

INFORMATION SECURITY POLICY SUITE

Data Security Policy

Glaxtons Consulting Limited

REF GCL-DSP-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-DSP-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 protects the confidentiality and integrity of Company and client data throughout its lifecycle, whether at rest, in transit, or at the point of disposal.

2 Scope

This policy applies to all Company and client data, and to all systems, devices and media on which that data is held or through which it is transmitted.

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 Encryption at rest

Data held on Company issued laptops and mobile devices, servers and cloud storage is encrypted at rest using industry standard algorithms of a minimum of AES-256 or an equivalent standard, with encryption enabled by default on all endpoint device builds before issue to Personnel.

4.2 Encryption in transit

Data transmitted over public networks, including through client portals, email attachments containing sensitive data, and remote access connections, is protected using TLS 1.2 or higher, or an equivalent encrypted virtual private network connection. Unencrypted transmission of sensitive or client data is prohibited.

4.3 Cryptographic key management

Encryption keys are generated, stored, distributed, rotated and retired in accordance with a documented key management procedure. Keys are held in a dedicated key management service or vault separate from the data they protect, access is restricted to authorised IT personnel on a need to know basis, and retired or compromised keys are securely destroyed and the destruction logged.

4.4 Segregation of environments

Production data is not used in test or development environments. Where realistic data is required for testing purposes, anonymised or synthetic data sets are used, and access to production and non-production environments is controlled separately.

4.5 Secure disposal

Media and devices that are no longer required are wiped using a certified secure erasure method, or physically destroyed by an accredited disposal contractor, before leaving the Company's control. A certificate of destruction is obtained and retained for each batch disposed of.

4.6 Data leakage prevention

The Company operates technical and procedural controls to prevent or detect unauthorised disclosure of data, including restrictions on the use of removable media and personal cloud storage, outbound email monitoring for sensitive content, data classification labelling for bid, financial and client information, and periodic review of sharing permissions on collaboration platforms.

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-17, V.RA-18, V.RA-19, V.RA-20, V.RA-21, V.RA-22. 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 implements and maintains the technical controls required by this policy, including key management and secure disposal.
- The Operations Director owns this policy and approves the key management procedure.
- All Personnel must apply data classification and handling controls correctly and must not circumvent data leakage prevention controls.

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
- Data Protection and Compliance 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.