accurri
statutory financial reporting software

accurri.com

Vulnerability disclosure policy

Introduction

This Vulnerability Disclosure Policy (VDP) establishes a clear, safe, and coordinated process for external security researchers to report potential security vulnerabilities to Accurri. It supports continuous improvement of Accurri's security posture and aligns with ISO 27001:2022 and the Australian Cyber Security Centre (ACSC) guidance.

Scope

The scope of the VDP applies to Accurri-owned or operated digital assets that are client or public-facing services or endpoints.

It specifically excludes:

- APIs
- Cloud-hosting infrastructure
- Third-party systems
- Social engineering
- Physical security testing
- Denial-of-service
- Accessing or exfiltrating client data

Reporting channel

Researchers must report vulnerabilities to support@accurri.com.

Reports should include:

- Date and time when vulnerability was identified
- A description of the vulnerability
- Steps to reproduce
- Potential impact
- Researchers' contact details (optional)

Authorised research activities

Authorised research activities include:

- Manual testing
- Automated scanning within reasonable limits
- Authentication/authorisation testing
- Input validation testing (XSS, injection, IDOR)
- Access control testing
- Business logic testing

Prohibited activities

The following activities are prohibited:

- Access, modify, or delete data
- Attempt data exfiltration
- Perform denial-of-service
- Use social engineering
- Access accounts without permission
- Introduce malware or backdoors
- Attempt physical intrusion

Researcher expectations

- Act in good faith
- Limit testing to in-scope systems
- Avoid privacy violations
- Stop immediately if personal data is encountered
- Report promptly
- Allow a reasonable remediation window (default 90 days)
- Use only the official reporting channel

Accurri commitments

- Acknowledge reports within 7 business days
- Provide status updates
- Work collaboratively with researchers
- Notify researchers when remediation is complete
- Apply the Safe Harbour Policy to good-faith research
- Not pursue legal action when Safe Harbour conditions are met

Coordinated disclosure

- Researchers agree not to publicly disclose until remediation is complete or 90 days have passed
- Accurri will work in good faith to remediate promptly
- Public credit may be provided with the researcher's consent

Compliance alignment

This policy aligns with ISO 27001:2022 — A.5.6, A.8.8, A.8.16.

Communication of this policy

This publicly available policy is accessible via the Accurri website https://accurri.com.