Group's prior written consent
- Vulnerabilities are reported promptly and exclusively through the approved reporting channels in clause 7.1
- The researcher does not publicly disclose the vulnerability prior to receiving written consent from Orro Group

Where these conditions are met, Orro Group will not initiate legal action solely in connection with the reported vulnerability, unless Orro Group is otherwise required to do so by law or by a regulator. Orro Group cannot bind any third party, so you must not assume this Safe Harbour extends to any third party (including in relation to any third party as set out in clause 7.3).

Nothing in this VDP:

- Authorises access to data, systems, services or networks beyond what is strictly necessary to validate a vulnerability or as otherwise outside the defined scope of the VDP including but not limited to the Scope in clause 5
- Authorises activities conducted outside the defined scope of the VDP, including but not limited to the Prohibited Testing Activities contained in clause 6
- Waives or limits Orro Group's legal rights or remedies in cases of reckless, malicious, or negligent activity, or activity which otherwise breaches this VDP or the law, including rights under clause 11
- Constitutes permission, authorisation, or a defence to unauthorised access.

9. Confidentiality of Reports

Researchers must:

- Not disclose any Report (or any content in the Report) you have made to us to any other person except to the extent you are required to do so by law, the vulnerability comes into the public domain other than due to your breach of this obligation, or Orro Group provides its prior written consent
- Subject to receiving Orro Group's prior written consent above, not mention in any public communication without Orro Group's prior written consent, Orro Group, any of Orro Group's systems, services or networks, Orro Group's employees, customers, or service providers, and coordinate any public communication with Orro Group
- Not publish exploit code or technical details sufficient for reproduction until Orro Group confirms mitigation is in place

Orro Group retains sole discretion over the timing and content of any public disclosure in relation to its systems, services and networks.

10. Privacy

Reports may include personal information as defined under the *Privacy Act 1988* (Cth) (e.g., your full name, email, and other information about you that you include in your report) and technical artifacts (logs, screenshots).

Orro Group will collect, use and disclose this information for the purposes as set out in our Privacy Collection Notice for the VDP, including but not limited to administering the VDP, which may include using your personal information for facilitating your participation in the VDP, our triage, investigation or remediation activities associated with your report, for the ongoing review and improvement of our cybersecurity posture, to fulfil our legal obligations, to seek external professional advice (such as legal advice) where required, respond and engage with you in relation to the VDP or any report you make, communicate with you, and for other purposes as permitted by law.

Orro Group may retain Reports and any information contained within the Report for up to 24 months, or longer where required under law.

Orro Group will handle any personal information contained in a Report in accordance with its Privacy Policy available here.

By submitting your report, you confirm you have a lawful basis to share the information.

11. Limitation of Liability and Indemnity

To the maximum extent permitted by law, Orro Group is not liable for any loss, damage, or cost arising from Researcher activities.

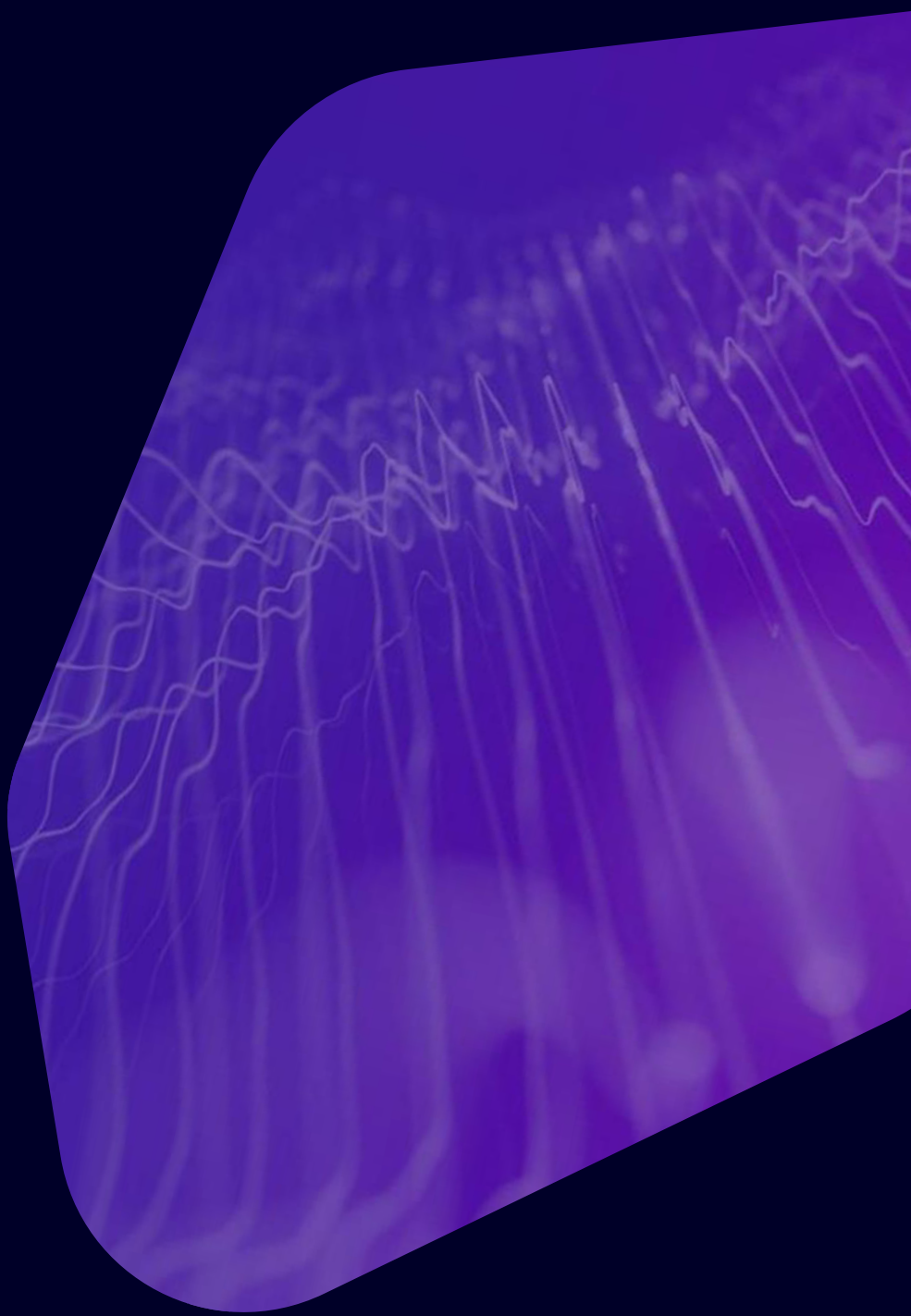
Researchers are responsible for their actions and agree to indemnify Orro Group to the extent permitted by law against claims or losses resulting from any breach of this VDP or applicable law, including but not limited to any unauthorised access to, or use or disclosure of, our systems and data, including the introduction of any harmful, destructive or disabling code which assists in or enables theft, alterations, denial of service, or unauthorised access, disclosure, corruption or destruction of data, arising from the course of your research over our security measures, system and data.

12. Governing Law

This VDP is governed by the laws of New South Wales, Australia, and any disputes arising out of or related to it shall be brought exclusively in the courts of New South Wales.

The future feels like this.®

1300 900 000
hello@orro.group
orro.group



Securely Connected Everything™

orro®