

INFORMATION SECURITY POLICY SUITE

Access Control Policy

Glaxtons Consulting Limited

REF GCL-ACP-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-ACP-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 that access to Company and client systems and data is granted, reviewed and removed on a controlled, least privilege, need to know basis.

2 Scope

This policy applies to all Company systems, applications and data, and to all Personnel who require access to them.

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 Access lifecycle

The Company operates a documented access control process covering the full lifecycle of a user account:

- Registration and approval:** access requests are raised in writing or via the Company's ticketing system and approved by the requester's line manager and, for systems holding client data, by the relevant system or data owner.

- **Provisioning:** access is provisioned by the IT function strictly in line with the approval given and the individual's defined role.
- **Periodic review:** access rights for all systems are reviewed at least every six months by the relevant system owner, with findings recorded and excess access removed within five working days.
- **Adjustment or removal:** access is amended within two working days of a role change, and revoked no later than the individual's last working day, or immediately where the departure is for cause.

4.2 Unique identity

Every individual is issued a unique user account. Shared, generic or group logins are prohibited other than for defined service accounts, which are separately risk assessed, documented and subject to enhanced monitoring.

4.3 Need to know and role based access

Access rights are assigned according to defined role profiles reflecting the minimum access necessary to perform the role. A request for access outside the standard role profile requires an explicit business justification and additional approval from the relevant system owner.

4.4 Privileged access

Administrative or privileged access is restricted to named individuals with a demonstrated business need. It is granted through a separate approval process requiring sign off from the Operations Director or the IT lead, is provisioned through dedicated privileged accounts distinct from day to day user accounts, is logged, and is recertified every three months.

4.5 Leavers

The Company operates a formal leaver process, triggered by HR notification, under which all system and building access is disabled no later than the individual's last working day, and immediately on notice of a security concern. Equipment is recovered and accounts are archived or deleted in accordance with the Data Security Policy.

4.6 Passwords and multi-factor authentication

All Company systems enforce complex passwords consistent with current National Cyber Security Centre guidance, including minimum length and screening against known compromised password lists, and support a secure self-service password reset procedure.

Two factor authentication is mandatory for all privileged and administrative accounts, for remote access to Company systems, and for access to cloud services holding client or business sensitive data.

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-7, V.RA-8, V.RA-9, V.RA-10, V.RA-11, V.RA-12, V.RA-13. 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 provisioning, logging and technical enforcement of this policy.

- System and data owners approve access requests and conduct periodic access reviews.
- HR notifies IT of leavers and role changes without delay.
- The Operations Director owns this policy and approves all requests for privileged access.

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
- HR 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.