Vulnerability and Threat Management Policy and Procedure

Date	Name	Role	Change	Version
Wed Aug 06 2025	Tim Murnaghan	CTO	Approved	V1.0

Vulnerability and Threat Management Policy

1. General

1.1 Vulnerability and threat management is the process of identifying, evaluating, treating, and reporting security vulnerabilities in systems and the software that runs on them. Ensuring that security patches and updates are quickly installed is essential to protecting Integrum ESG's ("the Company") from malware, attacks, and other vulnerabilities.

2. Purpose and Scope

2.1 This Vulnerability and Threat Management Policy and Procedure ("the Policy") provides the patch and vulnerability management procedure that maintains the integrity of the Company's network systems and data and establishes a process and time frame for patch management compliance.

2.2 This Policy applies to all Company employees.

3. Responsibilities

3.1 The responsibility to stay up-to-date and follow this Policy applies to all Company employees

3.2 The CISO is responsible for developing, maintaining, and implementing this Policy.

3.3 The roles and responsibilities of the Company employees are set out in the Roles and Responsibility Policy.

4. Document Ownership

4.1 The CISO is the owner of this Policy and is responsible for ensuring that this procedure is reviewed in line with the Company's review requirements. A current version of this document is available to all Company

employees in Sharepoint.

Vulnerability and Threat Management Procedure

5. Penetration Testing

5.1 Monthly vulnerability scanning (“Penetration Testing”) will be performed using a third-party service. A report dealing with all vulnerabilities found will be emailed to the CISO and the relevant Information Asset Owner. These vulnerabilities will be dealt with following the vulnerability management cycle detailed below.

6. Image Scanning

6.1 Monthly image vulnerability scanning will be performed by a scheduled container scan.

6.2 The following assets will be subject to screening:

- 6.2.1 Major client facing applications
- 6.2.2 Other minor microservices
- 6.2.3 Third party docker images

6.3 When the scan is completed, findings will be divided into four severity levels: low, medium, high, and critical. Categorisation of the severity levels will be performed automatically by the scanning tool and reviewed by the CISO.

7. Vulnerability Management Cycle

7.1 General

7.1.1 The Infrastructure Team must maintain an up-to-date inventory of all the Company’s critical assets that must be periodically scanned for security vulnerabilities

7.1.2 The Company’s assets must be scanned by vulnerability scanners to determine if there are weaknesses in the configuration of the assets.

7.2 Periodic Vulnerability Assessments

7.2.1 Conduct periodic vulnerability assessments and reviews within the specified timeframes to identify known and potential vulnerabilities, as follows;

7.2.1.1 Applications that interface with protected data: Monthly, using web applications scanning tools and also using tools such as Gitlab container scan for images.

7.2.1.2 Other Company-level applications: Monthly, using tools such as Gitlab container scan and external risk assessments.

7.2.1.3 Third party images: Monthly, using tools such as Gitlab container scan and external risk assessments.

7.2.2 Review the application code to identify known and potential vulnerabilities that are not discovered from the automated vulnerability scan (for example: hard-coded unencrypted credentials). Address and resolve vulnerabilities identified in the vulnerability scan report.

7.2.3 Keep records of identified vulnerabilities and remediation actions for a minimum of 6 months.

7.3 Vulnerability Management

7.3.1 We keep records of vulnerabilities in the respective external tools we use for the testing.

7.3.2 The repository must include the following items:

7.3.2.1 Vulnerability scanning reports (with detailed information about discovered vulnerabilities etc.)

7.3.2.3 Remediation Status Report (a documented process of mitigating the threats).

7.4. Remediation

7.4.1 If a vulnerability is found, a Change Management ticket containing the vulnerability details and remediation information must submitted to the Information Asset Owner. The vulnerability must be monitored until it is resolved.

7.4.2 The Information Asset Owner must assess the applicability of the vulnerability and evaluate the impact of the fix on production systems. The Information Asset Owner will then schedule the implementation of the fix following the timelines below and considering available resources.

7.5 Handling Timelines

7.5.1 Vulnerabilities will be handled according to the timelines described below:

7.5.1.1 Critical vulnerabilities: immediately or within 5 days.

7.5.1.2 High vulnerabilities: within 2 weeks.

7.5.1.3 Medium vulnerabilities: within 90 days.

7.5.1.4 Low vulnerabilities: within 180 days.

7.5.2 The timeline begins with the discovery of the relevant vulnerability.

8. Compliance Review Procedure

9.1 The CISO must ensure that critical systems are scanned for vulnerabilities monthly. Critical systems with unpatched vulnerabilities must be brought to the attention of the Infrastructure Team Lead for mitigation.