# VULNERABILITY DISCLOSURE POLICY

We take the security of all of our customers, engineers and users very seriously. We also greatly appreciate investigative work into security vulnerabilities that is carried out by well-intentioned, ethical security researchers. We are committed to collaborating with this community to investigate and resolve security issues. The purpose of this policy is set out how we will work with our users and security researchers to improve ITARMI's online and platform security.

If you are unsure at any stage whether the actions you are thinking of taking are acceptable or within the scope of this policy, please contact our Information Security Team for guidance at security@itarmi.com. Please do **not** include any sensitive information in this type of communication.

## SCOPE OF THIS POLICY

Please *only* report vulnerabilities relating to the following products:

- ITARMI's corporate website (www.itarmi.com)
- ITARMI's IT resourcing web application (cloud.itarmi.com)
- ITARMI's IT resourcing iOS mobile application
- ITARMI's IT resourcing Android mobile application
- ITARMI's public facing APIs

We are primarily interested in hearing about the following vulnerability categories:

- Sensitive Data Exposure – including Cross Site Scripting (XSS) Stored, SQL Injection (SQLi).
- Authentication or Session Management related issues
- Remote Code Execution
- Particularly clever vulnerabilities or unique issues that do not fall into explicit categories

We will review and update the scope of this policy as ITARMI's products continue to evolve.

## LEGALITIES

This policy is designed to be compatible with good practice among well-intentioned security researchers. Therefore, ITARMI will not seek to prosecute any security researcher who reports a security vulnerability *in good faith* and *in accordance with the scope and procedure of this policy*.

Security researchers must **not**:

- act in any manner that is inconsistent with any applicable laws or that would cause ITARMI to be in breach of any of any laws or legal obligations (including but not limited to: Computer Misuse Act 1990, General Data Protection Regulation 2016/679, Data Protection Act 2018, Copyright, Designs and Patents Act 1988)
- violate the privacy of ITARMI staff, customers, engineers or other users
- disrupt or damage any services, applications or systems of ITARMI or any of its users

- view data without authorisation in any way that corrupts the data
- seek or request compensation for the reporting of security issues from any third party or through any external marketplace
- disclose any vulnerabilities in our services, applications or systems to 3rd parties prior to ITARMI confirming that those vulnerabilities have been mitigated or resolved.

We request that all data retrieved during security research is securely held and then securely deleted as soon as it is no longer required (and, in any case, within 1 month after the vulnerability has been resolved).

**HOW TO SUBMIT A VULNERABILITY**

If you have discovered a security issue which you believe is within the scope of this policy, please e-mail us your report at security@itarmi.com .

What we would like to see in your report:

- written in clear, concise English
- details of the security issue, including non-destructive proof of concept code (reports that include only crash dumps or other automated tool output may receive lower priority)
- any suggested/potential remediation.

**Please do not include any details in your initial report that would allow reproduction of the security issue**. Our Information Security Team will request this information at a later stage, using encrypted communications.

By following the above criteria, you will allow our Information Security Team to give your report higher priority in reviewing, validating and resolving the security issue.

**WHAT TO EXPECT**

What you can expect from us:

- acknowledgment of your initial report (usually, within 2 business days), which will include details of an encrypted communications channel to use for any further communications about the reported issue
- our Information Security Team will work to triage the reported vulnerability and will respond to you as soon as possible to confirm whether further information is required and/or whether your report contains an in-scope vulnerability (including whether it is a duplicate report)
- vulnerability reports may take some time to triage and/or remediate, so you're welcome to check on the status of the process but please limit this to no more than once every 14 days, as this helps our Information Security Team to focus on the reports as much as possible

- our Information Security Team will notify you when the reported vulnerability is resolved (or remediation work is scheduled) and may ask you to confirm your view as to whether the solution adequately covers the vulnerability
- we may involve a neutral third party to assist in validating and resolving the security issue
- reporters of qualifying vulnerabilities will receive acknowledgment through our website or an equivalent medium and we will seek to agree details that you wish to be included in our acknowledgment.

**FEEDBACK**

This policy will evolve over time and your input will help us to ensure that it remains clear, complete and relevant. Therefore, if you wish to provide any feedback on this policy, please contact our Information Security Team at security@itarmi.com .

*Last updated: 6 April 2020*