SGC GROUP

SERVICE SCHEDULE FOR SECURITY SERVICES

Please read this Service Schedule in conjunction with the Company's Master Services Agreement and Privacy Notice which can be found on any of the Company's Websites.

The Company's Master Services Agreement, which has been accepted by the Customer, applies to this Service Schedule.

1. DEFINITIONS AND INTERPRETATION

1.1. In this service schedule (**Service Schedule**) the following definitions apply and any other defined terms used in this Service Schedule shall have the same meaning as set out in the Master Services Agreement:

Additional Services	the services described in section 6 of the Appendix and, to the extent specified, in the Order Form;
Appendix	the appendix to this Service Schedule;
CYBRVISION	the Service Assured Product described in Clause 7 and provided to the Customer subject to the terms of the Agreement;
CYBRVISION Report	has the meaning give to it in clause 7.2;
Data	the Customer's data identified in section 3 of the Appendix;
Master Services Agreement	the Company's Master Services Agreement made available to the Customer by the Company at the Company Website at https://scgcloud.com/terms-conditions;
Rolling Monthly Term	has the meaning given to it under Schedule 2 of the Master Services Agreement;
Security Services	the services supplied by the Company as described in section 4 of the Appendix and, to the extent specified, in the Order Form, and excludes the Third Party Security Product, the Setup Work and the Additional Services;
Service Assured Product	has the meaning given to it under Schedule 2 of the Master Services Agreement;
Service Assured Product Commencement Date	has the meaning given to it under Schedule 2 of the Master Services Agreement;
Setup Work	the setup work described in Part 1 of the Appendix and, to the extent specified, in the Order Form;
Third Party Security Product	the third party security product(s) identified in the Appendix, which is/are: (a) supplied under a separate agreement between the parties; or (b) used by the Company in providing services under this Service Schedule but not resold to the Customer; or (c) otherwise procured by the Customer;
Third Party Vendor	the vendor(s) of the Third Party Security Product(s).

2. MASTER SERVICES AGREEMENT

2.1. This Service Schedule incorporates the terms of the Master Services Agreement. For the avoidance of doubt, in the event of conflict between the Master Services Agreement and the terms of this Service Schedule, the terms of this Service Schedule shall prevail.

2.2. In this Service Schedule, expressions defined in the Master Services Agreement and used in this Service Schedule have the meaning set out in the Master Services Agreement unless otherwise defined. The rules of interpretation set out in the Master Services Agreement apply to this Service Schedule.

2.3. The Agreement constitutes the entire agreement between the parties in respect of its subject matter. The Customer acknowledges that it has not relied on any statement, promise, representation, assurance or warranty the Company has made or given, or which has been made or given on the Company's behalf which is not set out in the Agreement.

2.4. The Agreement shall govern the Services provided under this Service Schedule to the exclusion of any other terms that the Customer seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

3. CUSTOMER'S CYBER LIABILITY INSURANCE

3.1. Notwithstanding the Services provided under this Service Schedule, the Customer may still suffer a cyber-attack. Accordingly, the Customer should ensure that it has suitable insurance in place with a reputable insurance company to cover all cyber-related incidents and we suggest cover of at least £1million per claim.

3.2. The Customer shall ensure the insurance referred to in clause 3.1 is in place for the term of this Service Schedule and for 6 years following expiration or termination of this Service Schedule.

3.3. On the Company's written request, the Customer shall provide the Company with copies of the insurance policy certificates and details of cover provided.

4. CUSTOMER'S OBLIGATIONS

4.1.1. meet the Customer obligations described in this Service Schedule and the Master Services Agreement in a timely manner (and in accordance with any timeframes which the Customer has agreed to) and provide all assistance and information reasonably required by the Company;

4.1.2. provide the Company with such access to the Customer Computer System and any other systems and devices identified in section 3of the Appendix, and any other Customer systems, as reasonably required by the Company. The Customer represents and warrants that it has the legal right and all required licences to provide access to the Company as required to provide the Security Services.

5. DATA

5.1. Subject to the Master Services Agreement, the Company will access the Data only in the course of providing the services to the Customer under this Service Schedule.

6. INTELLECTUAL PROPERTY

6.1. The Company or its licensors (including third party service suppliers) own the Intellectual Property Rights in the means, methods, processes and know-how that the Company uses to provide the Setup Work, Security Services and Additional Services. Nothing in this Service Schedule operates to transfer ownership of any of the Company's (or its licensors' or third parties') Intellectual Property Rights to the Customer.

6.2. The Customer confirms that it has and will maintain at its cost all requisite rights, licenses and authority to the Customer Computer System or other systems, devices and Data as may be required to engage the Company to provide services under this Service Schedule.

7. CYBRVISION

7.1. Subject to the terms of this clause 7, the Company will provide CYBRVISION to the Customer whereby the Company will provide dark web monitoring against Customer domains to identify instances of unauthorised use and/or disclosure of Customer business credentials (usernames and passwords) on the dark web.

7.2. As part of the delivery of CYBRVISION, the Company will provide the Customer with a monthly report, detailing the instances in which its business credentials have been exposed to the dark web (**CYBRVISION Report**).

7.3. The Company will provide CYBRVISION from the Service Assured Product Commencement Date and shall continue to provide CYBRVISION to the Customer for successive periods of thirty (30) days (each 30-day period being a Rolling Monthly Term), until terminated in accordance with Clause 7.5.

7.4. The Charges for CYBRVISION are based on the number of Customer domains, and shall be payable by the Customer in advance and on a monthly basis in accordance with the Agreement. The Charges will be as set out in the Order Form, or as otherwise notified to the Customer in writing.

7.5. The Company or Customer may give written notice to the other, not later than thirty (30) days before the end of a Rolling Monthly Term, to terminate CYBRVISION and termination shall take effect on the last calendar day (inclusive) of the following Rolling Monthly Term. For the avoidance of doubt, on termination of CYBRVISION, howsoever arising, the Agreement shall continue in full force and effect for the remainder of the Term, unless terminated earlier accordance with the terms of the Agreement.

7.6. The Customer hereby agrees and acknowledges that CYBRVISION does not include remediation services. Subject to clause 7.7, if the Customer's CYBRVISION Report reveals certain risks or exposure, the Customer may request remediation services from the Company to help protect against unauthorised use or disclosure of its business credentials and enhance its overall cyber security measures.

7.7. Any remediation services must be requested by the Customer in writing. The Company shall evaluate such requests and may respond to the Customer with an Order Form, which will set out the Charges payable by the Customer for the provision of remediation services by the Company, as specified in the Order Form.

7.8. Following receipt of an Order Form issued pursuant to clause 7.7 above, the Customer may Offer to purchase remediation services by returning the duly executed Order Form to the Company. If the Company accepts such Offer, a separate Agreement between the Company and the Customer will come into existence comprising of the applicable Order Form to which the purchase of the remediation services relate, this Service Schedule and the Master Services Agreement.

APPENDIX
SECURITY SERVICES

1 Setup Work

The Company will undertake the Setup Work (if any) on the following basis:

(a) the Customer must meet its obligations in relation to Setup Work as described in this Service Schedule;

(b) the Customer acknowledges that the Setup Work has been determined based on information provided to the Company by the Customer. Where that information is incomplete or inaccurate, or where the Customer's requirements otherwise change before or during the course of the Setup Work, the Company will notify the Customer of any resulting changes to the Setup Work and may charge for the additional work at its standard hourly rates.

2 Third Party Security Products

The Company will provide Third Party Security Products in accordance with the terms contained in the SaaS Multi-product Service Schedule.

The Company takes no responsibility for the proper functioning of the Third Party Security Product.

3 Customer's systems and related data

Changes and additions to the Customer's network, applications and devices and related data are not covered by this Service Schedule unless expressly agreed in writing by the Company (and additional charges may apply which will be notified to the Customer).

4 Security Services

The Company provides the following Security Services under this Service Schedule.

Framework Function	Category	Security Services Description
Identify	Refer to Setup Work above Scope identification	Refer to Setup Work above and services identified on the Order Form.
Protect	Preventive Security	To prevent security incidents our team implements proactive measures to safeguard users, systems and data. These may include training, security controls, updates, and monitoring of services.
Detect	Threat detection	The Company's security team will monitor alerts and alarms generated from the Company's chosen vendors security products. They will review the alert and determine the best course of action in order to Respond to the incident.
Respond	Incident response	Upon reviewing alerts identified during the detect stage, the Company's team will take prompt action to minimise and contain the incidents impact. Where necessary, remediation steps will be implemented to fully address

		and resolve the issue. For critical incidents, a comprehensive incident report will be generated to document the findings and recommend next steps.

5 Customer responsibilities

5.1 The Customer must:

(a) ensure that all components of the Customer Computer System (including without limitation network, applications and devices and any changes agreed by the Company in writing to be covered under this Service Schedule) are kept up to date and that the Vendor's updates and new releases are adopted, or in the case of hardware components are under warranty, unless otherwise agreed in writing by the Company;

(b) comply with all reasonable recommendations from the Company to update components of the Customer Computer System network, applications and devices;

(c) Inform the Company of any new users, devices, endpoints or equipment that need to be included in the scope of the Agreement;

(d) be responsible for procuring, maintaining and securing its network connections and telecommunications links to and from its systems;

(e) be responsible for the legality, reliability, integrity, accuracy and quality of all Data.

6 Additional Services

The following services are out of scope for the Security Services and where provided by the Company will be treated as an Additional Service, for which the Company will charge the Customer at the Company's standard hourly rates:

(a) Recover Functions as described below:

Framework Function	Category	Security Services Description
Recover	Operational Recovery	The Company's team will focus on restoring affected systems and services to full operational capacity, and ensuring all operations are functioning as expected, or implement work arounds for a level of business continuity.

(b) any services not expressly included as part of the Security Services.

The Customer acknowledges that:

(a) recovering from a security incident is or may be complex and time-consuming and is dependent on factors which are outside of the control of the Company (including successful functioning of the Third Party Security Product);

(b) while the Company will use all reasonable commercial endeavours on any recovery work, where this is required the Company gives no guarantee that the recovery will be successful or complete;

(c) where any ransom is demanded in relation to a ransomware attack, it is the Customer's responsibility to manage that ransom demand and the Company has no obligation to and will not meet that ransom demand.

7 Security Incidents

A security incident will be raised by the Company if any of the following occur in respect of the Customer's systems and related data that are protected by the Security Services:

(a) any 'Detect' instance as described in the Security Services in section 4 above;

(b) An incident logged by the Customer to the Company.

8 Cause of security incidents

The Company is not responsible for security incidents howsoever caused, including without limitation where the incident is due to any of the following:

(a) failure or improper functioning of the Third Party Security Product;

(b) any unauthorised access to the Third Party Security Product;

(c) any unauthorised access to the Customer's network, systems, devices, applications, services or data (inclusion but not limited to the systems, devices and related data identified in section 3 above);

(d) a Force Majeure Event.

9 Third party services

The Customer acknowledges that the Company utilises or may utilise the services of a Third Party Vendor or associated third parties (and the Customer consents to the Company doing so for the purposes of this Service Schedule), which may include for example the distributor from which the Third Party Security Product was procured, in the provision of the Security Services and any Additional Services described in this Appendix. The Company will have no liability to the Customer whether direct, indirect or otherwise in respect of the acts or omissions of the Third Party Vendor or any such associated third party.