



End-User License Agreement

Customer Name

Contents List

Clauses

1	Definitions and Interpretation	3
2	Recordals	7
3	Scope	8
4	Equipment	12
5	Ownership	13
6	Restrictions, Responsibilities and Prohibited Use	14
7	Fees and Payment	19
8	Confidentiality	21
9	Personal Information and Data Privacy	22
10	Indemnity	23
11	Warranties and Disclaimers	27
12	Limitation of Liability	33
13	Term and Termination	35
14	Force Majeure	36
15	Suspension	37
16	Survival	38
17	Updates	38
18	General	38
19	Signature	43

Schedules

1	Service Requirements, Information and Levels	45
2	SOC Provisions	49

1 DEFINITIONS AND INTERPRETATION

1.1 In this agreement, unless inconsistent with, or otherwise indicated by the context, the following terms shall have the meanings assigned to them hereunder namely:

Affiliate	in relation to any Party, any entity that directly or indirectly controls, is controlled by, or is under common control with that Party, where “control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract, or otherwise;
Agreement	this end-user license agreement between the Parties as amended from time to time; including all appendices and schedules thereto;
Applicable Law	in relation to any relevant jurisdiction, the common law, statutory law applicable in such jurisdiction, including any present or future interpretation, constitution, decree, judgement, legislation, measure, requirement, order, ordinance, regulation, statute, treaty, directive, rule, guideline, practice, concession or request issued by any relevant authority, governmental body, agency or department or any central bank or other fiscal, monetary, regulatory, self-regulatory or other authority or agency;
Authorised Partner	has the meaning given to it in clause 2.2;
Business Day	any day other than a Saturday, Sunday or public holiday officially recognised as such in the United Kingdom;
Confidential Information	has the meaning given to it in clause 8.1;
ConnectProtect	ConnectProtect International Limited, company number 16744668, a private company registered in the United Kingdom;
Consumer Protection Laws	means any and all applicable laws, regulations, and directives, whether of the United Kingdom, the jurisdiction of the Customer, or any other relevant jurisdiction, that are intended to protect the rights of consumers, including but not limited to laws governing unfair trade practices, false advertising, and product liability, as well as any amendments or replacements thereof;

Customer	the end-user of the Solution/s as identified on an order form or quotation from time to time, whether electronically or otherwise;
Customer Data	has the meaning given to it in clause 3.1.3;
Data Protection Laws	one or more of the following data protection laws or regulations as applicable to the processing of Personal Information by ConnectProtect under this Agreement: (a) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (“GDPR”); (b) the United Kingdom (“UK”) Data Protection Act 2018 and the UK General Data Protection Regulation (“UK GDPR”); (c) Swiss Federal Data Protection Act on Data Protection of 25. September 2020 (Status as of 1. September 2023); (d) the data protection regulations of the United States of America, including but not limited to, California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020; (e) the South Africa Protection of Personal Information Act No. 4 of 2013; (f) the Australia Privacy Act No. 119 1988; (g) Canadian Personal Information Protection and Electronic Documents Act; (h) Singapore’s Personal Data Protection Act 2012; and (i) any relevant law, statute, regulation, legislative enactment, order or other binding instrument, that implements, supplements, or amends the above.
Dispute	a dispute that arises out of or in connection with this Agreement (including in relation to any non-contractual obligations);
Documentation	has the meaning given to it in clause 3.3;
DPA	the additional data protection terms available at www.ConnectProtect.com/Terms and as outlined and referenced in clause 9.2;
Fees	has the meaning given to it in clause 7.1;
Force Majeure Event	(a) act of God;

- (b) war (whether declared or not), hostilities, invasion, act of foreign enemies, civil war, insurrection, riot, rebellion, revolution, military or usurped power, civil commotion, act or threat of terrorism, sabotage or piracy;
- (c) lightning, earthquake, fire, explosion, flood, storm, or severe adverse weather condition;
- (d) theft, malicious damage;
- (e) any labour disturbance such as boycott, strike, lockout, industrial dispute (whether affecting the workforce of a party and/or any other person);
- (f) any destruction, breakdown or failure of equipment;
- (g) any inability to obtain or delay in obtaining supplies or materials;
- (h) any prolonged breakdown of transport, telecommunications, information or energy systems;
- (i) any failure, breach or default of a supplier or sub-contractor of ConnectProtect; or
- (j) any other event or circumstance to the extent it is beyond the reasonable control of the Party claiming relief, provided always that the relevant event or circumstance could not have been reasonably foreseen by the Party claiming relief at the time of execution of this Agreement;

Incorporated Terms	has the meaning given to it in clause 2.5;
MTTR	the average time measured from when an alert is first received, until the time when an initial response or action is taken by ConnectProtect, calculated as the total accumulated response time for all incidents within a calendar month divided by the number of incidents in that month, but excluding incidents logged in error, test events, or those outside the agreed service Solution/s scope;
Parties	ConnectProtect and the Customer, and “Party” shall mean either one of them as the context may indicate; and
Personal Information	has the meaning given to it in clause 9.1.1;
Privacy Policy	the ConnectProtect Privacy Policy available https://www.connectprotect.com/privacy/ ;

Signature Date	the earlier of the date of signature of this Agreement by the last signing of the signatories or the date on which the Customer indicates acceptance of this Agreement as further set out in clause 2.7;
Solution	any product or service, collectively “Solutions”, offered by ConnectProtect to a Customer from time to time and further set out in clause 3.1.4;
Start Date	the Signature Date;
Technology	has the meaning given to it in clause 5.1;
Term	the period starting on the Start Date and ending on the Termination Date;
Termination Date	the date on which this Agreement expires or terminates for whatever reason;
Third Party Products	any non-ConnectProtect branded products and services (including equipment, and any operating system software included therewith) and non-ConnectProtect licensed software products, including open-source components; and
Threat Intelligence Data	means and relates to any malware, spyware, virus, worm, trojan, or other potentially malicious or harmful code or files, URLs, DNS data, public IP addresses, network telemetry, commands, processes or techniques, tradecraft used by threat actors, metadata, or other information or data, in each case that is potentially related to unauthorised third parties associated therewith and that the Customer provides to ConnectProtect in connection with this Agreement or is collected or discovered during the course of ConnectProtect providing Solutions, excluding any such information or data that identifies the Customer or to the extent that it includes personal data of the data subjects of the Customer, but includes personal information of threat actors or as otherwise provided in the ConnectProtect Privacy Policy.

- 1.2** Headings of clauses have been inserted for convenience only and shall not be used for purposes of nor assist or affect its interpretation.
- 1.3** Unless the context clearly indicates a contrary intention, an expression which denotes any gender includes the other genders, a natural person includes an artificial person and vice versa and the singular includes the plural and vice versa.

- 1.4 Should any provision in a definition be a substantive provision conferring rights or imposing obligations on any Party, then effect shall be given to that provision as if it were a substantive provision in the body of this Agreement.
- 1.5 Any reference to an enactment, regulation, rule or by-law is to that enactment, regulation, rule or by-law as at the Signature Date, and as amended or replaced from time to time.
- 1.6 When any number of days is prescribed, such number shall exclude the first and include the last day, unless the last day falls on a day other than a Business Day, in which case the last day shall be the next succeeding Business Day.
- 1.7 Any reference to months or years shall be a reference to named months or calendar years, as the case may be.
- 1.8 The use of the word “including” and its derivatives followed by a specific example/s shall not be construed as limiting the meaning of the general wording preceding it and the ejusdem generis rule shall not be applied in the interpretation of such general wording or such specific example/s.
- 1.9 The expiration or termination of this Agreement shall not affect those provisions of this Agreement which expressly provide that they will operate after any such expiration or termination or which of necessity must continue to have effect after such expiration or termination, notwithstanding the fact that the clauses themselves do not expressly provide this.
- 1.10 In its interpretation, the contra proferentem rule of construction shall not apply (this Agreement being the product of negotiations between the Parties), nor shall this Agreement be construed in favour of or against any Party by reason of the extent to which any Party or its professional advisors participated in the preparation of this Agreement.
- 1.11 If a term is defined within the context of a particular clause in this Agreement, the term so defined, unless it is clear from the clause in question that the term so defined has limited application to the relevant clause, shall bear the meaning ascribed to it for all purposes in terms of the Agreement, notwithstanding that that term has not been defined in this interpretation clause.

2 RECORDALS

- 2.1 This Agreement is entered into by and between ConnectProtect and the Customer and governs any order forms, quotes, statements of work or other similarly intended ordering document, howsoever named, executed or accepted by the Customer that reference this Agreement or relate to the purchase and/or use of a ConnectProtect Solution.

- 2.2 Any order form may be issued to the Customer by ConnectProtect or an authorised resale partner, as applicable (“Authorised Partner”).
- 2.3 This Agreement is effective on the date the Customer executes an order form, accepts an order form by submitting a matching purchase order to ConnectProtect or to an Authorised Partner, as the case may be, or otherwise accepts delivery or receives benefit of the Solution/s.
- 2.4 This Agreement governs the Customer’s purchase, receipt, and/or use of the Solution/s, as identified in an order form, and records the terms and conditions under which those Solution/s, as the case may be, will be delivered and/or provided by ConnectProtect to its Customer.
- 2.5 The provision of the Solution/s are subject to any supplemental Solution terms, where applicable, and the DPA, together with any ConnectProtect’s Privacy Policy and acceptable URL terms are incorporated into this Agreement (“Incorporated Terms”).
- 2.6 In the event of any conflict or inconsistency of terms, the following order of precedence shall prevail: (i) the applicable supplemental Solution terms (where applicable), (ii) this Agreement, and then (iii) the ConnectProtect Privacy Policy. Should the terms of this Agreement conflict or be inconsistent with the DPA, the terms of the DPA shall prevail.
- 2.7 **By executing, whether manually or electronically, an order form, delivering a purchase order or other confirmation to ConnectProtect or an Authorised Partner documenting acceptance of an order form, or operating, downloading, installing, registering or otherwise using the Solution/s, or indicating acceptance in relation to this Agreement and/or supplemental Solution/s terms, the Customer (or its authorised representative) expressly and explicitly acknowledges and agrees that this is a binding Agreement and the Customer hereby agrees to the terms of this Agreement and accepts the offer to purchase or subscribe, as the case may be, for the Solution/s, pursuant to the terms herein.**

3 SCOPE

3.1 Solutions

- 3.1.1 The Customer will purchase, by way of subscription, and ConnectProtect, together with its Authorised Partners (where applicable), will provide the specific Solution/s as specified in the applicable order form.
- 3.1.2 A Solution may be comprised of components, if applicable, as delineated and defined in the supplemental Solution/s terms which may be updated from time to time by ConnectProtect in its sole discretion in accordance with clause 17 as

required to accommodate development, implementation, and deployment of new features and functionality and the Customer's use and licensing thereof.

3.1.3 Any data provided by the Customer to ConnectProtect necessary for the delivery of the Solution/s will be set forth herein and, to the extent applicable, in the supplemental Solution/s terms, and used in accordance with this Agreement and the Privacy Policy ("Customer Data"). The Customer Data will include information collected by ConnectProtect about the Customer's permitted users of the Solution/s, including administrators, during various phases of Solution delivery and/or provision of same. Customer Data may also include the following personal data: (i) first names; (ii) last names; (iii) corporate and/or personal email addresses (as the case may be); (iv) contact numbers; (v) job titles; (vi) physical addresses; and (vii) organisational hierarchy.

3.1.4 ConnectProtect shall deliver and/or provide managed extended detection and response services ("MXDR") in provision of the Solution/s, which combines advanced threat detection, continuous monitoring, automated response, and expert-led investigation to protect the Customer's IT environment against evolving cyber threats. The Solution/s are delivered through a unified, cloud-based platform supported by an around the clock security operations centre ("SOC"). Notwithstanding the service components set out in clause 3.1.5, any other terms relating to the services when providing the Solution/s are set out herein, at Schedule 1 (Service Requirements, Information and Levels) or are supplemented by supplemental Solution/s terms, where applicable.

3.1.5 Service components

3.1.5.1 Threat monitoring and detection

- (a) Continuous collection and correlation of security telemetry from supported endpoints, networks, cloud environments, applications and identities.
- (b) Use of advanced analytics, machine-learning, and threat intelligence feeds to identify anomalous and suspicious activities.
- (c) Prioritisation of alerts through noise reduction and false positive minimisation.

3.1.5.2 Incident investigation and response

- (a) Initial triage and validation of detected security events.
- (b) Escalation of confirmed incidents to the Customer's designated contacts, in accordance with agreed security levels.

- (c) Automated and manual response actions may include: (i) isolating compromised endpoints; (ii) blocking malicious IP addresses or domains; (iii) disabling or restricting compromised accounts; and (iv) containing and mitigating active threats.

3.1.5.3 Security orchestration, automation and response (SOAR)

- (a) Execution of predefined response playbooks for common incident types.
- (b) Orchestration of response actions across integrated security tools (for example: firewalls; endpoint protection; and identity management systems).
- (c) Maintenance of an audit trail for compliance and post-incident review.

3.1.5.4 Reporting and analytics

- (a) Real-time dashboards providing visibility into security posture, active threats, and incident trends.
- (b) Monthly service reports summarising incidents, responses, and overall security performance.
- (c) Recommendations for improving detection rules, response workflows, and overall security posture.

3.1.5.5 Threat hunting and continuous improvement

- (a) Proactive threat hunting activities to identify hidden risks not triggered by automated alerts.
- (b) Continuous tuning of detection and response mechanisms based on new threat intelligence and lessons learned from prior incidents.

3.2 License Grant

Provided the Customer is compliant with the terms of this Agreement, including payment of all applicable fees, ConnectProtect grants to the Customer a personal, revocable, non-exclusive, non-transferable license to internally install, access and/or use the Solution/s identified on an order form. Additional license grants specific to the applicable Solution/s may be set forth in the supplemental Solution/s terms.

3.3 Use Rights

To the extent the Customer has purchased a specific Solution/s, the Customer may access and use the Solution/s, including any components identified within the supplemental Solution/s terms and any other documentation associated with same, solely for its own and

its Affiliates' internal business purposes and in accordance with the provisions of this Agreement, any associated Documentation, any scope of use restrictions and license counts, including any server, user, endpoint, or such other licensing metric designated in the applicable order form, and the supplemental Solution/s terms (where applicable).

“Documentation” means user manuals, training materials, Solution descriptions (where applicable), specifications, and other information relating to the applicable Solution/s but expressly excluding marketing and sales collateral and materials.

3.4 Future Functionality

The Customer agrees that it has not relied on the promise of availability of any future functionality of the Solution/s or any other future product or service in executing this Agreement or any order form, subject however to the warranties set out in clause 11 . The Customer further acknowledges that information provided by ConnectProtect regarding future functionality should not be relied upon to make a purchase decision. Should ConnectProtect offer additional optional functionality in the future that complement the Solution/s, the Customer may elect to subscribe to or purchase and obtain a license to the optional functionality for an additional fee.

3.5 Authorised Partner

The Customer understands and agrees that any Authorised Partner may not modify this Agreement, except in the event specifically and expressly stated within this Agreement, or make any commitments related to the delivery or performance of the Solution/s on ConnectProtect's behalf and any proposals, marketing collateral, or other similar Solution/s descriptions provided by the Authorised Partner shall not apply.

3.6 Beta Solutions

3.6.1 From time-to-time ConnectProtect may invite the Customer to try, at no charge, new or additional Solutions, features, or functionality that are not generally available to Customers (“Beta Solutions”). Customers may accept or decline any such trial in their sole discretion. Any Beta Solutions will be clearly designated as beta, pilot, limited release, developer preview, non-production or by a description of similar import.

3.6.2 Beta Solutions are provided for evaluation purposes and not for production use, are not supported, may contain bugs or errors, and may be subject to additional terms. To the full extent permitted by the applicable Consumer Protection Laws, Beta Solutions are not considered Solutions hereunder and are provided solely and exclusively “as they come” with no express or implied warranty of any kind. **TO THE FULL EXTENT PERMITTED BY APPLICABLE CONSUMER PROTECTION LAWS, THE CUSTOMER ASSUMES AND UNCONDITIONALLY RELEASES CONNECTPROTECT FROM ALL RISKS ASSOCIATED WITH THE USE OF ANY BETA SOLUTIONS.** ConnectProtect may discontinue the Beta Solutions at any time in its sole discretion and ConnectProtect will make reasonable efforts to provide the

Customer with advanced notice of any such discontinuance. ConnectProtect does not promise or represent that Beta Solutions will be made generally available.

3.6.3 ANY DATA ENTERED INTO A BETA SOLUTION MAY BE PERMANENTLY LOST UNLESS THE CUSTOMER:

3.6.3.1 PURCHASES OR SUBSCRIBES TO (WHERE APPLICABLE) THE COMMERCIALLY AVAILABLE VERSION OF THE BETA SOLUTIONS AS MAY BE MADE AVAILABLE BY CONNECTPROTECT; OR

3.6.3.2 TO THE EXTENT POSSIBLE, EXPORTS SUCH DATA PRIOR TO TERMINATION OF THE BETA SOLUTIONS.

3.6.4 TO THE FULLEST EXTENT PERMITTED BY LAW, INCLUDING CONSUMER PROTECTION LAWS, CONNECTPROTECT'S ENTIRE LIABILITY IN CONNECTION WITH ANY USE OF THE BETA SOLUTIONS (AS THE CASE MAY BE) WHETHER IN CONTRACT, DELICT OR OTHERWISE, WILL NOT, AS TO ANY INDIVIDUAL CLAIM OR IN THE AGGREGATE, EXCEED £50 (FIFTY POUNDS). IF THE CUSTOMER DOES NOT AGREE TO THE ALLOCATION OF RISK IN THIS CLAUSE, ITS SOLE RECOURSE IS TO IMMEDIATELY DISCONTINUE THE USE OF THE BETA SOLUTIONS.

3.6.5 Notwithstanding anything to the contrary or inconsistent in this Agreement, the Customer further acknowledges that:

3.6.5.1 Beta Solutions may not be supported and may be changed and adapted at any time, including in a manner that reduces initial functionality;

3.6.5.2 Beta Solutions may not be available or reliable; and

3.6.5.3 Beta Solutions may not be subject to the same security or audits as the Solutions.

4 EQUIPMENT

- 4.1** If the order form specifies that the Customer will receive equipment, then the Customer is responsible for installing the equipment at the location(s) identified by the parties and for the implementation of appropriate data protection practices related to the protection of any information included on such equipment while the equipment is located within the Customer's environment. The equipment may be included as part of the purchase of or subscription to certain Solutions, as defined within the supplemental Solution terms, for use by the Customer during the applicable term or subscription term (as the case may be).

- 4.2 If the Customer attempts to install or use the equipment at a location other than the locations determined by the Customer and communicated to ConnectProtect during onboarding or at any time thereafter, the Solutions may fail to function or may function improperly.
- 4.3 If the Customer installs, uses, or relocates the equipment, the Customer understands it must promptly notify ConnectProtect so that equipment deployment information can be updated within the Customer's account. Other than normal wear and tear, the Customer is directly responsible for the replacement cost of the equipment associated with any loss, repair, or replacement, including any other ancillary costs, damages, fees, and charges to repair the equipment.
- 4.4 If applicable, ConnectProtect will ship equipment to the Customer and will pay the freight costs associated with shipping the equipment to the Customer's designated locations. The Customer is responsible for all additional costs and expenses associated with shipping the equipment to its designated locations and, unless otherwise agreed, for the return of the equipment to ConnectProtect. Such additional costs and expenses may be reflected on an order form, from time-to-time, following shipment of the equipment and will be invoiced by ConnectProtect or the Authorised Partner. The Customer understands and agrees if the equipment is shipped outside of the United Kingdom (or such other locations identified by ConnectProtect), the Customer is responsible for acting as the importer of record.

5 OWNERSHIP

- 5.1 ConnectProtect owns or has the right to license its Technology (where relevant). "Technology" means the Solutions and Documentation and any such other ConnectProtect technology set forth in any supplemental Solution terms (where applicable).
- 5.2 The Customer acknowledges and agrees that:
- 5.2.1 the Technology is protected by United Kingdom and international copyright, trademark, patent, trade secret and other intellectual property or proprietary rights laws;
 - 5.2.2 ConnectProtect retains all right, title and interest (including, without limitation, all patent, copyright, trade secret and other intellectual property rights) in and to the Technology (excluding any rights, title, and interest in any Third Party Products which shall be retained by its third party licensor(s)), Threat Intelligence Data, and any other deliverables, know-how, databases, developed programs, and registered or unregistered intangible property rights related to the foregoing;
 - 5.2.3 there are no implied licenses and any rights not expressly granted to Customer hereunder are reserved by ConnectProtect;

5.2.4 the Solutions, excluding any professional services, are licensed on a basis in terms of which the Customer acquires no ownership or other interest (other than the license rights expressly stated herein); and

5.2.5 the Customer has no right to obtain source code related to the software components included in any Solutions offered as an on-line, hosted Solution.

5.3 The Customer shall not use any Technology to contest the validity of any ConnectProtect intellectual property, and any such use of the Technology constitutes a material, non-curable breach of this Agreement.

5.4 Threat Intelligence Data is created by ConnectProtect and is derived from Customer Data.

5.5 The Customer shall retain all right, title, and interest (including any and all intellectual property rights) in and to the Customer Data, but excluding any Technology used with the Customer Data. The Customer hereby grants ConnectProtect, during the term of this Agreement, a non-exclusive, worldwide, royalty-free right to collect, use, copy, store, transmit, modify, and create derivative works of the Customer Data to the extent necessary to provide the Solution/s to the Customer in accordance with this Agreement.

6 RESTRICTIONS, RESPONSIBILITIES AND PROHIBITED USE

6.1 Restrictions

6.1.1 The Customer agrees not to, directly or indirectly:

6.1.1.1 modify, translate, copy (except to the extent reasonably necessary for back-up purposes), or create derivative works of the Technology except as otherwise expressly permitted under United Kingdom and foreign copyright laws ("Copyright Laws") which may not be excluded by agreement between parties;

6.1.1.2 reverse engineer, decompile, disassemble, or otherwise seek to obtain the intellectual property contained within the Solution/s, except as otherwise expressly permitted under the Copyright Laws which may not be excluded by agreement between the parties;

6.1.1.3 interfere with or disrupt the integrity or performance of the Solution/s or the data and information contained therein or block or disrupt any use or enjoyment of the Solution/s by any third party;

6.1.1.4 attempt to gain unauthorised access to the Technology or related systems or networks;

- 6.1.1.5 remove or obscure any proprietary or other notice contained in the Technology, including on any reports or data printed from the Technology;
- 6.1.1.6 use the Solution/s in connection with a service bureau offering or as a service provider whereby Customer operates or uses the Solution/s deployed within its end-user environments for the benefit of any unrelated third party (excluding use with the Customer's Affiliates, but including any end user or customer of the Customer);
- 6.1.1.7 use the Solution/s to monitor or scan any environments for which Customer has not received consent;
- 6.1.1.8 include material or information in the Technology that is obscene, defamatory, libelous, slanderous, that violates any person's right of publicity, privacy or personality, or otherwise results in any tort, injury, damage or harm to any person;
- 6.1.1.9 challenge the title or any other rights of ConnectProtect in or to the Technology or any parts, derivatives or variations thereof;
- 6.1.1.10 contest the validity of the copyrights or other proprietary interests in or to the Technology;
- 6.1.1.11 claim any right, title or interest in or to the Technology or any parts, derivatives or variations thereof except as explicitly granted in this Agreement;
- 6.1.1.12 provide Customer Data or make its software, hardware, equipment, or systems available to ConnectProtect in violation of any Applicable Law or contract;
- 6.1.1.13 take any action that imposes an unreasonable or disproportionately large load on the infrastructure of the Solution/s; and/or
- 6.1.1.14 disclose the results of any benchmark testing, technical results or other performance data relating to the Solution/s without ConnectProtect's prior written consent.

6.2 ConnectProtect's Responsibilities

ConnectProtect shall provide the Solution/s that the Customer subscribes to or purchases as identified on an order form in accordance with the terms of this Agreement and as may be provided for in any supplemental Solution/s terms. Any software provided as part of the Solution/s shall include any updates, upgrades, bug fixes, version upgrades or any similar changes that are made generally available to a Customer free of charge from time to time during any term or subscription term (as the case may be), as applicable.

6.3 Customer Responsibilities

- 6.3.1 The Customer is responsible for identifying the administrative users for its account which may include the Customer's and its Affiliates' authorised (email authorization sufficient) third party service providers and agents ("Administrators"). Each Administrator will receive an administrator ID and password and will need to register with ConnectProtect. The Customer is responsible for registering and updating its

Administrators, or notifying ConnectProtect, as applicable, about changes to Administrators, including but not limited to termination, change of authority, and the addition of Administrators. The Customer acknowledges and agrees that:

- 6.3.1.1 Administrators will be able to view all Customer Data and other traffic and activities that occur on the Customer's network and that Customer is responsible for all activities that occur under Administrator accounts; and
- 6.3.1.2 Administrators may communicate with ConnectProtect using chat features within the Solution dashboards and such communications may be monitored and recorded by ConnectProtect and the third party tool provider for purposes of customer service, quality assurance, and any other business purposes and the Customer consents to such activity. Administrator IDs are granted to individual, named persons and cannot be shared or used by more than one Administrator but may be reassigned from time-to-time to new Administrators.
- 6.3.2 The Customer and any third parties under its control shall keep its account and passwords confidential. Accordingly, the Customer shall not permit any third party to access or use the applicable Solution/s except as otherwise set forth in this Agreement or unless ConnectProtect has provided prior express written consent.
- 6.3.3 The transmission of the Customer's Data to ConnectProtect using the Solution/s may be impacted by in-country technical issues and requirements. ConnectProtect will provide reasonable assistance to the Customer in such instances but is not liable if the Customer's Data cannot be transmitted outside of such country. The Customer is responsible for implementing appropriate internal procedures and oversight to the extent it utilises the configuration of workflows and processes, including but not limited to response actions, and similar functionalities included with the Solution/s.
- 6.3.4 Hosting providers used by ConnectProtect to deliver the Solution/s may experience service interruptions and service outages outside the control of ConnectProtect. If such a hosting provider issues an outage notice that could materially impact delivery of the Solution/s, ConnectProtect will use commercially reasonable efforts to promptly notify the Customer about the outage and communicate the planned recovery time provided by the hosting provider. As part of the Solution/s, ConnectProtect may make recommendations to the Customer relating to the Customer's environment, the deployment of software and services, and enablement of Solution features.
- 6.3.5 The Customer is responsible for making decisions, in its sole discretion, pertaining to the implementation of any ConnectProtect recommendations and ConnectProtect has no liability for such decisions. The Customer acknowledges that any changes the

Customer makes to its code, infrastructure, or configuration of certain Solution/s after initial deployment may cause the Solution to cease working or function improperly or could prevent ConnectProtect from delivering the Solution/s and ConnectProtect will have no responsibility for the impact of any such Customer changes.

- 6.3.6 The Customer understands that depending on the Solution deployed, a Solution may consume additional CPU and memory in the Customer's environment while running in production.

6.4 Anti-corruption

- 6.4.1 In no event shall ConnectProtect be obligated to take any action or omit to take any action that it believes in good faith would cause it to be in violation of any laws or regulations of the United States, United Kingdom, European Union, or other applicable jurisdictions regarding bribery or corruption, including, without limitation, the U.S. Foreign Corrupt Practices Act (the "FCPA"), as amended, or UK Bribery Act 2010.

- 6.4.2 Neither Party will:

- 6.4.2.1 attempt to, directly or indirectly, improperly influence the sale or purchase of products by payments or other actions contrary to law or regulation;

- 6.4.2.2 take any action or permit or authorize any action that would violate or cause a party to violate the FCPA, the UK Bribery Act, or other applicable anti-corruption laws or regulations;

- 6.4.2.3 for the purpose of influencing any act or decision to obtain or retain business or direct business to any person, pay, offer or promise to pay, or authorize the payment of, directly or indirectly, any money or anything of value to or for the use or benefit of any of the following:

- (a) any government official (including any person holding an executive, legislative, judicial or administrative office, whether elected or appointed, any representative of any public international organization, any officer, director, or employee of a state-owned or controlled entity, or any person acting in any official capacity for or on behalf of any government, state-owned entity or public international organization);

- (b) any political party, official thereof, or candidate for political office; or

(c) any other person if a party or any respective partner, officer, director, employee, agent, representative or shareholder of such party knows or has reason to suspect or know that any part of such money or thing of value will be offered, given, or promised, directly or indirectly, to any of the above-identified persons or organizations.

- 6.4.3 Each Party acknowledges and agrees that none of its officers, directors, employees, agents or representatives is a government official or employee or an official or employee of any department or instrumentality of any government, nor is any of them an officer of a political party or candidate for political office, who will share directly or indirectly any part of the sums that may be paid pursuant to performance of this Agreement.
- 6.4.4 Each Party agrees to immediately notify the other Party should the abovementioned elements change during the term of this Agreement.
- 6.4.5 Each Party represents and warrants that neither this Agreement nor the performance of or exercise of rights under this Agreement is restricted by, in conflict with, requires registration or approval or tax withholding under, or will require any termination or expiration, compensation, or any compulsory licensing under, any Applicable Law of any country or other governmental entity, and each Party will not make any claim to the contrary. For the avoidance of doubt, each Party is relying on this representation and warranty, among other provisions of this Agreement, in entering this Agreement and would not enter this Agreement in its absence.

6.5 Public Entity Customers

- 6.5.1 This clause is only applicable where the Customer is a public entity. If the Customer is a public entity, the Customer acknowledges and agrees that this Agreement, including the Incorporated Terms, order form and other materials, if any, are the sole set of terms governing the delivery of the Solution/s to the Customer and for the avoidance of doubt, terms related to acceptance related to any services or work product shall not apply unless otherwise set out in supplemental Solution/s terms.
- 6.5.2 The terms of any request for proposal/s, request for information, invitation to qualify, purchasing agreement or cooperative contract, or similar agreement the Customer is using to purchase or subscribe to the Solution/s from an Authorised Partner do not apply to ConnectProtect.
- 6.5.3 Notwithstanding anything contrary in any other agreement or contract, the Customer understands and agrees that during a subscription term or engagement term, as applicable, ConnectProtect will maintain security controls and processes as described in the applicable supplemental Solution/s terms or in the DPA.

Accordingly, the Customer is responsible for determining if ConnectProtect's controls and processes comply with the Customer's data handling and security policies.

6.5.4 The Customer further represents that in subscribing for or purchasing the Solution/s:

6.5.4.1 the Customer is not relying on ConnectProtect for performance of any governmental contract or subcontract; and

6.5.4.2 the Customer is not receiving public funds to subscribe for or purchase the Solution/s.

6.5.5 If the Customer does intend to rely on the Solution/s to fulfil its obligations under a governmental contract or subcontract or utilise public funds to subscribe for or purchase the Solution/s, the Customer agrees to provide ConnectProtect advance written notice of that intention, and ConnectProtect shall have the option to terminate this Agreement by providing notice to the Customer to this effect.

7 FEES AND PAYMENT

7.1 Pricing for the Solution/s will be specified on an order form. The Solution/s may be provided:

7.1.1 on a subscription basis for a set term designated on the order form (as the case may be);

7.1.2 on a time and materials basis;

7.1.3 for a one-time fixed fee cost; and/or

7.1.4 such other bases set out in an order form, (collectively, the "Fees").

7.2 All Fees are non-cancellable and non-refundable, except as otherwise required by Consumer Protection Laws or set out in this Agreement.

7.3 The applicable term or subscription term for provision of the Solution/s (as the case may be) will be set forth on an order form.

7.4 Order forms and invoices issued by ConnectProtect

7.4.1 If an order form is issued to the Customer by ConnectProtect, the following terms, in addition to any other supplemental Solution/s terms, shall apply:

- 7.4.1.1 all Fees are payable in the currency set forth in the order form (or applicable invoice) and shall be due, payable and owing thirty (30) days from the date of invoice unless otherwise set forth on an order form.
- 7.4.1.2 late payments shall bear interest at a rate equal to the maximum rate permitted by Applicable Law.
- 7.4.1.3 in the event any action is taken to pursue collection of any fees payable hereunder, the Customer will reimburse ConnectProtect for ConnectProtect's costs associated with such collection, including reasonable legal fees where applicable.
- 7.4.1.4 the amounts payable to ConnectProtect are exclusive of any sales tax, use tax, excise tax, VAT, GST, HST, or other similar taxes ("Indirect Taxes"). The Customer is solely responsible for payment of all Indirect Taxes. If the Customer is required to pay any Indirect Taxes, the Customer shall pay such Indirect Taxes with no reduction or offset in the amounts payable to ConnectProtect hereunder and the Customer will pay and bear such additional amount as shall be necessary such that ConnectProtect receives the full amount of the payment required as if no such reduction or offset were required.
- 7.4.1.5 where the ConnectProtect has the legal obligation to pay or collect Indirect Taxes for which the Customer is responsible, the Customer authorises ConnectProtect to charge the Customer for such amount.
- 7.4.1.6 if the Customer believes that ConnectProtect has billed the Customer incorrectly, the Customer must contact ConnectProtect no later than thirty (30) days after the closing date on the first billing statement in which the error or problem appeared to receive an adjustment or credit. Inquiries should be directed to ConnectProtect's customer support department.
- 7.4.1.7 the Customer shall pay all amounts in the currency reflected in the order form and by the method listed on the invoice. Any suspension because of the Customer's failure to pay fees when due will not relieve Customer of its payment obligations.

7.5 Order forms issued by an Authorised Partner

- 7.5.1 if an order form and/or invoice is issued to the Customer by an Authorised Partner, clause 7.4 does not apply, and the following terms apply:
 - 7.5.1.1 the Customer is subscribing for or purchasing the Solution/s through the Authorised Partner.

- 7.5.1.2 the order form containing terms related to Fees, payment, taxes and any other related terms shall be between the Customer and the Authorised Partner.
- 7.5.1.3 the amounts paid by the Authorised Partner to ConnectProtect for the Customer's use of the Solution/s under this Agreement will be deemed the amount actually paid or payable under this Agreement for purposes of calculating ConnectProtect's liability under clause 12 .
- 7.5.1.4 the Customer's renewal pricing will be communicated to the Customer by the Authorised Partner in accordance with the terms the Customer has with the Authorised Partner or by ConnectProtect prior to any renewal term or subscription term, as applicable.

7.6 Online purchased subscriptions

If the Customer's subscription is purchased online, subscription Fees shall be remitted via an online third-party payment processor at the time of processing of the subscription within the Solution or on the ConnectProtect website. In such event, subscription fees will be collected by ConnectProtect's third-party payment processor and will be subject to such third-party payment processor's terms and conditions, including any terms related to data privacy.

8 CONFIDENTIALITY

- 8.1 For the purposes of this Agreement, "Confidential Information" shall include all information, data, and materials disclosed by one Party ("Disclosing Party") to the other Party ("Receiving Party"), whether orally, in writing, or in any other form, that is marked as confidential or would reasonably be understood to be confidential given the nature of the information and the circumstances of disclosure, including but not limited to, trade secrets, business plans, technical data, product plans, software, and customer information.
- 8.2 The Receiving Party agrees to maintain the confidentiality of the Disclosing Party's Confidential Information with at least the same degree of care it uses to protect its own confidential information, but in no event less than a reasonable degree of care. The Receiving Party shall not disclose any Confidential Information to any third party without the prior written consent of the Disclosing Party, except to employees, agents, or contractors who need to know such information for the purpose of fulfilling the Receiving Party's obligations under this Agreement and who are bound to confidentiality obligations no less stringent than those contained herein.
- 8.3 The Receiving Party agrees to use the Disclosing Party's Confidential Information solely for the purpose of exercising its rights and performing its obligations under this Agreement.

8.4 Confidential Information shall not include information that:

- 8.4.1 is or becomes publicly known through no act or omission of the Receiving Party;
- 8.4.2 is received from a third party without breach of any obligation of confidentiality;
- 8.4.3 is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information; or
- 8.4.4 is required to be disclosed by Applicable Law, provided that the Receiving Party gives the Disclosing Party prompt written notice of such requirement prior to disclosure and assists in obtaining an order protecting the information from public disclosure.

8.5 The Parties acknowledge that the unauthorised use or disclosure of the Disclosing Party's Confidential Information could cause irreparable harm for which monetary damages may be inadequate. Accordingly, the Disclosing Party shall have the right to seek injunctive relief or other equitable remedies in addition to any other rights and remedies available at law.

9 PERSONAL INFORMATION AND DATA PRIVACY

9.1 Personal information

9.1.1 Confidential Information provided by the Customer may include information that identifies, relates to, describes, is reasonably capable of being associated with or linked to a particular individual, whether directly or indirectly ("Personal Information"). The Customer is responsible for the lawfulness of any such Personal Information and the receipt, use, and processing of it under this Agreement. Accordingly, the Customer represents and warrants that, where it provides Personal Information to ConnectProtect or requests ConnectProtect to collect or process such information, it:

- 9.1.1.1 has complied with any Applicable Laws relating to the collection or provision of such information;
- 9.1.1.2 possesses any consents, authorisations, rights and authority, and has given all required notices to individual data subjects as are required to transfer or permit ConnectProtect to collect, receive, or access the Customer Data, including any Personal Information therein, for the Solution/s; and
- 9.1.1.3 to the extent required by Applicable Law, informed the individuals of the possibility of ConnectProtect processing their Personal Information on the Customer's behalf and in accordance with its instructions.

9.2 Data Protection

- 9.2.1 As required by Applicable Law or as otherwise agreed by the Parties, additional data protection terms are outlined in a separate DPA between the Parties (or such other data processing addendum which might from time to time be executed by the Parties). The DPA shall be incorporated into, and form an addendum to, this Agreement.
- 9.2.2 With respect to Customer Data that constitutes Personal Information, the Customer shall act as the accountable organization or the data controller, and ConnectProtect shall act as the service provider or the data processor.
- 9.2.3 Except as may be required by Data Protection Laws, ConnectProtect will process the Personal Information solely in accordance with the Customer's instructions. The "instructions" are defined in this Agreement, the DPA, and as may be additionally communicated by the Customer to ConnectProtect in writing from time-to-time.
- 9.2.4 Where permitted by a lawful basis, ConnectProtect may process Personal Information in the United Kingdom or other countries or jurisdictions outside of the country where it was collected, as described in the supplemental Solution/s terms (as the case may be) and the DPA.
- 9.2.5 The Customer will comply with its obligations under all laws applicable to it as an employer, the accountable organization, and/or data controller, including the responsibility for providing any requisite notices and obtaining any consents for such collection, processing, and transfer of Personal Information, including international transfers.

10 INDEMNITY

10.1 ConnectProtect's Indemnity

- 10.1.1 Subject to clause 10.3, ConnectProtect will defend and indemnify the Customer from any unaffiliated third-party claim (excluding claims by (i) the Customer's Affiliates, customers, end-users, or any party in a commercial relationship with the Customer; (ii) any person or entity acting at the Customer's direction or with the Customer's assistance; or (iii) any patent assertion entity, non-practicing entity, or other party whose primary business is licensing or asserting intellectual property rights) or action to the extent a court of competent jurisdiction determines, or the Parties agree in a written settlement agreement, that the Solution/s infringe any intellectual property right (patents, utility models, design rights, copyrights and trademarks or any other intellectual property right) having effect in the United

Kingdom and such other jurisdictions expressly identified on the applicable order form, provided that ConnectProtect's aggregate exposure across all jurisdictions shall not exceed the cap threshold specified in clause 10.1.2 below.

10.1.2 ConnectProtect will pay any settlements that ConnectProtect agrees to in a writing signed by an authorised officer of ConnectProtect or final judgments awarded to the third-party claimant by a court of competent jurisdiction, provided that ConnectProtect's total cumulative liability under this clause 10.1 shall not exceed the greater of:

10.1.2.1 the total Fees paid by the Customer in the 12 (twelve) months immediately preceding the first notice of the claim; or

10.1.2.2 £10,000 (ten thousand pounds sterling).

10.1.3 The above obligations do not apply with respect to the Solution/s, or portions or components thereof, that are:

10.1.3.1 not provided by ConnectProtect;

10.1.3.2 combined with other products, processes or materials that are not reasonably contemplated by the Documentation (where applicable) where the alleged infringement relates to such combination;

10.1.3.3 modified other than with ConnectProtect's express consent;

10.1.3.4 used after ConnectProtect's notice to the Customer of such activity's alleged or actual infringement;

10.1.3.5 not used by the Customer in strict accordance with this Agreement or the published Documentation (where applicable);

10.1.3.6 used in violation of any restrictions or prohibitions set forth in clause 6.1 or elsewhere in this Agreement;

10.1.3.7 based on Customer Data, content, or materials provided by Customer or entered into the Solution/s by Customer or its users;

10.1.3.8 used in any application, combination, or manner not documented in the Documentation or otherwise expressly authorised in writing by ConnectProtect;

10.1.3.9 based on compliance with Customer's specifications, instructions, or requirements that are not part of the standard Solution/s functionality;

- 10.1.3.10 arising from use of Beta Solutions, trial versions, or any Solution/s provided free of charge or for evaluation purposes;
 - 10.1.3.11 based on infringement that would have been avoided by use of an update, upgrade, or replacement made available by ConnectProtect at no additional charge, provided ConnectProtect notified Customer of the availability of such update and the infringement risk; or
 - 10.1.3.12 arising from use of the Solution/s beyond the scope, license counts, user numbers, endpoints, or other metrics specified in the applicable order form.
- 10.1.4 The indemnification obligations set forth in this clause 10.1 are ConnectProtect's sole and exclusive obligations, and the Customer's sole and exclusive remedies, with respect to infringement or misappropriation of third-party intellectual property rights of any kind.
- 10.1.5 ConnectProtect's indemnification obligations under this clause 10.1 shall apply only to claims of which ConnectProtect receives written notice during the Term or within twelve (12) months following the Termination Date. ConnectProtect shall have no obligation to indemnify the Customer for any claim of which it receives notice more than twelve (12) months after the Termination Date, regardless of when the alleged infringement occurred.
- 10.1.6 For the avoidance of doubt, this indemnity constitutes ConnectProtect's sole and entire obligation concerning the infringement or misappropriation of third-party intellectual property rights. ConnectProtect makes no warranty or representation that the Solution/s or the Customer's use thereof will not infringe or misappropriate any third-party intellectual property rights. The Customer acknowledges that the risk of intellectual property infringement claims is inherent in the technology industry and that this indemnity is a limited remedy subject to the conditions, exclusions, and limitations set forth in this Agreement.
- 10.1.7 To the extent any infringement claim arises in whole or in part from:
- 10.1.7.1 Customer Data
 - 10.1.7.2 the Customer's combination of the Solution/s with other products, services, or materials;
 - 10.1.7.3 the Customer's modification of the Solution/s, or

10.1.7.4 the Customer's instructions or specifications, the Customer shall indemnify, defend, and hold harmless ConnectProtect for that portion of any damages, costs, or expenses (including reasonable attorneys' fees) attributable to such Customer actions.

10.1.8 ConnectProtect's indemnification obligations under this clause 10.1 extend solely to monetary damages, costs, and expenses. ConnectProtect shall have no obligation to indemnify the Customer for, and shall not be liable for, any injunctive relief, specific performance, or any other equitable remedy that may be ordered against the Customer.

10.1.9 To the extent that the Customer maintains insurance coverage that covers intellectual property infringement claims, Customer shall first pursue recovery under such insurance policies before seeking indemnification from ConnectProtect. ConnectProtect's indemnification obligations shall be reduced by any amounts actually recovered by the Customer under such insurance policies.

10.2 Customer's Indemnity

10.2.1 Subject to clause 10.3 and to the extent permitted by law, the Customer agrees to defend and indemnify ConnectProtect from any third-party claim or action brought against ConnectProtect to the extent based on the Customer's alleged breach of clauses 6 or 9.1 .

10.2.2 The Customer agrees to pay any settlements that the Customer agrees to in writing signed by an authorised officer of the Customer or the Customer themselves (where a natural person) or final judgments awarded to the third-party claimant by a court of competent jurisdiction.

10.3 Procedure

10.3.1 Each Party's indemnification obligations are conditioned upon the indemnified Party:

10.3.1.1 providing the indemnifying Party with immediate written notice of any claim within 5 (five) Business Days of becoming aware of such claim, provided that failure to provide such notice shall void the indemnifying Party's obligations under this clause 10.1 if such failure materially prejudices the indemnifying Party's ability to defend the claim, including but not limited to the loss of any defence, right to appeal, or ability to mitigate damages;

10.3.1.2 granting the indemnifying Party the sole control of the defence or settlement of the claim;

10.3.1.3 providing reasonable information and assistance to the indemnifying Party in the defence or settlement of the claim at the indemnifying Party's expense; and

10.3.1.4 maintaining strict confidentiality regarding the existence and terms of any settlement discussions and refraining from making any public statements regarding the claim without ConnectProtect's prior written consent.

10.3.2 Notwithstanding clause 10.3.1 above:

10.3.2.1 the indemnifying Party may not make an admission of fault on behalf of the indemnified Party without its written consent;

10.3.2.2 any settlement requiring the indemnified Party to admit liability requires their prior written consent, which consent shall not be unreasonably withheld or delayed; and

10.3.2.3 the indemnified Party may join in the defense with its own counsel at its own expense.

10.4 If the Customer's use of the Solution/s has become, or in ConnectProtect's sole and absolute discretion is likely to become, the subject of any claim of infringement, ConnectProtect may at its sole option and in the following order of priority:

10.4.1 procure for the Customer the right to continue using and receiving the Solution/s at no additional cost to ConnectProtect exceeding 10% (ten percent) of the annual Fees for the affected Solution/s;

10.4.2 replace or modify the Solution/s to make them non-infringing, provided such replacement or modification does not materially decrease the functionality described in the Documentation;

10.4.3 substitute functionally equivalent alternatives for the Solution/s; or

10.4.4 if ConnectProtect, in its sole discretion, determines that options in clauses 10.4.1 to 10.4.3 above are not commercially practicable, terminate this Agreement upon 30 (thirty) days' written notice and refund any pre-paid unused Fees attributable to the terminated Solution/s calculated on a pro-rata basis as of the effective date of termination, which refund shall constitute Customer's sole and exclusive remedy.

11 WARRANTIES AND DISCLAIMERS

11.1 Each Party represents and warrants to the other Party that:

- 11.1.1 it is duly organized, validly existing and in good standing as a corporation or other entity under the Applicable Laws of its jurisdiction of incorporation;
- 11.1.2 it has the full right, power and authority to enter into this Agreement, to grant the rights and licenses granted hereunder and to perform its obligations hereunder;
- 11.1.3 the execution of this Agreement by its representative has been duly authorised by all necessary corporate action of the Party; and
- 11.1.4 this Agreement will constitute the legal, valid and binding obligation of such Party, enforceable against such Party.

11.2 Product warranty

- 11.2.1 ConnectProtect warrants that during the term of this Agreement and provided that the Customer is not in breach of this Agreement or as otherwise prohibited by Consumer Protection Laws that:
 - 11.2.1.1 the Solution/s provided under this Agreement do not infringe or misappropriate any intellectual property rights of any third party;
 - 11.2.1.2 the Solution/s shall substantially perform as described in the Documentation; and
 - 11.2.1.3 it will comply with Applicable Laws as it pertains to its obligations and the Customer Data required for the delivery and performance of the Solution/s.
- 11.2.2 In the event of any breach of clause 11.2.1 above, ConnectProtect shall, unless otherwise provided for in the indemnification obligations in clause 10.1 , prohibited by Consumer Protection Laws, or provided in clause below), repair or replace the Solution/s that are subject to the warranty claim at no cost to the Customer or, to the extent a repair or replacement is not practicable, refund any pre-paid Fees for the Solution/s, or parts thereof (where applicable), subject to the warranty claim.
- 11.2.3 Other than those warranties applicable or available at law or set out in this clause 11 , the Solution/s are provided without warranty of any kind, whether express or implied, including those implied warranties or conditions of design, merchantability, fitness for a particular purpose, and any warranties of title.
- 11.2.4 The Customer further acknowledges that ConnectProtect does not warrant:
 - 11.2.4.1 that the Solution/s will at all times be uninterrupted or error free;

11.2.4.2 that the Solution/s are not vulnerable to fraud or unauthorised use; and

11.2.4.3 that all threats, vulnerabilities, attacks or malware will be discovered, reported or remedied.

11.2.5 The Customer is responsible and ConnectProtect shall have no responsibility for determine that the use of the Solution/s complies with Applicable Law in which the Customer may deploy and use the Solution/s.

11.2.6 The Customer further acknowledges and agrees that the Solution/s are not designed or intended for use in any hazardous environment requiring specific levels of performance or operation, nor are the Solution/s intended for the operation of navigation, nuclear facilities, weapons systems, life-support systems, or any application or installation where failure of the Solution/s could result in death, severe injury or proprietary damage.

11.3 The Customer acknowledges, understands, and agrees that new threats are constantly evolving. Accordingly, ConnectProtect does not guarantee or warrant that it will find, locate, or discover all of the Customer's system threats, vulnerabilities, malware, and malicious software, or that all such system threats, vulnerabilities, malware, and malicious software can or will be contained or uncontained in the delivery and performance of the Solution/s.

11.4 The Customer acknowledges that certain features and activities performed by ConnectProtect could possibly result in interruptions or degradation to the Customer's systems and environments and accepts those risk and consequences.

11.5 The Customer further assumes all risks associated with any third-party systems, but not including Third Party Products, or services, including any cloud IAAS and SAAS systems, tools, and/or environments and any diagnostic tools, APIs, and other such integrations, that the Customer uses or deploys in connection with the delivery or provision of the Solution/s.

11.6 The Customer acknowledges that certain components of the Solution/s ("Open Source Components") may be covered by so-called "open source" software licenses, which means any software licenses approved as open source licenses by the appropriate authority or body. ConnectProtect hereby represents and warrants that all Open Source Components in the Solution/s will be provided to the Customer by ConnectProtect hereunder in a manner compliant with their applicable open source licenses.

11.7 Where the Solution/s incorporate third-party Open Source Components, the Customer acknowledges that:

11.7.1 such Open Source Components are governed by their respective open source licenses, which take precedence over the terms of this Agreement to the extent of

any direct conflict with respect to the use, modification, or distribution of such Open Source Components specifically;

11.7.2 ConnectProtect shall make available to the Customer, upon reasonable request, copies of the applicable open source licenses governing such Open Source Components;

11.7.3 the Customer's rights and obligations regarding such Open Source Components are subject to compliance with the applicable open source license terms; and

11.7.4 any restrictions in this Agreement that would be prohibited by the applicable open source licenses shall not apply, but shall continue to apply to all other aspects of the Solution/s.

11.8 To the extent required by the licenses governing Open Source Components incorporated in the Solution/s, ConnectProtect hereby offers to provide the Customer, upon written request submitted to ConnectProtect's designated support channels, with:

11.8.1 complete corresponding source code for such Open Source Components;

11.8.2 access to copy the source code from a network server at no charge beyond the cost of distribution; or

11.8.3 a written offer valid for at least 3 (three) years to provide such source code.

11.9 For purposes of clause 11.8, any such request must specify the particular Open Source Component and version for which source code is sought. ConnectProtect may fulfill such requests by directing the Customer to the publicly available source code repositories maintained by the respective open source projects. The Customer acknowledges that ConnectProtect provides no warranties, support, or indemnification with respect to Open Source Components beyond those expressly required by the applicable open source licenses, and that any modifications to Open Source Components by the Customer shall be at the Customer's sole risk and responsibility.

11.10 Third Party Products may carry a limited warranty from the third party publisher, provider, or original manufacturer of such Third Party Products. Where required or allowed, ConnectProtect will pass through to the Customer or directly manage for the benefit of the Customer's use of the Third Party Products as part of the Solution/s the manufacturer warranties related to such Third Party Products.

11.11 Customer represents and warrants that it shall:

- 11.11.1 be responsible for ensuring the security and confidentiality of all its Administrator IDs, usernames, and passwords;
- 11.11.2 use commercially reasonable efforts to prevent unauthorised access to, or use of, the Solution/s;
- 11.11.3 notify ConnectProtect promptly upon discovery of any unauthorised use of the Solution/s or any breach, or attempted breach, of security of the Solution/s;
- 11.11.4 not violate any Applicable Laws relevant to its performance of its obligations herein, including those of any governmental (including any regulatory or quasi-regulatory) agency;
- 11.11.5 not use the Solution/s and transfer any Customer Data to ConnectProtect for any fraudulent purposes; and
- 11.11.6 implement safeguards within the Customer's environment to protect the Solution/s, including specifically, any equipment, from the introduction, whether intentional or unintentional, of:
 - 11.11.6.1 any virus or other code, program, or sub-program that damages or interferes with the operation of the equipment or halts, disables, or interferes with the operation of the Solution/s; or
 - 11.11.6.2 any device, method, or token whose knowing or intended purpose is to permit any person to circumvent the normal security of the Solution/s .

11.12 The Customer authorises ConnectProtect to perform the service components of the Solution/s as identified in any applicable supplemental Solution/s terms (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform such services) on network resources with the internet protocol addresses or other designated identifiers identified by the Customer. The Customer further represents that, if the Customer does not own such network resources, it will have obtained consent and authorisation from the applicable third party/ies to permit ConnectProtect to provide such services on such third party's network resources.

11.13 Insurance coverage and financial protection

- 11.13.1 Notwithstanding anything to the contrary in this Agreement, the Customer acknowledges and understands that ConnectProtect may maintain its own insurance coverage from time to time, including but not limited to professional indemnity, cyber liability, and errors and omissions insurance as it deems appropriate in its sole discretion ("Insurance Coverage").

11.13.2 ConnectProtect therefore makes no representation or warranty regarding the existence, scope, adequacy, or limits of any such Insurance Coverage, and the Customer expressly agrees that it shall not rely upon, nor is it entitled to the benefit of, any Insurance Coverage maintained by ConnectProtect.

11.14 Customer insurance obligations

11.14.1 The Customer acknowledges that the use of the Solution/s does not eliminate or reduce cybersecurity risks and that the Customer remains solely responsible for protecting its systems, data, operations, and business continuity against all threats, incidents, and losses.

11.14.2 The Customer agrees to procure and maintain, at its own cost and expense, throughout the Term and for a period of 12 (twelve) months thereafter, adequate insurance coverage with reputable insurers, including but not limited to:

11.14.2.1 cyber liability insurance with coverage as is commercially reasonable given the Customer's business operations and risk profile;

11.14.2.2 professional indemnity insurance with coverage as is commercial reasonable given the Customer's business operations and risk profile;

11.14.2.3 business interruption insurance covering losses arising from cyber incidents, security breaches, and system failures;

11.14.2.4 data breach and privacy liability insurance covering the loss, theft, or unauthorised disclosure of Customer Data or Personal Information; and

11.14.2.5 such other insurance coverage as may be required by Applicable Law or reasonably necessary to protect against losses arising from or in connection with the Customer's use of the Solution/s or its IT environment generally.

11.14.3 Upon ConnectProtect's reasonable request, the Customer shall provide certificates of insurance or other satisfactory evidence demonstrating compliance with the insurance obligations set forth in clause 11.14.2, the Customer shall ensure that all such policies:

11.14.3.1 name the Customer as the named insured;

11.14.3.2 provide that they shall not be cancelled, materially altered, or allowed to lapse without at least 30 (thirty) days' prior written notice to ConnectProtect;

11.14.3.3 include a waiver of subrogation in favour of ConnectProtect, its Affiliates, officers, directors, employees, agents, and contractors; and

11.14.3.4 are primary and non-contributory with respect to any insurance maintained by ConnectProtect.

11.15 Waiver of claims and subrogation

11.15.1 To the fullest extent permitted by Applicable Law, the Customer hereby waives and releases any and all claims, demands, actions, or causes of action against ConnectProtect, its Affiliates, officers, directors, employees, agents, contractors, and insurers arising from or relating to any loss, damage, liability, cost, or expense that is covered, or should have been covered, by insurance that the Customer is required to maintain pursuant to clause 11.14 or that the Customer would reasonably be expected to maintain in the ordinary course of its business operations.

11.15.2 The Customer shall cause its insurers to waive all rights of subrogation against ConnectProtect, its Affiliates, officers, directors, employees, agents, and contractors with respect to any insurance policies maintained by the Customer.

11.15.3 The Customer acknowledges and agrees that any failure to maintain adequate insurance coverage as required herein, or to procure waivers of subrogation as required herein, shall not increase ConnectProtect's liability or obligations under this Agreement, and that the limitations of liability set forth in clause 12 or otherwise in this Agreement shall remain in full force and effect regardless of the Customer's insurance position.

11.16 Remedies exclusive

The Customer agrees that its sole and exclusive remedies for any losses arising from or in connection with the use of the Solution/s are those expressly set forth in this Agreement, and that neither the existence nor absence of Insurance Coverage maintained by either Party shall expand, modify, or otherwise affect such remedies or the limitations of liability set forth in clause 12 or otherwise in this Agreement.

12 LIMITATION OF LIABILITY

12.1 To the fullest extent permitted by Applicable Law and subject to clause 12.2 below, ConnectProtect shall not be liable, for any cause related to or arising out of or in connection with this Agreement, whether based on a contract, tort or otherwise, howsoever arising, to the Customer or any third party for:

- 12.1.1 damages based on use or access, interruption, delay or inability to use the Solution/s, lost revenues or profits, loss of products, business or goodwill, loss or corruption of data, loss resulting from system failure, malfunction or shutdown, failure to accurately transfer, read or transmit information, failure to update or provide correct information, system incompatibility or provision of incorrect compatibility information, breaches by an Authorised Partner , or breaches in the Customer's security system;
- 12.1.2 any indirect, special, incidental, or consequential damages;
- 12.1.3 any amounts that exceed the total Fees paid or payable by the Customer for the Solution/s that are the subject of the claim pertaining to the 12 (twelve) month period immediately preceding the event which gives rise to a damages claim; or
- 12.1.4 any losses, damages, costs, or expenses that are covered, or would have been covered but for any act or omission of the Customer, by insurance that the Customer is required to maintain under clause 11.14 or that a reasonably prudent business operating in the Customer's sector would ordinarily maintain in the course of its business operations.

12.2 This limitation of liability clause 12.2 only pertains to those Customers utilising the Solution/s in Australia as a "consumer" under the Competition and Consumer Act 2010 (CH) Schedule 2. ConnectProtect shall not be liable to a Customer for:

- 12.2.1 any lost profits, revenue, or savings, lost business opportunities, lost data, or special, incidental, consequential, or punitive damages, even if ConnectProtect has been advised of the possibility of such damages or losses or such damages or losses were reasonably foreseeable; or
- 12.2.2 an amount that exceeds the total Fees paid or payable by the Customer for the Solution/s that are the subject of the claim pertaining to the 12 (twelve) month period immediately preceding the event which gives rise to such damages, and these limitations will apply notwithstanding any failure of essential purpose of any remedy specified in this Agreement and multiple claims will not expand the limitations specified in this clause 12.2 .

12.3 Clauses 12.1 and 12.2 do not limit or exclude liability of ConnectProtect or its Affiliates in the event of death or personal injury caused by its negligence or wilful misconduct, including liability for which it is not by Applicable Law permitted to exclude.

12.4 Aggregate liability cap

- 12.4.1 Subject to clause 12.3 above, the limitations set forth in this clause 12 shall apply in the aggregate to all claims, demands, actions, and causes of action of every kind and

nature arising under or related to this Agreement or the provision or use of the Solution/s, regardless of:

- 12.4.1.1 the number of incidents, events, breaches, or occurrences giving rise to liability;
- 12.4.1.2 the theory or theories of liability asserted (whether in contract, tort, negligence, breach of statutory duty, strict liability, or otherwise);
- 12.4.1.3 the number of claimants or affected parties;
- 12.4.1.4 whether claims arise from related or unrelated events; or
- 12.4.1.5 whether claims are brought concurrently or consecutively.

12.4.2 For the avoidance of doubt, the maximum aggregate liability of ConnectProtect under this Agreement, including for all claims arising during or in connection with the Term and any period thereafter, shall not exceed the amount specified in clause 12.1.3 above, regardless of the number or nature of claims asserted.

12.4.3 Multiple or repeated breaches arising from the same root cause, or from substantially similar facts or circumstances, shall be treated as a single claim for purposes of calculating the limitation period in clause 12.1.3, with the 12 (twelve) month period measured from the date of the first occurrence.

13 TERM AND TERMINATION

13.1 This Agreement shall be in effect for the Term (i.e., for as long as the Customer is subscribed to the ConnectProtect Solution/s (“Subscription Term”)) or for a term otherwise specified in an order form or set out in supplemental Solution/s terms to the extent applicable.

13.2 Any Subscription Term will automatically renew in its entirety at the end of the initial Subscription Term, but in no event more than a 12 (twelve) month term, unless otherwise set out in writing by ConnectProtect, and the renewal will be subject to the then-current terms and applicable price at the time of renewal (“Automatic Renewal”).

13.3 Notwithstanding clause 13.2 above, should either Party wish to opt out of the Automatic Renewal or reduce the Solution/s scope for which the Customer may be subscribed for, then such Party must notify the other Party no less than 30 (thirty) days prior to the expiration of the relevant Subscription Term.

13.4 Either Party may also terminate this Agreement if:

13.4.1 the other Party becomes insolvent, files a petition or application (as the case may be) for bankruptcy, liquidation or any other similar or akin process, or makes an assignment or compromise for the benefit of its creditors generally;

13.4.2 breaches any of its obligations under this Agreement in any material respect, which breach is not remedied within 10 (ten) days following written notice to such Party, including any non-payment by the Customer of undisputed Fees; or

13.4.3 as otherwise provided for in any supplemental Solution/s terms.

13.5 Upon termination in accordance with clause 13.3 or clause 13.4 , the Customer agrees to cease all use of the Technology, installed or otherwise, and permanently erase or destroy all copies of any Technology, including all content and virtual equipment, that are in its possession or under its control and promptly, to the extent applicable, remove and return all physical equipment to ConnectProtect.

13.6 Except as otherwise provided for by Applicable Law, ConnectProtect will remove, delete, or otherwise destroy all copies of Confidential Information in its possession.

13.7 Should a Customer elect to have its Customer Data returned upon expiration, it is the Customer's responsibility to work with ConnectProtect to ensure such information is returned prior to destruction.

14 FORCE MAJEURE

14.1 A Party will not be in breach of this Agreement or otherwise liable to the other party for any failure to perform or delay in performing its obligations under this Agreement to the extent that such failure or delay is due to a Force Majeure Event or to the effects of a Force Majeure Event.

14.2 Subject to clauses 14.4 and 14.5 , a Party will not be in breach of this Agreement or otherwise liable to the other Party for any failure to perform or delay in performing its obligations under this Agreement to the extent that this is due to a Force Majeure Event affecting the other Party's failure to perform or delay in performing any of its obligations under this Agreement due to a Force Majeure Event.

14.3 If a Force Majeure Event occurs and a Party affected by that Force Majeure Event wishes to claim relief under clause 14.1 , that Party will:

14.3.1 give the other Party written notice of the occurrence, anticipated duration and impact of the Force Majeure Event and its wish to claim relief;

14.3.2 give written notice to the other Party promptly upon the Force Majeure Event ceasing to delay or prevent performance of its obligations under this Agreement;

14.3.3 continue to perform all of its obligations under this Agreement the performance of which is not affected by the Force Majeure Event; and

14.3.4 take all reasonable measures, without being required to incur additional expenditure, to mitigate the effects of the Force Majeure Event.

14.4 If ConnectProtect is the Party affected by the Force Majeure Event the Customer will continue to pay the Fees for which ConnectProtect continues to supply or perform notwithstanding the occurrence of the Force Majeure Event.

14.5 If the Customer is the Party affected by the Force Majeure Event, the Customer will continue to pay the Fee in accordance with the provisions of this Agreement.

14.6 If ConnectProtect is unable to provide all or substantially all of the Solution/s services for a period of more than 30 (thirty) days or for a total of 30 (thirty) days or more in a 3 (three) month period due to a Force Majeure Event, ConnectProtect will be entitled to terminate this Agreement by giving not less than 30 days' written notice to that effect to the Customer.

15 SUSPENSION

15.1 ConnectProtect may suspend its delivery or provision of the Solution/s, whether wholly or in part, and the Customer's use thereof where the Customer fails to make payment of any undisputed Fees within 15 (fifteen) days, unless otherwise extended or reduced by ConnectProtect in its sole discretion from time to time, of ConnectProtect's, or its Authorised Partner's (where applicable), notice to the Customer of such failure to pay or to comply with any Applicable Law, court order or governmental request.

15.2 In addition, if the Customer's account is the subject of denial-of-service attacks, hacking attempts, or other malicious activities, or the Customer's activities reasonably appear to be in breach of clause 6.1, ConnectProtect may delete any files, programs, data, and email messages associated with the Customer's account and/or will work with Customer to resolve such matters as soon as possible.

15.3 In accordance with clause 15.2, ConnectProtect may be required to suspend the Solution/s until the issues are resolved. ConnectProtect will provide advance notice to the Customer of such suspension, where reasonably practicable. ConnectProtect will restore access to the applicable Solution/s as soon as the event giving rise to the suspension in question has been resolved.

15.4 ConnectProtect reserves the right to charge a reconnection fee if any of the events listed above occur in connection with any Customer act or omission.

16 SURVIVAL

The Customer's payment obligations and provisions relating to property rights and confidentiality shall survive expiration or termination of this Agreement. In particular and including this clause 16, clauses 5, 8 through 10, 12, 13, 17 and 18 shall survive expiration or termination of this Agreement.

17 UPDATES

ConnectProtect reserves the right to modify this Agreement, including any Incorporated Terms its sole discretion. In no event will any changes materially decrease the Solution/s features and functionalities that the Customer has purchased or subscribed to during the then-current term. Should ConnectProtect make any modifications, ConnectProtect will post the amended terms on the applicable URL links and notify the Customer via email or such other direct written communication method implemented by ConnectProtect from time-to-time. The Customer may notify ConnectProtect within 30 (thirty) days after the effective date of the change of its rejection of such change. If the Customer notifies ConnectProtect of its rejection during such 30 (thirty) day period, then the Customer will remain governed by the terms in effect immediately prior to the change until the end of the Customer's then-current Term. However, any subsequent renewal of the Subscription Term will be renewed under the then-current Agreement, unless otherwise agreed to in writing by the Parties.

18 GENERAL

18.1 Notice

18.1.1 Unless otherwise provided for in this Agreement, all notices, requests, consents, claims, demands, waivers and any other communications in terms of this Agreement shall be in writing and shall be deemed to have been given:

18.1.1.1 when delivered by hand (with written confirmation of receipt);

18.1.1.2 on the next business day after the date sent if sent for overnight delivery by a generally recognized international courier (e.g., FedEx, UPS, DHL); or

18.1.1.3 on the date sent by e-mail (with confirmation of transmission) if sent during normal business hours of the recipient, and on the next business day if sent after normal business hours of the recipient.

18.1.2 ConnectProtect's address for notification purposes shall be: E-mail: Legal@connectprotect.com; and Physical Address: Office 616, Linen Hall, 162-168 Regent Street, London, United Kingdom, W1B 5TB.

18.1.3 Either Party may update its notice address upon written notice to the other Party, with the Customer's chosen address and other information being that which is set out on an order form with ConnectProtect.

18.2 Publicity

Unless the Customer otherwise directs ConnectProtect by way of written notice, which may be given at any time, the Customer consents to and agrees that ConnectProtect may list the Customer's company name (where applicable) and/or logo (in accordance with any trademark guidelines a Customer may provide) as a ConnectProtect customer within its customer lists and for use with ConnectProtect's partners in a manner that does not suggest the Customer's endorsement of any specific ConnectProtect Solution.

18.3 Independent Contractors

The Parties to this Agreement are independent contractors. Neither Party has the authority to bind the other Party without the express written authorisation of the other Party. Nothing herein may be construed to create an employer-employee, franchisor-franchisee, agency, partnership, or joint venture relationship between the Parties. Each Party shall be liable for the actions and obligations of its and its Affiliates, including any of their respective users, employees, subcontractors, agents, consultants, advisors, or such other similar third parties.

18.4 Assignment

The Customer shall not be entitled to assign or otherwise transfer any of its rights and/or duties arising out of or in connection with this Agreement and/or parts thereto to any third party, voluntarily or involuntarily, including by change of control, operation of law or any other manner, without ConnectProtect's express prior written consent. Any purported assignment or other transfer in violation of this clause 18.4 shall be null and void. No such assignment or other transfer shall relieve the assigning Party of any of its obligations.

18.5 Governing Law, Disputes and Jurisdiction

18.5.1 Governing Law

18.5.1.1 The rights and obligations of the Parties under this Agreement shall not be governed by the provisions of the 1980 U.N. Convention on Contracts for the International Sale of Goods or the United Nations Convention on the Limitation Period in the International Sale of Goods, as amended.

18.5.1.2 This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by the law of England and Wales.

18.5.2 Dispute Resolution

- 18.5.2.1 Subject to clauses 18.5.2.5 and 18.5.2.6 , neither Party may during the Term commence proceedings in relation to a Dispute unless that Party has:
- (a) served a written notice (a “Referral Notice”) on the other Party notifying it of the relevant Dispute;
 - (b) already received a Referral Notice from the other Party in relation to the same Dispute.
- 18.5.2.2 Following service of a Referral Notice in relation to a Dispute, each Party will respectively procure that such Dispute will be referred for resolution to any person of senior management level (or above) for the time being on behalf of ConnectProtect and any person of senior management level (or above) for the time being on behalf of the Customer. Those representatives will meet at the earliest convenient time and in any event within 10 (ten) days of the date of service of the relevant Referral Notice and will negotiate in good faith and attempt to resolve the Dispute.
- 18.5.2.3 If a Dispute has not been resolved within 10 (ten) days of the date of service of the relevant Referral Notice each Party will respectively procure that such Dispute be referred for resolution to the Chief Executive Officer for the time being on behalf of ConnectProtect and the Chief Executive Officer (or another representative of the same level) for the time being on behalf of the Customer. Those representatives will meet at the earliest convenient time and in any event within 14 (fourteen) days of the date of service of the relevant Referral Notice and will negotiate in good faith to resolve the Dispute.
- 18.5.2.4 If a Dispute is not resolved within 14 (fourteen) days of service of the relevant Referral Notice either Party may commence proceedings in accordance with clause 18.5.3 or, if both Parties agree in writing to do so, the Parties will attempt to settle the Dispute by mediation in accordance with the CEDR Model Mediation Procedure in each case irrespective of whether clauses 18.5.2.2 and 18.5.2.3 have been complied with. The provisions of this clause 18.5.2.4 are without prejudice to any right that either Party may have to damages in respect of any breach by the other Party of clauses 18.5.2.2 and 18.5.2.3 . Either Party may withdraw from mediation at any time.
- 18.5.2.5 Nothing in this clause 18.5.2 will prevent either Party from:
- (a) seeking orders for specific performance, interim or final injunctive relief;
 - (b) exercising any rights it has to terminate this Agreement; or

(c) commencing any proceedings where this is necessary to avoid any loss of a claim due to the rules on limitation of actions.

18.5.2.6 Nothing in this clause 18.5.2 will prevent or delay ConnectProtect from:

(a) commencing any proceedings in relation to infringement of its intellectual property rights; or

(b) commencing any proceedings for non-payment of dispute invoices.

18.5.3 Jurisdiction

18.5.3.1 Subject to clauses 18.5.2 and 18.5.3.2, the courts of England and Wales have exclusive jurisdiction to determine any dispute arising out of or in connection with this Agreement (including in relation to any non-contractual obligations).

18.5.3.2 Either Party may seek interim injunctive relief or other interim measure of protection in any court of competent jurisdiction.

18.5.3.3 Subject to clause 18.5.3.2, each Party waives any objection to, and agrees to submit to, the jurisdiction of the courts of England and Wales. Each Party agrees that a judgment or order of any such court is binding upon it and may be enforced against it in the courts of any other jurisdiction.

Whole Agreement

18.5.4 Save as otherwise provided for in this Agreement, this Agreement constitutes the sole record of the agreement between the Parties in relation to its subject matter.

18.5.5 No Party shall be bound by any representation, warranty, promise or the like not recorded in this Agreement.

18.6 Variation

No addition to, variation, novation or agreed cancellation of this Agreement shall be of any force or effect unless in writing and signed by or on behalf of the Parties. For the purposes of this clause 18.6, “writing” shall include e-mail.

18.7 Counterparts

This Agreement may be signed in separate counterparts, each of which shall be deemed to be an original and all of which taken together shall constitute one and the same instrument. A counterpart of this Agreement in electronic form shall be conclusive evidence of the original

signature and shall be as effective in law as the counterparts in original form showing the original signatures.

18.8 Severance

All provisions in this Agreement are, notwithstanding the manner in which they have been put together or linked grammatically, severable from each other. Any provision of this Agreement which is or becomes unenforceable, whether due to voidness, invalidity, illegality, unlawfulness or for any other reason whatsoever, shall only to the extent that it is so unenforceable, be treated as pro non scrip to and the remaining provisions of this Agreement shall be of full force and effect. The Parties declare that it is their intention that this Agreement would be executed without such unenforceable provisions if they were aware of such unenforceability at the time of its execution.

18.9 Indulgence

18.9.1 No indulgence which a Party may grant to any other Party shall constitute a waiver of any of the rights of the grantor.

18.9.2 The provisions of this Agreement shall be binding upon the successors-in-title and the permitted assigns of the Parties. Accordingly, the rights and obligations of each Party pursuant to this Agreement shall devolve upon and bind its successors-in- title and permitted assigns.

18.10 Warranty

Each Party warrants to the other Parties that it has the power, authority and legal right to sign and perform this Agreement, and that this Agreement has been authorised by all necessary actions of its directors, as the case may be, and that this Agreement constitutes valid and binding obligations on it in accordance with its terms. Each Party further warrants to the other Parties that the conclusion and implementation of this Agreement does not conflict with any obligation or restriction applicable to that Party, whether in terms of any Applicable Law, its memorandum of incorporation or otherwise.

18.11 Costs

All costs, charges and expenses of any nature whatsoever which may be incurred by a Party in enforcing its rights in terms of this Agreement, including legal costs on the scale of attorney and own client and including collection commission, irrespective of whether any action has been instituted, shall be recoverable from the Party against which such rights are successfully enforced.

18.12 Rights of third parties

Subject to the rights of Authorised Partners as expressly set out in the terms of this Agreement, this Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement. The rights of the Parties to rescind or vary this Agreement are not subject to the consent of any other person.

18.13 Independent advice

Each Party acknowledges that it has been free to secure independent legal and other advice as to the nature and effect of all of the provisions of this Agreement and that it has either taken such independent legal and other advice or voluntarily decided not to do so.

19 SIGNATURE

Signed on behalf of the Parties, each signatory hereto warranting that he/she has due authority to do so.

2026

1. _____

2. _____

Name: _____

2026

1. _____

2. _____

Name: _____

44

SCHEDULE 1

SERVICE REQUIREMENTS, INFORMATION AND LEVELS

1 SERVICE REQUIREMENTS, INFORMATION AND LEVELS

1.1 Availability

24/7 / 365 monitoring by ConnectProtect's SOC.

1.2 Response times

1.2.1 Critical (P1) incidents: notification and response initiation within 30 minutes.

1.2.2 High (P2) incidents: notification and response initiation within 60 minutes.

1.2.3 Medium to low (P3 and P4) incidents: notification and response initiation within 240 minutes.

1.3 Reporting

Monthly reports will be delivered electronically to the authorised Customer contact.

1.4 Exclusions

MXDR does not include: (i) remediation or recovery services beyond detection, containment, and initial response; (ii) security responsibilities related to unsupported systems or environments not integrated with the MXDR platform; (iii) onsite support, unless separately agreed to in writing by both Parties; and (iv) forensic investigations, legal advisory services, or regulatory breach reporting, unless explicitly agreed to in writing amongst the Parties.

1.5 Customer success (optional)

ConnectProtect shall conduct a monthly service review ("Optional Monthly Service Review") with the Customer as part of their MXDR service Solution. Each review shall encompass without limitation, an examination of security incidents, threat activity, and the efficacy of detection and response measures undertaken during the preceding month. The review shall further address overall service performance, recommended remedial or enhancement measures, and any material developments in threat intelligence, technology, or best practices relevant to the Customer's environment. The Parties acknowledge that the purpose of the Optional Monthly Service Review is to ensure continued alignment of the service Solution/s with the Customer's security objectives and to facilitate identification of opportunities to improve the Customer's security posture.

1.6 Service Level Penalties

- 1.6.1 Service Credit Model: For each calendar month in which ConnectProtect fails to meet the agreed MTTR service levels, the Customer shall be entitled to a service credit equivalent to 5% of the monthly service Fee for each breach, capped at 25% of the monthly Fee.
- 1.6.2 The Service Credit Model shall not apply where:
 - 1.6.2.1 the delay was caused by inaccurate or delayed information from the Customer;
 - 1.6.2.2 the incident originated from systems not under the agreed monitoring scope; and/or
 - 1.6.2.3 Force Majeure events impacted the delivery or provision of the service Solution/s.

1.7 Customer responsibilities

- 1.7.1 The Customer shall:
 - 1.7.1.1 provide and maintain accurate system, network, and endpoint inventories required for monitoring;
 - 1.7.1.2 ensure necessary integrations and data connectors are in place to allow ingestion of security telemetry;
 - 1.7.1.3 designate appropriate points of contact for incident notifications and escalations;
 - 1.7.1.4 cooperate with ConnectProtect's SOC analysts in incident investigations and remediations;
 - 1.7.1.5 be solely responsible for the implementation, in a timely and effective manner, of all security recommendations provided by ConnectProtect. Where ConnectProtect designates any recommendation as "critical", the Customer shall, without delay, either (i) implement such recommendation in full, or (ii) formally accept the risk in writing. For the avoidance of doubt, ConnectProtect shall have no liability whatsoever, whether in contract, tort (including negligence), statute, or otherwise, for any security incident, breach, loss, damage, claim, or expense arising, directly or indirectly, from the Customer's failure to implement any such critical recommendation.

The Customer expressly waives any and all claims against ConnectProtect in connection therewith; and

- 1.7.1.6 be solely responsible for ensuring that all designated contact details, including names, telephone numbers, email addresses, and escalation paths, access rights, are accurate, current, and properly maintained within ConnectProtect's portal at all times. The Customer acknowledges and agrees that ConnectProtect shall rely exclusively on such information for the purposes of notification and escalation in the event of a potential or actual security incident. To the fullest extent permitted by law, ConnectProtect shall bear no liability or responsibility whatsoever, whether in contract, tort (including negligence), statute, or otherwise, for any failure, delay, or inability to contact the Customer, or any of its representatives, where such failure, delay, or inability is attributable, whether wholly or in part, to the Customer's failure to maintain accurate and current contact information. For the avoidance of doubt, ConnectProtect shall not be liable for any security incident, breach, loss, damage, claim, or expense arising, directly or indirectly, from such failure, delay, or inability to establish contact.

1.8 Customer security logs

- 1.8.1 All subscriptions to the service Solution/s include 30 (thirty) days of hot storage for Customer logs ("Security Log Window"). "hot storage" means that logs are immediately accessible for detection, hunting, automation, and investigations during the Security Log Window.
- 1.8.2 ConnectProtect shall retain system and security event logs generated as part of the MXDR service Solution for a period of 11 (eleven) months from the date of creation ("Retention Period". Following initial processing and analysis, such logs shall be archived in secure cold storage for the remainder of the Retention Period. During this Retention Period, logs shall remain accessible to authorised ConnectProtect personnel solely for the purposes of audit, investigation, or compliance. Upon expiry of the Retention Period, the logs shall be securely deleted or anonymised in accordance with ConnectProtect's data retention and disposal policy.
- 1.8.3 The Customer acknowledges and agrees that all Customer Data, including but not limited to events, logs, alerts, and cases, processed by ConnectProtect as part of the services Solution/s shall be stored and processed within ConnectProtect's designated hosting regions, namely France (FRA1, FRA2), the European Union (EUR1), Monaco (MCO1), and the United Arab Emirates (UAE1), as applicable to the Customer's subscription.

- 1.8.4 Unless otherwise expressly agreed in writing, Customer Data shall remain hosted within the European Economic Area (“EEA”). Any transfer of Customer Data outside the EEA shall be conducted in strict compliance with the requirements of Chapter V of the General Data Protection Regulation (GDPR) and shall rely on appropriate safeguards, including the European Commission’s Standard Contractual Clauses. The Provider shall publish and maintain an up-to-date list of its sub-processors and hosting regions at <https://www.ConnectProtect.com/SubProcessors>.
- 1.8.5 Upon termination of this Agreement, Customer Data shall be returned to the Customer in an industry-standard encrypted format and thereafter securely erased from ConnectProtect’s systems.
- 1.8.6 For the avoidance of doubt, ConnectProtect shall have no liability, whether in contract, tort (including negligence), statute or otherwise, arising from or in connection with: (i) the storage of Customer Data in any designated hosting region set forth above; or (ii) the lawful transfer of Customer Data outside the EEA in accordance with this Agreement and applicable Data Protection Laws.

1.9 Fair usage (asset-based consumption model)

- 1.9.1 Each asset has a quota of 2 GB, 3 GB, or 5 GB per month, depending on the selected plan for the service Solution. Any usage above this constitutes “excessive use”.
- 1.9.2 Data sent to ConnectProtect is monitored continuously to ensure compliance.
- 1.9.3 If a Customer exceeds their quota, ConnectProtect is automatically discharged from liability, including service level penalties and performance issues, during the period of excessive use.
- 1.9.4 If excessive use is deemed illegitimate, prolonged, or repeated, ConnectProtect reserves the right to suspend or terminate services with 30 (thirty) days’ notice. Customers remain fully liable for Fees and no refunds apply.
- 1.9.5 ConnectProtect may apply overage fees for excessive use.
- 1.9.6 Customers are advised to avoid excessive use by upgrading their consumption model (for example from 3 GB to 5 GB per asset).
- 1.9.7 Customers will receive warnings at 80%, 85%, 90%, 95%, and 100% of usage so they can remediate with ConnectProtect’s support.
- 1.9.8 If limits are exceeded, the service enters a downgraded mode and whilst still functional will mean slower detection, storage, and automation, and the service levels will no longer apply.

2 SOC PROVISIONS

2.1 Scope

ConnectProtect shall deliver MXDR service Solution/s through its SOC. The SOC is responsible for continuous monitoring, detection, triage, escalation, and incident response support in accordance with the service Solution/s description. The SOC may access and process Customer Data, including logs, alerts, and case information, solely for the purposes of providing the service Solution/s.

2.2 Data processing and international access

- 2.2.1 the Customer acknowledges and agrees that SOC personnel may access and process Customer Data from facilities located in the Philippines, South Africa, the United Kingdom, and other jurisdictions as reasonably required. Such access and processing are integral to the delivery of the service Solution/s.
- 2.2.2 all access and processing by SOC personnel shall be conducted in full compliance with all applicable data protection and privacy laws, including but not limited to the United Kingdom General Data Protection Regulation (UK GDPR), the European Union General Data Protection Regulation (“EU GDPR”), the California Consumer Privacy Act (CCPA), the South African Protection of Personal Information Act (POPIA), and any other mandatory data protection legislation to which the Customer is subject.
- 2.2.3 ConnectProtect shall implement appropriate legal transfer mechanisms, including Standard Contractual Clauses, the UK International Data Transfer Addendum or International Data Transfer Agreement, or such other lawful mechanisms as may be recognised from time to time.

2.3 Confidentiality and security measures

ConnectProtect warrants that:

- 2.3.1 all SOC personnel are subject to written confidentiality obligations and security policies equivalent to those applied in the UK and EU;
- 2.3.2 access to Customer Data is strictly limited on a least-privilege basis and subject to logging and monitoring;
- 2.3.3 technical and organisational measures, including encryption, access controls, monitoring, and audits, are implemented to ensure the security, integrity, and confidentiality of Customer Data; and
- 2.3.4 international transfers of Customer Data shall not relieve ConnectProtect of its obligations under this Agreement.

2.4 Service levels and escalation

- 2.4.1 the SOC shall operate 24 (twenty-four) hours a day, 7 (seven) days a week.
- 2.4.2 escalation shall be made to Level 2 and Level 3 analysts as appropriate
- 2.4.3 service response times and escalation procedures shall be as described or referenced in this Agreement, unless otherwise set out in a separate service levels agreement entered into amongst the Parties in writing.

2.5 Customer Responsibilities

- 2.5.1 maintain accurate and up-to-date contact information in ConnectProtect's portal to enable timely SOC escalation
- 2.5.2 cooperate fully with SOC personnel in the investigation and resolution of incidents
- 2.5.3 implement in a timely manner any critical recommendations issued by the SOC, or formally accept the associated risk in writing and
- 2.5.4 ensure that necessary access, permissions, and integrations are provided for the SOC to perform its duties.

2.6 Limitations of Liability

Without derogating from any other limitations of liability within this Agreement but in addition to, ConnectProtect shall bear no liability, responsibility, or obligation whatsoever for any breach, incident, loss, damage, or claim arising, directly or indirectly, from:

- 2.6.1 the Customer's failure to implement any critical SOC recommendation;
- 2.6.2 the Customer's failure to maintain accurate contact information, where such failure prevents or delays SOC escalation;
- 2.6.3 the Customer's failure to provide required access or cooperation; or
- 2.6.4 circumstances beyond ConnectProtect's reasonable control, including but not limited to excessive use as defined in the usage policy, to the extent applicable, and for the avoidance of doubt, nothing in this paragraph shall limit or exclude Customer liability for gross negligence, wilful misconduct, or any liability which cannot lawfully be excluded under Applicable Law.

2.7 Audit and Compliance

- 2.7.1 upon reasonable written request, ConnectProtect shall make available to the Customer information necessary to demonstrate compliance with the obligations set forth in this section, which may include relevant certifications, audit reports, or summaries of security measures.
- 2.7.2 the Customer shall not be entitled to conduct direct audits of the SOC facilities unless required by law or a regulator with the authority to do so, and in such case any audit shall be subject to reasonable notice, scope, and confidentiality obligations.