FirstWave

Responsible Vulnerability Disclosure Policy

Contents

1. Overview 3
1.1. Purpose of Document 3
1.2. Document Scope 4
1.3. Document Ownership and Review 4
1.4. Definitions 4
1.5. References 5
2. Policy 6
2.1. Our Commitment to Ethical researchers 6
2.2. Our Expectations for Researchers (Responsible Disclosure) 6
2.3. Exclusions and Forbidden Activities 6

1. OVERVIEW

FirstWave Cloud Technologies (FirstWave) is a leading Australian cloud security services company and provides design, transition, deployment and management services to customers moving / managing components of their security environment in the cloud. FirstWave also provides consulting and operations support services ancillary to its cloud security offerings.

The security of our systems and the trust of our users are paramount. We are committed to protecting our customers and our platform from security threats. We believe that a strong security posture benefits from the collaboration of security researchers and the broader community. This policy outlines our guidelines for security researchers to responsibly report vulnerabilities discovered in our systems. Patching of systems in a timely manner is now a vital component of maintaining the security of FirstWave's information assets, network and systems.

We appreciate the efforts of security researchers who help us identify and address potential weaknesses before they can be exploited. We commit to working with you to validate and respond to vulnerabilities in a transparent and timely manner, ensuring that our services remain secure.

1.1. Purpose of Document

The purpose of this document is to define and communicate the policy to determine when an ethical security researcher identifies public facing vulnerabilities and how it will be managed. It has been developed based on good industry practice, and with a view to minimising the impact on FirstWave's systems.

This policy is binding on all FirstWave employees, including contractors and consultants, who develop, view, transact and maintain information assets.
It is FirstWave's intention that this Policy is implemented, and that appropriate security measures and procedures are in place, supported by related policies, standards, guidelines, processes and procedures to ensure compliance.

1.2. Document Scope

This document relates to all FirstWave businesses and units. It is applicable to all levels of FirstWave staff, contractors and business partners. In exceptional circumstances, deviations or exemptions from this policy may be granted (refer to the Information Security Policy Deviation/Exemption from Policy [3]).

This policy applies to vulnerabilities found in:

- FirstWave public websites, including www.firstwave.com, www.cloudcontrolaws.firstcloudsecurity.com
- Any public facing instance of CyberCision, NMIS Suite, STM
- Any other internet-facing systems, services, or infrastructure owned, operated, or controlled by FirstWave

1.3. Document Ownership and Review

The Chief Executive Officer (CEO), of FirstWave is the owner of this document and has delegated the responsibility for maintaining the currency and accuracy of the document to the Chief Information Security Officer (CISO) who shall conduct a review of this document no less than annually.

1.4. Definitions

TERM	DEFINITION
Accountability	Responsibility of a person or entity for their actions and decisions
Asset	Anything that has value to FirstWave
Availability	Continuity of operational processes and recoverability in the event of a disruption.
BYOD	Bring Your Own Device
Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Control	A mechanism for managing risk (e.g. policy).
DoS	Denial of Service, a type of remote or local attack
Information Asset	Knowledge or data that has value to the organization. Interchangeable with Data Asset. In this context: Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems,

	storage media, network accounts providing electronic mail, browsing, VPN
Information Processing Facilities	Any information processing system, service or infrastructure, including the physical location housing them.
Integrity	The context of completeness, accuracy and resistance to unauthorised modification or destruction.
Media	In this context, refers to computer media such as hard drives, removable drives (such as Zip disks), CD-ROM or CD-R discs, DVDs, flash memory, USB drives, floppy disks as well as “hardcopy” media such as paper documents and files.
Risk	Risk is the uncertainty about deviation from an expected outcome. ISO 31000: “The effect of uncertainty on outcomes”
Risk Assessment	An assessment of the impact of risk and the adequacy of treatments to deal with the risk in the context of the RMF
Role	Within an organization, roles are created for various job functions
Sanitisation	In this context, the activities performed on an electronic device to ensure sensitive, personal and confidential information is securely wiped from the device before it is disposed of or redeployed.
Sensitive Data	Includes information assets classified at Confidential, Protected, or Highly Protected as per the Information Security Classification Standard
Staff	Employees and contractors of FirstWave. The term is used interchangeably with “users” in most sections of this document, unless there is a need to differentiate.
Teleworking	Teleworking allows staff to perform work duties from a remote location using communication tools, such as such as VPN, phone, fax, modem, Internet teleconferencing, e-mail or IM, etc.
User	Any entity (human or machine, with a legitimate reason to access FirstWave’s information assets

1.5. References

[1] FirstWave Information Security Risk Assessment and Treatment V0.3

[2] FirstWave Information Security Management System V0.43

[3] FirstWave Information Security Policy V0.51

[4] FirstWave Business Continuity Management Policy

2. POLICY

2.1. Our Commitment to Ethical researchers

Upon receiving a valid vulnerability report, we commit to:

- **Acknowledgement:** We will acknowledge receipt of the researcher's report.
- **Investigation:** We will thoroughly investigate the reported vulnerability.
- **Communication:** We will keep the researcher informed of our progress, including remediation efforts, within a reasonable timeframe.
- **Remediation:** We will work diligently to fix validated vulnerabilities.
- **Non-Retaliation:** We will not pursue legal action against researchers who follow this policy and disclose vulnerabilities responsibly.

2.2. Our Expectations for Researchers (Responsible Disclosure)

To ensure a safe and constructive process, we expect researchers to:

- **Do No Harm:** Make every effort to avoid privacy violations, degradation of user experience, disruption of production systems, and destruction or manipulation of data.
- **Responsible Testing:** Only test against your own accounts or with explicit permission from the account owner. Do not access, modify, or delete any user data that is not your own.
- **Private Disclosure:** Do not publicly disclose any vulnerability details until we have completed our investigation and remediation efforts and have provided explicit written permission for disclosure.
- **No Exploitation:** Do not exploit any discovered vulnerabilities beyond what is necessary to prove its existence and severity.
- **No Unauthorized Access:** Do not attempt to gain unauthorized access to our systems, data, or accounts belonging to others.
- **Comply with Laws:** Conduct all activities in compliance with applicable laws and regulations.

2.3. Exclusions and Forbidden Activities

Any activities that violate the terms of this policy or applicable laws are strictly forbidden. This includes, but is not limited to:

- Testing services in a manner that would degrade our service or impact our users.
- Attempting to gain access to customer data or accounts without explicit consent.
- Using automated tools that generate a high volume of traffic.
- Any form of social engineering, phishing, or spear-phishing against our employees or users.

4. FCT RESPONSIBLE VULNERABILITY DISCLOSURE POLICY - RATIFICATION AND SIGN OFF

Chief Executive Officer

Chief Executive Officer: Danny Maher

Review Date:

Signature:

Chief Information Security Officer

Chief Risk Officer: Tony Bishop

Review Date:

Signature:

REVISION HISTORY (filled out by Legal and Compliance Services)

Revision / Ref. No.	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Resolution / Change
IS18.01	Approved	31 July 2023	Board	

Policy Name	Responsible Vulnerability Disclosure Policy
Policy Manager	Chief Information Security Officer
Policy Department	Information Security
Contact	Tony Bishop Tel: +61 2 9409 7000 Email: tony.bishop@firstrwavecloud.com
Approval Authority	Board
Release Date	31 July 2023
Reviewed	21 November 2024
Distribution Level	All officers, employees and agents of FirstWave
Version Reference	IS18.01