CyberWhiz Vulnerability Disclosure Policy (VDP)

Version: 1.0 | Effective date: 16 March 2026

Purpose

CyberWhiz welcomes good-faith security research and responsible reporting of security vulnerabilities. This Vulnerability Disclosure Policy (VDP) explains how security researchers can report potential vulnerabilities affecting CyberWhiz products and services, and how CyberWhiz will respond.

Scope

This policy applies to CyberWhiz "products with digital elements", including:

- CyberWhiz hardware devices and their firmware
- CyberWhiz mobile application components (iOS/Android)
- CyberWhiz cloud and backend components (APIs, web portals, admin consoles, remote data processing solutions)
- SBOM, VDP, Security Incident Event Logging, telemetry and other supporting services operated by CyberWhiz

Third-party services may be out of scope; however, CyberWhiz-managed integrations and components remain in scope. If you are unsure, please report anyway and our PSIRT will confirm scope.

How to Report

Please send vulnerability reports by email to:

psirt@cyberwhiz.co.uk

In the email subject, please include "VDP / Vulnerability Report" and the affected product/service name if possible.

Safe Harbor (Good-Faith Research)

CyberWhiz supports good-faith security research intended to improve the security of our products and services. When conducting research under this policy, please:

- Use only accounts you own or have explicit permission to test, and avoid accessing others' data.
- Avoid actions that could degrade service availability (e.g., DoS/DDoS, heavy scanning, load testing).

- Do not use social engineering, phishing, or physical attacks against CyberWhiz staff, customers, or partners.
- Minimize data access and retention. If you accidentally access sensitive data, stop, do not store/share it, and report immediately.
- Do not publicly disclose details before coordinating with CyberWhiz (see Coordinated Disclosure below).

Nothing in this policy is intended to authorize unlawful activity. CyberWhiz will not pursue legal action against researchers who comply with this policy and act in good faith.

What to Include in a Report

To help us validate and fix issues quickly, please include as many of the following as possible:

- Affected product/service and version (if known), environment (prod/test), and relevant URLs/IPs
- Vulnerability type and impact (e.g., unauthorized access, RCE, data exposure, privilege escalation)
- Step-by-step reproduction instructions
- Proof of concept (PoC), preferably non-destructive and reversible
- Evidence such as logs, screenshots, request/response samples
- Your preferred name/handle and a contact email for follow-up

Testing Rules and Out-of-Scope Activities

The following activities are out of scope and are not permitted under this policy:

- Denial of service (DoS/DDoS), spam, brute forcing, and other disruptive activities
- Unauthorized access to, or exfiltration of, customer or third-party data
- Extortion, ransom demands, or threats
- Social engineering of employees, contractors, suppliers, or customers
- Public disclosure without coordination
- Findings limited to missing security headers / cookie flags
- Automated scanner outputs only (e.g., reports without a verifiable PoC)
- Low-impact CSRF (e.g., logout-only) or clickjacking that does not require authentication
- robots.txt-related findings, broken links/redirects, low-impact error messages
- Issues that occur only in outdated/unsupported browsers

Our Process and Response Targets

CyberWhiz PSIRT will handle reports as follows:

- Acknowledgement: we aim to confirm receipt within 2 business days.

- Triage: we aim to perform an initial scope/impact assessment within 5 business days.
- Validation and analysis: we may request additional information to reproduce the issue.
- Remediation: issues are prioritized and fixed based on risk and exploitability; mitigations may be issued when appropriate.
- Communication: we will keep you reasonably informed of progress when feasible.

In urgent cases (e.g., evidence of active exploitation), CyberWhiz may accelerate response and remediation.

Coordinated Disclosure

CyberWhiz follows coordinated vulnerability disclosure. Key principles:

- Please give CyberWhiz a reasonable opportunity to investigate and remediate before public disclosure.
- We may agree on an expected public disclosure date based on severity, affected users, and fix complexity.
- We may publish a security advisory and/or release notes once a fix or mitigation is available.
- In justified cases where immediate publication could increase risk (e.g., exploitation likely), we may request a delay in public disclosure.

If you would like attribution in an advisory, please let us know your preferred name/handle.

Confidentiality and Data Handling

Please avoid including personal data or confidential customer information in your report. CyberWhiz will handle vulnerability reports and related information with appropriate confidentiality.

Vulnerability Rating and Identifiers

CyberWhiz may use industry-standard scoring (e.g., CVSS) to assess severity and prioritize remediation. Where appropriate, CyberWhiz may request or assign a CVE identifier and publish an advisory describing affected versions, impact, and mitigations.

Security Updates and Customer Guidance

When a vulnerability is confirmed, CyberWhiz will work to provide fixes and/or mitigations in a timely manner. Where applicable, CyberWhiz will provide guidance to help users apply updates securely.

Legal and Regulatory Context (EU Cyber Resilience Act)

CyberWhiz maintains vulnerability handling processes and a coordinated vulnerability disclosure policy as part of its product security governance, including for alignment with the EU Cyber

Resilience Act (Regulation (EU) 2024/2847), which requires manufacturers to have policies and procedures to process and remediate vulnerabilities reported from internal or external sources.

Policy Updates

CyberWhiz may update this policy from time to time. The latest version will be published on our website. If you have feedback on this policy, please contact psirt@cyberwhiz.co.uk.

We do not currently have any security advisories to share. If this changes, we will publish updates here.

Advisory No	Publish Date	Product	Version	Impact	Rating	Remediation	CVE	Notes
-	-	-	-	-	-	-	-	-