

INFORMATION SECURITY POLICY SUITE

Business Continuity and Disaster Recovery Policy

Glaxtons Consulting Limited

REF GCL-BCP-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-BCP-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 ensures the Company can maintain, or promptly resume, critical operations, including services delivered to clients, following a disruptive event.

2 Scope

This policy applies to all critical business functions, systems and premises of 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 Business continuity and disaster recovery plan

The Company maintains a documented business continuity and disaster recovery plan identifying critical business functions, dependencies, recovery time objectives and recovery point objectives, and setting out the actions, roles and communication steps to be followed in the event of a disruption. A summary of the plan, including the relevant service level and business continuity provisions, is made available to clients on request under the terms of the applicable engagement.

4.2 Alternate processing facilities

The Company's core systems and data are hosted on cloud infrastructure that provides automatic failover between geographically separate availability zones, and Personnel are equipped to work remotely, so that the loss of the Company's primary office premises does not by itself prevent the continued delivery of services.

4.3 Backups

Business critical data is backed up at least daily to storage held in a location or cloud region separate from the primary system. Backups are retained in accordance with the Company's retention schedule and encrypted in accordance with the Data Security Policy.

4.4 Testing of the plan

The business continuity and disaster recovery plan is tested at least annually, through a combination of tabletop exercises and, where practicable, a technical failover test. Results and any resulting improvements are documented and reported to the Board.

4.5 Backup and restore testing

The ability to restore data from backup is tested at least quarterly on a sample basis, and the outcome, including time to restore, is recorded. Any failure is investigated and remediated before the next scheduled test.

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-23, V.RA-24, V.RA-25, V.RA-26, V.RA-27. 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 the business continuity and disaster recovery plan.
- The IT function performs backups, failover configuration and restore testing.
- The Board reviews the outcome of annual tests and approves any material change to recovery objectives.

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
- 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.