

INFORMATION SECURITY POLICY SUITE

Risk Assessment and Vulnerability Management Policy

Glaxtons Consulting Limited

REF GCL-RAP-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-RAP-01
CLASSIFICATION	Confidential, internal and authorised third parties
POLICY OWNER	Operations Director
APPROVED BY	The Board of Glaxtons Consulting Limited
EFFECTIVE DATE	May 2026
NEXT SCHEDULED REVIEW	May 2027
APPLIES TO	Glaxtons Consulting Limited, 3 More London Place, London SE1 2RE

1 Purpose

This policy governs how the Company identifies, evaluates and treats information security risks, and manages vulnerabilities in its systems, on an ongoing basis.

2 Scope

This policy applies to all Company information assets, systems and services.

3 Definitions

In this policy, "Company" means Glaxtons Consulting Limited, "Personnel" means employees, workers, contractors, consultants and temporary staff of the Company, and "client" means any current or prospective client, customer or partner of the Company.

4 Policy

4.1 Risk assessment process

The Company maintains a risk register identifying information assets, threats and vulnerabilities, assessed on a likelihood and impact basis. The register is formally reviewed at least quarterly by the Operations Director, and additionally whenever a new system is introduced, a material change is made to the Company's infrastructure or services, or following a security incident or credible threat intelligence relevant to the Company's sector.

4.2 Penetration testing

The Company commissions an independent penetration test of its external facing systems, and, where proportionate, its internal network and key applications, at least once every twelve months, carried out by a suitably qualified third party tester. Identified findings are risk rated, remediated according to defined timescales by severity, and retested to confirm resolution.

4.3 Anti-malware

All Company endpoints and critical servers run centrally managed anti-malware software providing real time scanning and automatic definition updates, with alerts routed to the IT function for investigation and detected threats quarantined pending review.

4.4 Vulnerability and patch management

Security patches are applied to Company systems according to defined timescales based on severity, informed by regular vulnerability scanning. Any exception to these timescales requires a documented risk acceptance approved by the Operations Director.

5 Alignment with client due diligence requests

This policy addresses the following reference points commonly raised in client and prospective client vendor due diligence and security assessments: V.RA-36, V.RA-37, V.RA-38. Where a client raises a due diligence question falling within this policy's scope, the relevant section of this policy may be used as the basis for the Company's response, subject to review by the Operations Director.

6 Roles and responsibilities

- The IT function carries out vulnerability scanning, patching and anti-malware operation.
- The Operations Director owns the risk register and commissions and oversees remediation of penetration test findings.
- The Board reviews residual risk on the register as part of its quarterly reporting.

7 Non-compliance and exceptions

Breach of this policy may result in disciplinary action up to and including dismissal, and, in the case of a contractor, consultant or supplier, termination of the relevant engagement or contract. Any exception to this policy must be requested in writing, is subject to a documented risk assessment, and requires the approval of the Operations Director before it takes effect.

8 Related policies

- Information Security Policy
- Data Security Policy
- Data Protection and Compliance Policy
- Change Management Policy

9 Version history

VERSION	DATE	SUMMARY OF CHANGE	AUTHOR
6.0	May 2026	Scheduled annual review, reissued and approved by the Board.	Legal Department

Glaxtons Consulting Limited · 3 More London Place, London SE1 2RE · 020 3668 5488 · info@glaxtons.co.uk · glaxtons.co.uk
This document is issued under the Company's information security policy suite and is reviewed at least annually. Printed copies are uncontrolled.