



DATED 6 OCTOBER 2026

GLAXTONS CONSULTING LIMITED

INFORMATION SECURITY POLICY

relating to

THE PROTECTION OF CLIENT AND COMPANY INFORMATION

Version 1.0

Glaxtons Consulting Limited

3 More London Place, London SE1 2RE

CONTENTS

Clauses

1	DEFINITIONS AND INTERPRETATION.....	3
2	PURPOSE AND SCOPE.....	4
3	RESPONSIBILITIES.....	4
4	HANDLING OF INFORMATION.....	4
5	ACCESS CONTROL.....	5
6	SYSTEMS AND STORAGE.....	5
7	DEVICES.....	5
8	UPDATES AND MALWARE PROTECTION.....	6
9	ARTIFICIAL INTELLIGENCE TOOLS.....	6
10	SUPPLIERS AND ASSOCIATES.....	6
11	PERSONNEL.....	6
12	WORKING SECURELY.....	7
13	BACKUP AND RECOVERY.....	7
14	SECURITY INCIDENTS.....	7
15	RETENTION, RETURN AND DISPOSAL.....	7
16	CLIENT REQUIREMENTS.....	8
17	COMPLIANCE AND REVIEW.....	8

Schedule

Schedule 1	DEVICE SECURITY STANDARD.....	9
------------	-------------------------------	---

INFORMATION SECURITY POLICY

1. DEFINITIONS AND INTERPRETATION

1.1 In this Policy the following expressions have the following meanings:

“Approved System” means a system, application or cloud service that the Information Security Lead has approved for holding or processing Information and has entered in the Systems Register;

“Client” means any person for whom the Company provides, or proposes to provide, services;

“Client Contract” means any contract, engagement letter or confidentiality agreement between the Company and a Client;

“Client Information” means all information in any form that a Client, or a person acting for a Client, makes available to the Company, together with all material that the Company prepares for that Client;

“Company” means Glaxtons Consulting Limited, registered in England and Wales with company number 12065176;

“Company Information” means all information in any form that the Company holds for the purposes of its own business, including its financial, commercial and personnel records;

“Data Protection Legislation” means the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003;

“Device” means any computer, tablet or phone that is used to hold or to reach Information, whoever owns it;

“Directors” means the directors of the Company from time to time, and “Director” means any one of them;

“Information” means Client Information and Company Information;

“Information Security Lead” means the Director appointed by the Directors to own this Policy and to oversee its operation;

“Personal Data” has the meaning given to it in the Data Protection Legislation;

“Personnel” means the Directors, the employees of the Company and every associate, contractor or other individual who works for the Company and has access to Information;

“Policy” means this information security policy;

“Schedule” means the schedule to this Policy;

“Security Incident” means any actual or reasonably suspected unauthorised access to, or accidental or unlawful loss, disclosure, alteration or destruction of, Information, and any loss or theft of a Device or of removable storage media that holds Information; and

“Systems Register” means the register of Approved Systems kept under clause 6.1.

1.2 In this Policy, unless the context otherwise requires:

- (a) the Schedule forms part of this Policy;
- (b) headings do not affect its interpretation;

- (c) the words “including” and “in particular” do not limit the words that come before them; and
- (d) a reference to legislation is a reference to it as amended or replaced from time to time.

2. PURPOSE AND SCOPE

- 2.1 This Policy sets out how the Company protects the confidentiality, integrity and availability of Information.
- 2.2 The Company provides bid writing, bid management and related consultancy services. In doing so it is trusted with commercially sensitive Client Information, including pricing, bid strategy and details of key people. The Company treats the protection of that information as a condition of doing business.
- 2.3 This Policy applies to all Personnel, to all Information, and to every Device and Approved System, wherever the work is carried out.
- 2.4 Compliance with this Policy is a condition of working for the Company.

3. RESPONSIBILITIES

- 3.1 The Directors are accountable for information security. They approve this Policy and provide the resources needed to operate it.
- 3.2 The Information Security Lead shall:
 - (a) keep this Policy and the Systems Register up to date;
 - (b) decide requests for access to Approved Systems;
 - (c) keep the record of Security Incidents required by clause 14.6;
 - (d) carry out the checks required by clause 17.1; and
 - (e) report the results of those checks to the Directors.
- 3.3 All Personnel shall:
 - (a) comply with this Policy;
 - (b) complete the training required by clause 11.3; and
 - (c) report every Security Incident in accordance with clause 14.1.

4. HANDLING OF INFORMATION

- 4.1 All Client Information is confidential, whether or not it is marked as such.
- 4.2 Personnel shall use Client Information only for the engagement for which it was provided. Information received from one Client shall not be used for the benefit of another Client or of any other person.
- 4.3 Access to Client Information shall be limited to the Personnel who need it for the engagement.
- 4.4 Client Information shall be exchanged only through an Approved System or through a channel that the Client has provided or approved.
- 4.5 Printed copies of Client Information shall be kept to the minimum needed, kept out of sight when not in use and shredded when no longer needed.

5. ACCESS CONTROL

- 5.1 Each member of Personnel shall have an individual account for each Approved System. Accounts and credentials shall not be shared.
- 5.2 Multi factor authentication shall be switched on for every account on every Approved System. A system that cannot support multi factor authentication shall not be used to hold Client Information.
- 5.3 Passwords shall be at least twelve characters long, shall be unique to each system and shall be kept only in a password manager approved by the Information Security Lead.
- 5.4 Administrator rights shall be given only to Personnel who need them and shall be used only for administration. Day to day work shall be carried out from an account without administrator rights.
- 5.5 Access to an Approved System shall be granted only on the written approval of a Director. It shall be removed on or before the day on which the individual stops working for the Company or no longer needs it.
- 5.6 Where a Client gives the Company access to a tender portal or to a Client system, that access shall be used only by named Personnel, using credentials issued to them individually. No terms shall be accepted, and no declaration or submission shall be made, on a Client's behalf without the Client's written authority.

6. SYSTEMS AND STORAGE

- 6.1 Information shall be held only in Approved Systems. The Information Security Lead shall keep the Systems Register, which shall record for each Approved System its purpose, its owner within the Company, the country in which its data is held and whether multi factor authentication is switched on.
- 6.2 The Company's primary systems for email and files are Microsoft 365 services. The Company's data in those services is held at rest in the United Kingdom.
- 6.3 Client Information shall not be stored in, or sent through, any personal email account, personal cloud storage account or messaging account that is not an Approved System.
- 6.4 Information shall be encrypted in transit and at rest.
- 6.5 Client Information shall not be copied to removable storage media unless the Information Security Lead has approved the copy and the media is encrypted.
- 6.6 Where a Client Contract requires Client Information to be held in a particular country, it shall be held only in an Approved System that meets that requirement.

7. DEVICES

- 7.1 Every Device shall meet the standard set out in the Schedule. A Device that does not meet that standard shall not be used to hold or to reach Client Information.
- 7.2 The Information Security Lead shall keep a record of the Devices used for the Company's work.
- 7.3 Personnel may use a Device that they own only if it meets the standard set out in the Schedule and is included in that record.
- 7.4 Devices shall not be left unattended in a public place or in a vehicle.

- 7.5 The storage of a Device shall be securely erased before the Device is sold, returned, recycled or passed to another user.

8. UPDATES AND MALWARE PROTECTION

- 8.1 Devices and Approved Systems shall run only software that its supplier still supports with security updates.
- 8.2 Security updates shall be installed within 14 days of release.
- 8.3 Malware protection shall be switched on and kept up to date on every Device.
- 8.4 Software shall be installed only from its supplier or from the official application store for the Device.
- 8.5 Any request received by email or message to change bank details, to make a payment or to disclose credentials shall be verified by a telephone call to a known number before it is acted on.

9. ARTIFICIAL INTELLIGENCE TOOLS

- 9.1 A generative artificial intelligence tool may be used with Information only if it is an Approved System.
- 9.2 The Information Security Lead shall approve such a tool only where the terms on which it is supplied prevent the supplier from using Information to train or improve any model.
- 9.3 Client Information shall not be entered into any such tool where the Client Contract prohibits or restricts that use, unless the Client has approved the tool in writing.
- 9.4 Personnel remain responsible for the accuracy of any work produced with the help of such a tool.

10. SUPPLIERS AND ASSOCIATES

- 10.1 Before a system is approved, or a supplier is given access to Information, the Information Security Lead shall review the security and data protection terms on which the system or service is supplied.
- 10.2 An associate or contractor shall be given access to Client Information only after agreeing in writing to confidentiality obligations no less protective than those that the Company owes to the Client.
- 10.3 Where a Client Contract requires the Client's consent to subcontracting, or to the disclosure of Client Information to an associate or other third party, the Company shall obtain that consent first.
- 10.4 The Company shall engage a sub processor of Personal Data only as the Data Protection Legislation and the relevant Client Contract allow.

11. PERSONNEL

- 11.1 Before an individual is given access to Client Information, the Company shall carry out screening that is proportionate to the role and that complies with employment law and the Data Protection Legislation.
- 11.2 All Personnel shall be bound by written confidentiality obligations before they are given access to Information.

- 11.3 All Personnel shall complete information security and data protection training when they join and at least once in every twelve months after that. The Company shall keep a record of the training completed.
- 11.4 On leaving the Company, an individual shall return all Information and every Device belonging to the Company, and shall delete Information from any Device that the individual owns.
- 11.5 A breach of this Policy may be dealt with under the Company's disciplinary procedure. In the case of an associate or contractor it may lead to the end of the engagement.

12. WORKING SECURELY

- 12.1 Screens shall be locked whenever a Device is left unattended.
- 12.2 Client Information shall not be worked on, or discussed, where it can be seen or overheard by people who are not entitled to it.
- 12.3 Devices and papers shall be stored securely when they are not in use.

13. BACKUP AND RECOVERY

- 13.1 Information that is needed to deliver Client work shall be held in an Approved System that keeps previous versions and allows deleted items to be recovered. It shall not be held only on a Device.
- 13.2 The ability to recover a file from each such Approved System shall be tested as part of the checks required by clause 17.1.

14. SECURITY INCIDENTS

- 14.1 Personnel shall report every Security Incident to the Information Security Lead as soon as they become aware of it.
- 14.2 On receiving a report the Information Security Lead shall take immediate steps to contain the Security Incident, establish what Information is affected and decide what further action is needed.
- 14.3 Where Client Information is or may be affected, the Company shall notify the Client in writing without undue delay and within any period that the Client Contract requires. Where the Client Contract sets no period, the Company shall notify the Client within 24 hours of becoming aware of the Security Incident.
- 14.4 Where Personal Data is or may be affected, the Company shall assess the Security Incident under the Data Protection Legislation and, where notification is required, shall notify the Information Commissioner's Office within 72 hours of becoming aware of it.
- 14.5 The Company shall not disclose a Security Incident affecting Client Information to any third party without the Client's consent, unless the law requires it to do so.
- 14.6 The Information Security Lead shall keep a record of every Security Incident, whether or not it is notified to anyone. The record shall state what happened, what Information was affected and what action was taken.

15. RETENTION, RETURN AND DISPOSAL

- 15.1 Information shall be kept only for as long as it is needed for the purpose for which it is held, or for as long as the law or a Client Contract requires.

- 15.2 At the end of an engagement, or earlier at the Client's written request, the Company shall return or securely delete Client Information as the Client Contract requires, and shall confirm in writing that it has done so where the Client asks.
- 15.3 Deletion shall extend to Approved Systems and to Devices. Information held in automatic backups that cannot be deleted selectively shall not be accessed or used and shall be left to expire.
- 15.4 The periods for which the Company keeps Personal Data are set out in its published privacy policy.

16. CLIENT REQUIREMENTS

- 16.1 Where a Client Contract sets a requirement that is stricter than this Policy, that requirement shall apply to that Client's information and shall prevail over this Policy.
- 16.2 The Director responsible for an engagement shall record any such requirement at the start of the engagement and shall brief the Personnel assigned to it before they are given access to the Client Information.
- 16.3 Where a Client Contract requires it, the Company shall keep an up to date list of the Personnel who have access to that Client's information and shall provide the list to the Client on request.

17. COMPLIANCE AND REVIEW

- 17.1 At least once in every three months the Information Security Lead shall check, and shall record:
- (a) that every Device in use meets the standard set out in the Schedule;
 - (b) who has access to each Approved System, and that each of them still needs it;
 - (c) that multi factor authentication is switched on for every account; and
 - (d) that a file can be recovered from each Approved System used to hold Client Information.
- 17.2 Any failure found by those checks shall be recorded with an owner and a date for putting it right.
- 17.3 An exception to this Policy may be made only with the written approval of the Information Security Lead. An exception shall be limited in time and shall be recorded.
- 17.4 The Company shall give a Client reasonable evidence of its compliance with this Policy on request, subject to the confidentiality that it owes to others.
- 17.5 The Directors shall review this Policy at least once in every twelve months, and after any significant Security Incident or any significant change to the Company's systems or legal obligations.

SCHEDULE 1

DEVICE SECURITY STANDARD

Every Device shall meet each requirement in this Schedule that its operating system is capable of meeting.

No.	Control	Requirement
1	Supported software	The operating system and every application is a version that its supplier still supports with security updates.
2	Security updates	Automatic updates are switched on. Security updates are installed within 14 days of release.
3	Disk encryption	Full disk encryption is switched on.
4	Firewall	The firewall built into the operating system is switched on.
5	Malware protection	The protection built into the operating system, or a product approved by the Information Security Lead, is switched on and up to date.
6	Screen lock	A password, passcode or biometric check is needed to unlock the Device. The Device locks itself after no more than ten minutes without use.
7	User accounts	Each user has a separate account. Day to day work is carried out from an account without administrator rights. Guest accounts are switched off.
8	Software sources	Software is installed only from its supplier or from the official application store for the Device.
9	Disposal	The storage is securely erased before the Device is sold, returned, recycled or passed to another user.

Document control	
Policy owner	Information Security Lead: Jean-Pascal Olivier, Director
Approved by	Jean-Pascal Olivier, Director
Version	1.0
Status	Approved
Effective date	6 October 2026
Next review due	6 October 2027
Applies to	All Personnel, Devices and Approved Systems

Glaxtons Consulting Limited. Registered in England and Wales, company number 12065176.
Registered office: 3 More London Place, London SE1 2RE. D-U-N-S 225164801.