

INFORMATION SECURITY POLICY SUITE

# Third Party and Supplier Security Policy

Glaxtons Consulting Limited

REF GCL-TPM-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

|                       |                                                                  |
|-----------------------|------------------------------------------------------------------|
| DOCUMENT REFERENCE    | GCL-TPM-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 manages the information security risk arising from suppliers, subcontractors and cloud service providers engaged by the Company.

## 2 Scope

This policy applies to all suppliers, subcontractors and service providers with access to Company or client information, or to information systems that store, process or transmit business sensitive data.

## 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 Supplier due diligence and annual review

Before engaging a supplier with access to Company or client information, or to information systems that store, process or transmit business sensitive data, the Company carries out proportionate due diligence, including a security questionnaire and a review of relevant certifications. Suppliers in this category are subject to a

documented annual security review, covering any change in the services provided, any reported incidents, and the continued adequacy of contractual protections.

#### 4.2 Cloud service providers

Cloud service providers used by the Company are assessed prior to onboarding, and at least annually thereafter, against the applicable shared responsibility model, their published security certifications such as ISO/IEC 27001 or SOC 2, their incident notification commitments, and their data location. Findings are recorded and any gaps are tracked to resolution.

#### 4.3 Confidentiality

Suppliers and third parties are required to sign a non-disclosure or confidentiality agreement, or to accept equivalent confidentiality terms within their master services agreement, before any Company or client confidential information is shared with them.

#### 4.4 Contractual protections

Supplier contracts include, where proportionate to the risk presented, obligations to maintain appropriate technical and organisational security measures, to notify the Company promptly of any security incident affecting Company data, restrictions on the use of subprocessors without consent, audit or assurance rights, and obligations to return or securely destroy Company data on termination.

### 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-28, V.RA-29, V.RA-30. 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 approves the engagement of new suppliers within scope of this policy and owns the annual review programme.
- Engagement leads carry out initial due diligence before a new supplier is onboarded.
- The Data Protection Lead reviews data processing terms in supplier contracts.

### 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

■ Incident 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.