**Head Office:**
Level 1, 255 Port Road
Hindmarsh, SA 5007.

**Phone:** (08) 8377 0101
**Fax:** (08) 8377 3911

# Eighty9 Limited and its wholly owned subsidiaries Status Works Pty Ltd and Allied Services Worldwide Pty Ltd

# Vulnerability Disclosure Policy

| Version Control | | | |
|---|---|---|---|
| Version | Date | Changes made | Changed by |
| 1.0 | 07/03/25 | Initial version | CIO |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Table of Contents

## Purpose

At Eighty9 Limited, we take the security of our systems seriously. We are committed to protecting our users, clients and visitors, and recognize the important role that security researchers and ethical hackers play in helping us achieve this goal.

If you discover a potential security vulnerability in any of our systems, we encourage you to report it responsibly. This policy outlines how to do so and what you can expect from us.

## In Scope

We welcome reports for:

- Any public-facing web assets under our control, related to any of our brands
- Web services or APIs provided by Eighty9 Limited
- User authentication and/or authorization issues
- Data leakage, access control, or permission escalation flaws

**Note:** Internally developed tools and non-public services are currently *out of scope* unless otherwise agreed.

## Not in scope

To protect our systems and avoid unnecessary disruption, please avoid:

- Distributed Denial of Service (DDoS) attacks
- Social engineering and/or phishing
- Physical intrusions or threats
- Spam, brute force attacks, or anything that degrades our services
- Automated vulnerability scans

## Reporting guidelines

Please include as much detail as possible:

- A clear description of the vulnerability
- Steps to reproduce the issue
- Any proof-of-concept (PoC) code or screenshots
- Your contact details (if you want recognition)

Please send reports to ict@eighty9.org.au. We aim to acknowledge your report within 3 business days.

## Recognition

While we don’t currently offer monetary rewards, we will provide written thanks and/or references, and credit you in any security advisories, where applicable.

Thank you for helping us keep our systems secure. We appreciate your contribution to the safety of our ecosystem.