

INFORMATION SECURITY POLICY SUITE

HR Security Policy

Glaxtons Consulting Limited

REF GCL-HRS-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-HRS-01
CLASSIFICATION	Confidential, internal and authorised third parties
POLICY OWNER	Head of HR
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 ensures that individuals engaged by the Company are suitable for their role, understand their information security responsibilities, and are equipped to protect Company and client information throughout their engagement and on departure.

2 Scope

This policy applies to all employees, workers, contractors and temporary staff engaged by the Company.

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 Pre-engagement screening

Before an offer of employment or engagement is confirmed, the Company verifies the candidate's identity and right to work in the United Kingdom, and obtains at least two references covering the immediately preceding period of employment, engagement or study.

For roles with access to client financial data, bid sensitive information or elevated system privileges, the Company additionally carries out a basic criminal record check and, where proportionate and lawful, a credit or financial probity check.

Contractors and consultants engaged through a third party agency are subject to equivalent checks, obtained either directly by the Company or by way of written confirmation from the supplying agency, before access to Company systems is granted.

4.2 Confidentiality, acceptable use and conduct

All employees and contractors sign, before being granted access to Company systems, a contract of employment or engagement letter containing confidentiality undertakings, together with the Company's Acceptable Use Policy and Code of Ethics. Acknowledgement of these documents is refreshed annually and on any material change to their terms.

The Acceptable Use Policy governs permitted use of Company equipment, email and internet access, prohibits the use of unauthorised software and personal cloud storage for Company data, and sets requirements for remote and mobile working.

4.3 Security awareness and training

All new starters complete information security induction training within their first two weeks of engagement, covering data protection, phishing and social engineering, password and access hygiene, incident reporting, and clear desk and clear screen practice.

All Personnel complete refresher training at least annually. Phishing simulation exercises are run at least twice a year, with targeted coaching provided to individuals identified as requiring it.

4.4 Leavers and role changes

HR notifies the Company's IT function of leavers and role changes in accordance with the Access Control Policy. Exit interviews include a reminder of ongoing confidentiality obligations that survive termination of engagement, and return of Company equipment is tracked to completion.

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-4, V.RA-5, V.RA-6. 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

- HR is responsible for carrying out and recording pre-engagement screening, and for notifying IT of leavers and role changes.
- Line managers are responsible for booking induction training and for day to day oversight of conduct.
- The Head of HR owns this policy and reports annually to the Operations Director on training completion rates.
- All Personnel must comply with the Acceptable Use Policy and Code of Ethics and complete required training.

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
- Access Control 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.