

DT

Arup Digital Vulnerability Disclosure Statement(VDP)

Statement – POL0021 – Vulnerability Disclosure

Reference:

| 28 July 2026

Version 1.2

Next Review Date – 28th July 2027

Contents

1	Purpose	1
2	Scope	1
3	Policy	1

No table of contents entries found.

1 Welcome

At Arup, we believe that collaboration with the security community is essential to maintaining the integrity of our systems. This statement explains how security researchers can report potential vulnerabilities to Arup and how Arup will handle those reports.

Nothing herein creates any obligation or warranty on the part of Arup, and all responses are subject to Arup's discretion based on the nature and validity of the report.

2 Purpose

Our priority is the safety, security, and control of Arup's and our customers' data. We acknowledge the vital role that security researchers play in keeping systems and data safe. To encourage the responsible reporting of potential security vulnerabilities, the Arup Cyber Security team is committed to working with the community to respond to legitimate reports and handling them in good faith.

3 Scope

This Statement applies to Arup-owned or operated external-facing digital products and services, unless expressly stated otherwise.

In scope: publicly accessible, internet-facing systems and services owned or operated by Arup, except where stated otherwise.

Out of scope: client systems, third-party platforms not controlled by Arup, social engineering, phishing, physical security testing, denial-of-service testing, bulk automated scanning, spam, and any activity that accesses, alters or extracts data beyond what is strictly necessary to demonstrate a vulnerability.

We welcome reports that demonstrate a realistic, reproducible, and exploitable security vulnerability with a clear, actionable impact on the confidentiality, integrity, or availability of our systems, users, or data.

Arup does not operate a bug bounty or financial reward programme. Submissions are voluntary and non-remunerated.

4 How to Report a Vulnerability

Please send your report to vulnerability@arup.com and include the following information:

- A detailed, reproducible Proof-of-Concept (PoC)
- A clear explanation of the potential security risk, including the affected system(s) and likely impact;
- Evidence that the issue is within scope

Please refrain from submitting any personal or confidential data unless strictly necessary to demonstrate the issue.

If you encounter personal data, confidential information, or credentials, please stop testing immediately and report the issue. Do not access, copy, retain, disclose or use that information except to the minimum extent

strictly necessary to demonstrate the vulnerability.

5 Response Timeline

We aim to acknowledge receipt within five business days and provide a status update within 20 business days. Timeframes may vary depending on the complexity and validity of the report.

Arup reserves sole discretion to determine whether a report is in scope and whether remediation or other action is warranted. Arup has no obligation to respond to reports.

6 Legal Safe Harbour

If you act in good faith and in accordance with this Statement, Arup does not intend to pursue action against you solely for your responsible disclosure activity. This does not apply to unlawful, disruptive, harmful or abusive conduct.

Arup reserves all rights where behaviour exceeds what is reasonably necessary for responsible disclosure.

7 Reporting Requirements

If you believe you have identified a potential security vulnerability, please report it to us immediately at vulnerability@arup.com. We will investigate all legitimate reports and do our best to quickly address the problems.

To encourage responsible disclosure, security researchers must adhere to the following:

- Please notify Arup before making any vulnerability information public and allow us a reasonable opportunity to investigate and address the issue.
- Provide all details of the discovered vulnerability to support validation and reproduction of the issue.
- Make every effort to avoid data destruction, theft, privacy violations and interruption or degradation of our services.
- Do not perform actions that may negatively affect Arup or its users (e.g. Spam, Brute Force, Denial of Service, social engineering.)
- Do not access or corrupt data or information that does not belong to you.
- Do not conduct any kind of physical or electronic attack on Arup personnel, property or data centres.
- Do not attempt social engineering on any Arup service desk, employee or contractor.
- Do not violate any laws or breach any agreements in order to discover vulnerabilities.

Report Acceptance Criteria

To be accepted and reviewed, a report must:

- Be within the defined scope (see section 3)
- Contain a detailed, reproducible Proof-of-Concept (PoC)
- Have a clear explanation of **why** the issue is a potential security risk and its impact
- Not rely solely on automated scanner output

- Comply with applicable laws and privacy standards

Zero-Tolerance for Malicious or Unauthorised Behaviour

Activities outside this Statement, including phishing, social engineering, denial-of-service, extortion, unauthorised access to data, or any action causing harm, may be referred to law enforcement or other appropriate authorities.

Arup reserves the right to refer such conduct to the appropriate law enforcement or regulatory authorities and pursue all available remedies under law.