PiSYS
Since 1988

VULNERABILITY DISCLOSURE

POLICY

REV	DATE	REVISION	PREPARED	CHECKED	APPROVED
1	08/11/2024	Issued	KRC	RAG	PIH

TABLE OF CONTENTS

LIST OF FIGURES

No table of figures entries found.

LIST OF TABLES

No table of figures entries found.

ASSOCIATED DOCUMENTS

Pisys Ref. Number	Title / Description

DOCUMENT REVISION NOTES

REV	Title / Description

SECTION A. SCOPE

Pisys is committed to maintaining the security of its information assets and those of its customers. As part of this commitment, we encourage the responsible disclosure of any vulnerabilities that may be found in our products or services. This Vulnerability Disclosure Policy applies to any vulnerability that affects the security of our products, services, or websites that are within the Pisys infrastructure.

Section A.1. REPORTING A VULNERABILITY

If you have discovered a vulnerability in a Pisys product or service, please report it to us as soon as possible through our Support team at support@pisys.co.uk.

Your report should include:

- Vulnerability Details: A detailed description of the vulnerability, including steps to reproduce it.
- Affected Products/Services: The name and version of the affected product or service, along with any relevant URLs or IP addresses.
- Severity: A classification of the vulnerability's severity (e.g., low, medium, high, critical) and the potential impact if exploited.
- Date Discovered: The date you discovered the vulnerability.
- Contact Information: Your name, email address, and any other contact information you wish to provide.

Please include as much information as possible to help us understand and validate the vulnerability.

Section A.2. RESPONSIBLE DISCLOSURE

We ask that you:

- Do not publicly disclose the vulnerability until we have had a reasonable amount of time to review and address the issue.
- Do not exploit the vulnerability or attempt to access unauthorized data.
- Act in good faith and with the intent to help us improve our security.

We do not require a non-disclosure agreement (NDA) to report vulnerabilities. However, we do appreciate it if you give us the opportunity to address the issue before disclosing it publicly.

Section A.3. WHAT TO EXPECT FROM PISYS

Upon receiving a vulnerability report, we will:

- Acknowledge your report within 5 business days.
- Investigate the reported vulnerability.
- Provide updates on the status of the investigation and any action taken.
- Work with you to understand and resolve the issue quickly and efficiently.
- Credit you for your contribution if you wish, after the vulnerability has been validated and resolved.

Section A.4. Reporting Process

1. **Submission**: You submit the vulnerability to our Support team.
2. **Acknowledgement**: We acknowledge receipt of your report.
3. **Triage**: We review the report for completeness and assess the potential impact.
4. **Investigation**: We investigate the vulnerability and determine its validity.
5. **Resolution**: If the vulnerability is confirmed, we will take appropriate steps to resolve the issue.
6. **Communication**: We will keep you informed of the progress and provide a timeline for resolution.
7. **Public Disclosure**: Once the vulnerability is resolved, we will coordinate with you on the public disclosure of the vulnerability, if applicable.

Section A.5. Incident Response and Disaster Recovery

CSPs must provide clear and comprehensive incident response and disaster recovery plans.

Pisys will regularly test these plans to ensure they are effective and up-to-date.

Any security incidents involving cloud services must be reported immediately to the Information Security Team.

Section A.6. Legal

By submitting a vulnerability report, you agree not to take any legal action against Pisys or its employees for any disclosure made under this policy. Pisys will not take legal action against you if you have acted in good faith and adhered to the guidelines set forth in this policy.

Thanks for helping us improve our security!

We value the contributions of security researchers and are grateful for the assistance in making our products and services safer. We look forward to working with you to enhance our security posture.