

INFORMATION SECURITY POLICY SUITE

Incident Management Policy

Glaxtons Consulting Limited

REF GCL-IMP-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-IMP-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 enables the Company to identify, contain, investigate and communicate information security incidents promptly, so as to limit harm to the Company, its clients and any affected data subjects.

2 Scope

This policy applies to all suspected or confirmed information security incidents affecting Company or client systems, data or premises.

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 Incident response process

The Company maintains a documented incident management process that defines severity classification (Critical, High, Medium and Low), an incident response team drawn from Operations, IT and, where personal data is involved, the Data Protection Lead, and defined roles for triage, containment, eradication, recovery and closure.

The process includes a communication plan covering internal escalation to the Board for Critical and High severity incidents, notification to affected clients under the terms of the relevant engagement letter or contract, and, where personal data is affected, assessment of the requirement to notify the Information Commissioner's Office within seventy two hours and affected data subjects without undue delay, in accordance with the UK GDPR.

4.2 Reporting channel

A single point of contact, comprising a dedicated security incident mailbox and an out of hours contact number, is published to all Personnel and contractors for reporting suspected incidents, with a commitment to acknowledge reports within one hour during business hours.

4.3 Testing

The incident management process is tested at least annually by way of a tabletop exercise based on a realistic scenario, involving the incident response team and, where appropriate, senior management. Outcomes and any resulting actions are recorded.

4.4 Review and continuous improvement

Following every incident, and following each test, a documented post-incident review is conducted to identify the root cause and any contributing control weaknesses. Resulting actions are logged on the Company's risk register, tracked to closure by the Operations Director, and reported to the Board.

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-14, V.RA-15, V.RA-16. 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 Operations Director owns this policy and acts as incident commander for Critical incidents.
- The Data Protection Lead advises on and makes regulatory notification decisions.
- The IT function carries out technical containment and recovery.
- All Personnel must report suspected incidents through the published channel without delay.

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 Protection and Compliance Policy
- Business Continuity and Disaster Recovery 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.