vorboss

Vorboss Limited - Supplier Standard Terms
Managed Security Service (Lot 3 - Cloud Support)

1. Definitions and Interpretation

1.1. Any capitalised terms not defined herein shall have the meaning given to them in the Call-Off Contract.

1.2. In these Supplier Standard Terms, the following terms shall have the following meanings:

"**Buyer Content**" means any software or data, or any text, audio, video, images or other content that the Buyer runs on the Services, causes to interface with the Services, uploads to the Services, or transfers, processes, uses or stores in connection with the Services;

"**Buyer Helpdesk Representative(s)**" means the named individual(s) identified in an Order Form who will be empowered to contact the Helpdesk;

"**Data Processing Agreement**" means the Supplier Data Processing Agreement set out at Appendix 1, as amended by Clause 3.3;

"**Helpdesk**" means the aspect of the Services provided by Supplier to assist the Buyer to troubleshoot and solve issues arising with the Services;

"**Services**" has the meaning set out in the CCS General Terms, but in relation to these Supplier Standard Terms means the Managed Security Service set out in a Call-Off Contract; and

"**Supplier Equipment**" has the meaning set out in the CCS General Terms, but in relation to the delivery of the Services shall primarily mean the materials (e.g. software and other tools) used to provide the Services.

2. Supplier Acceptable Use Policy

2.1. The Buyer shall not use or attempt to use the Services fraudulently or for committing any other illegal or unlawful act.

2.2. Other than as expressly permitted in Supplier Licence Terms or elsewhere in the Call-Off Contract, the Buyer shall not resell or attempt to resell the Services (or any part of facility of them) to any third party.

2.3. The Buyer shall ensure that any Buyer Content and the use of anything provided under a Call-Off Contract by the Buyer, its employees, agents and representatives, will not violate any applicable laws.

2.4. The Buyer shall comply with any acceptable use obligations contained in any applicable EULA (as defined in the Supplier Licence Terms).

3. Supplier Data Processing Agreement

3.1. Where the Supplier is a Processor of Customer Personal Data, the terms of the Data Processing Agreement shall apply.

3.2. The terms "Customer Personal Data" and "Processor" shall be as defined in the Data Processing Agreement.

3.3. Any reference in the Data Processing Agreement to:

(a) "Customer" or "Client" shall be read as a reference to the Buyer (including in relation to "Customer Personal Data", above);

(b) "Vorboss" shall be read as a reference to the Supplier;

(c) "Order" shall be read as a reference to an Order Form; and

(d) "Agreement" shall be read as a reference to a Call-Off Contract.

3.4. The Supplier may act as Controller in respect of certain Personal Data provided by the Buyer to the Supplier. This includes, for example, account information (such as usernames, email addresses and billing information) that the Buyer provides to the Supplier in connection with the creation and administration of the Buyer's account and to allow the Supplier to provide and support the Service. The Data Processing Agreement does not apply in such situations where the Supplier Processes such Personal Data as Controller.

4. Supplier Specific Shared Responsibility Model

4.1. The Buyer acknowledges that certain additional responsibilities of the Buyer, and additional details of the Shared Responsibility Model may be set out in the Supplier Service Description, in addition to those set out below, including under the headings "Customer Responsibilities" and "Technical Requirements and Client-Side Requirements".

4.2. Operating procedures relating to, and availability of, the Helpdesk shall be as set out in an Order Form, Supplier Service Description, or as otherwise communicated to the Buyer, and the Helpdesk shall be contactable via the process notified in writing by the Supplier or as otherwise agreed in the Order Form or Supplier Service Definition.

4.3. Prior to contacting the Helpdesk the Buyer shall: (i) use its reasonable endeavours to troubleshoot and solve any issues that are within its control, including using online guidance and FAQs provided by the Supplier from time to time; and (ii) assemble such information and data about the issue as it is able. Thereafter the Buyer shall respond promptly to Supplier's requests for information and shall provide such other information and assistance as the Supplier may request.

4.4. Unless otherwise specified in an Order Form only the Buyer Helpdesk Representative(s) shall be permitted to contact the Helpdesk.

4.5. The Buyer shall (to the extent required to enable the Supplier to deliver and provide the Services) prepare and make accessible to the Supplier and any of its subcontractors the Buyer Systems, Buyer Equipment and Buyer Premises for delivery, installation, maintenance continuation and configuration of the Services and any Supplier Equipment (which may include onsite and remote activities).

4.6. The Buyer shall be responsible for maintaining security and access, and for procuring all consents, permits, licences and waivers required, to enable the Supplier and any of its subcontractors to carry out activities in Clause 4.5 above.

4.7. The Buyer shall cooperate with Supplier and comply with Supplier's (or any of its sub-contractors') reasonable instructions, requirements, recommendations, advice or specifications in relation to:

(a) the set-up, ongoing configuration and use of the Services including those specified in an Order Form or notified to it from time to time, including in relation to any Supplier Equipment used by the Buyer, and including in relation to the preparation of Buyer Systems, Buyer Equipment and Buyer Premises;

(b) resolving or remediating any cybersecurity issues Supplier identifies as part of the Services (save to the extent Supplier undertakes in an Order Form or Service Change to remediate the same); and

(c) the existence, configuration and maintenance of Buyer Systems required to enable the Buyer to receive or Supplier to provide the Services. The Buyer shall be responsible for compliance of the Buyer Systems with the relevant portions of such recommendations and specifications.

4.8. The Buyer shall be responsible for monitoring communications from Supplier relating to the Services and shall promptly approve (or otherwise) any response actions proposed by Supplier relating to any cybersecurity incident.

4.9. The Buyer shall be responsible for supplying constant space and power for any Buyer Systems, Buyer Equipment, and/or Supplier Systems or Supplier Equipment located at the Buyer Premises, and for any other environmental conditions required for receipt of the Services.

4.10. The Buyer shall be responsible for Buyer Systems, the Buyer's wider IT and network environment, including compliance with 4.5 and 4.7 above.

4.11. The Buyer shall be responsible for any Buyer Content, including providing appropriate security, protection and backup of the Buyer Content, unless expressly stated otherwise in a Call-Off Contract.

4.12. The Supplier will not be responsible for guaranteeing that the Buyer Systems will be free from cybersecurity incidents given the complex and evolving nature of cyber threats.

APPENDIX 1 - DATA PROCESSING AGREEMENT

vorboss

DATA PROCESSING AGREEMENT

This agreement (the "**Data Processing Agreement**") is incorporated in full, where referenced, into each Order or Agreement between Vorboss Limited, a company incorporated in England and Wales (company number 05678571), with Registered Office 10 Exchange Square, London, United Kingdom, EC2A 2BR, United Kingdom ("**Vorboss**") and the counterparty detailed in the Order or Agreement (the "**Customer**") (each a "**Party**" and together "**Parties**"). Capitalised terms not defined in this Data Processing Agreement shall have the meaning set out in the General Terms where applicable.

SCOPE OF THIS DATA PROCESSING AGREEMENT

1.1 A Customer or its end users may provide data to Vorboss under or through the Services ("**Customer Data**"). That Customer Data may include Personal Data ("**Customer Personal Data**").

1.2 This Data Processing Agreement applies to the Processing of Customer Personal Data that is subject to Data Protection Law under any Order or Agreement between the Parties.

1.3 The following definitions shall apply in this Data Processing Agreement:

(A) **Commissioner:** the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018 (as defined below));

(B) **Data Protection Law:** all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) ("**DPA 2018**"); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; the Data (Use and Access) Act 2025; and all other legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of Personal Data (including the privacy of electronic communications); and

(C) **UK GDPR:** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.4 Terms such as "**Process**", "**Processing**", "**Personal Data**", "**Personal Data Breach**" "**Data Subject**", **"Controller**" and "**Processor**" shall have the meaning ascribed to them in the Data Protection Law.

1.5 Vorboss may act as Controller in respect of certain Personal Data provided by Customer to Vorboss. This includes, for example, account information (such as usernames, email addresses and billing information) that Customer provides to Vorboss in connection with the creation and administration of Customer's account. This Data Processing Agreement does not apply where Vorboss Processes such Personal Data as Controller.

1.6 Schedule 1 describes the subject matter, duration, nature and purpose of the Processing and the Personal Data categories and Data Subject types in respect of which Vorboss may Process the Customer Personal Data.

ROLES AND RESPONSIBILITIES

2.1 Customer is the Controller of the Customer Personal Data covered by this Data Processing Agreement. The Customer will determine the scope, purposes and manner by which the Customer Personal Data may be accessed or Processed by Vorboss.

2.2 Customer will:

(A) comply with its obligations as a Controller under Data Protection Law in how it Processes Customer Personal Data and when giving instructions to Vorboss;

(B) provide notice and/or obtain all consents and rights necessary for Vorboss to Process Customer Personal Data under the Order or Agreement and provide the Services, and will ensure it keeps a record of these; and

(C) immediately give notice to Vorboss of any revocation of consent or similar related to Customer Personal Data covered by this Data Processing Agreement.

2.3 Vorboss is the Processor. Vorboss shall only Process Customer Personal Data for the Authorised Purposes (as defined below) and on the documented instructions of Customer, unless Vorboss is required by applicable laws to otherwise Process that Customer Personal Data. Where Vorboss relies on applicable laws as the basis for Processing Customer Personal Data, Vorboss shall notify Customer of this before performing the relevant Processing unless those applicable laws prohibit Vorboss from so notifying Customer on important grounds of public interest.

2.4 Vorboss will Process the Customer Personal Data only for the following purposes ("**Authorised Purposes**"):

(A) to perform Services in accordance with the Order or Agreement;

(B) to perform any of the steps necessary for the Services; and

(C) to comply with any other lawful and reasonable written instructions from Customer that are consistent with the Order or Agreement.

2.5 Where Vorboss is unable to Process Customer Personal Data under clause 2.3 because of a legal obligation (including under Data Protection Law), Vorboss shall inform Customer unless the law prohibits this.

CONFIDENTIALITY

3.1 Without prejudice to the existing contractual confidentiality arrangements between the Parties, Vorboss shall ensure any person authorised by Vorboss to Process Customer Personal Data has signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

SECURITY

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, Vorboss and Customer shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Customer Personal Data appropriate to the risk. These measures shall include as appropriate: (a) the measures referred to in Article 32(1) of the UK GDPR; and (b) the measures further detailed in Schedule 2.

4.2 In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by Processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, Processing, access or disclosure of Customer Personal Data.

4.3 Vorboss will maintain records of its security standards and certifications. Upon Customer's written request, Vorboss will provide (on a confidential basis) copies of relevant external certifications, audit report summaries and/or other documentation as reasonably required by Customer to satisfy it of compliance with this Data Processing Agreement. Vorboss shall in addition provide responses to Customer's reasonable written questions relating to information security as necessary to confirm compliance with this Data Processing Agreement.

4.4 Customer acknowledges that security measures are constantly being improved and Vorboss may update these measures and the related policies, provided that these do not reduce the overall security of Customer's Services.

TRANSFER

5.1 Vorboss will not transfer any Customer Personal Data outside the European Economic Area without Customer's written authorisation.

5.2 Where such consent is granted, Vorboss may only Process, or permit the Processing, of the Customer Personal Data outside the European Economic Area under the following conditions:

(A) Vorboss is Processing the 0Personal Data in a territory which is subject to adequacy regulations under Data Protection Law that the territory provides adequate protection for the privacy rights of individuals; or

(B) Vorboss participates in a valid cross-border transfer mechanism under Data Protection Law, so that Vorboss (and, where appropriate, Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR; or

(C) the transfer otherwise complies with Data Protection Law (for example, where Customer has consented to it or there is a specific exception which applies under Data Protection Law).

5.3 If any Personal Data transfer between Customer and Vorboss requires execution of standard contractual clauses ("**SCCs**") in order to comply with Data Protection Law, the Parties will complete all relevant details in, and execute, the SCCs adopted by the Commissioner (or other relevant supervisory authorities or regulators) from time to time, and take all other actions required to legitimise the transfer.

INCIDENT MANAGEMENT

6.1 Vorboss shall, upon becoming aware of a Personal Data Breach affecting Customer's Services:

(A) without undue delay notify Customer about the Personal Data Breach; and

(B) at all times cooperate with Customer, and shall follow Customer's reasonable instructions relating to the Personal Data Breach, to enable Customer to perform a thorough investigation into the Personal Data Breach, to formulate a correct response, and to take suitable further steps in respect of the Personal Data Breach.

SUB-PROCESSORS

7.1 Customer hereby grants a general authorisation to Vorboss to engage sub-processors from time to time, including: (a) Vorboss Affiliates; and (b) the list of sub-processors which Vorboss maintains at the following URL: https://security.vorboss.com/subprocessors.

7.2 Vorboss will add the names of new and replacement sub-processors to the list referenced at clause 7.1 above prior to them starting sub-processing Personal Data and shall provide a mechanism at such URL for Customer to obtain notice of such changes including any information necessary for the Customer to exercise its right to object. If Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Vorboss of such objections in writing within 10 days of the notification, and the parties will seek to resolve the matter in good faith. If Vorboss requires use of the sub-processor in its discretion and is unable to satisfy Customer as to the suitability of the sub-processor then Customer shall have the right to terminate the relevant portion of the Services affected by the proposed sub-processing, or the Order or Agreement in its entirety, by providing written notice to Vorboss. Such termination shall take effect no earlier than 30 days after the date of Customer's notice of termination.

7.3 Vorboss will ensure that any sub-processor is bound by materially the same data protection obligations contained in this Data Processing Agreement and must, in particular, ensure that the sub-processor meets the requirements of Data Protection Law.

7.4 Even if authorised under clause 7.1, Vorboss shall remain responsible for ensuring that the sub-processor's Processing of Customer Personal Data meets this Data Processing Agreement.

RETURN OR DESTRUCTION OF PERSONAL DATA

8.1 This clause 8 shall apply where Customer Personal Data no longer needs to be Processed by Vorboss because: (a) the Agreements or any Order has been terminated; and/or (b) all purposes for the Processing of Customer Personal Data in relation to the Services have been fulfilled.

8.2 Customer may make a written request for Vorboss to delete, destroy or (at Customer's request) return all Customer Personal Data to Customer and delete, destroy or return any existing copies, unless the law requires storage. Vorboss shall in such cases notify within 25 Business Days that this clause has been complied with.

8.3 Where Customer does not make a request under clause 8.2 within 30 days, Vorboss will delete or destroy all Customer Data in accordance with applicable law. Vorboss will complete this as soon as reasonably practicable and within a maximum period of 180 days, unless the law requires storage.

8.4 Customer shall be responsible for exporting any Customer Data that it wishes to retain before clause 8.1 applies.

ASSISTANCE TO CONTROLLER

9.1 Vorboss shall, taking into account the nature of processing and the information available, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the data subject's rights under Data Protection Law.

9.2 Vorboss shall assist Customer in meeting Customer's compliance obligations under Data Protection Law, taking into account the nature of Vorboss' Processing and the information available to Vorboss, including in relation to security, breach notifications, impact assessments and consultations with the Commissioner (or other relevant supervisory authorities or regulators) under Data Protection Law.

9.3 Vorboss shall make available to Customer all information necessary to demonstrate compliance with Customer's obligations under Data Protection Law and allow for reasonable audits by Customer, or by Customer's designated auditor, for this purpose on reasonable written notice.

DURATION AND TERMINATION

10.1 This Data Processing Agreement shall come into effect on the effective date of the Order or Agreement into which this Data Processing Agreement is incorporated and shall remain in force for the duration of that Order or Agreement.

10.2 Termination or expiry of this Data Processing Agreement shall not discharge Vorboss from its confidentiality obligations under clause 3.

MISCELLANEOUS

11.1 In the event of any inconsistency between this Data Processing Agreement and any other terms in the Order or Agreement in relation to those matters covered by clause 1.2, this Data Processing Agreement shall prevail.

11.2 As set out in the General Terms, the Orders and Agreements shall be governed by and interpreted in accordance with the laws of England, the courts of

England shall have exclusive jurisdiction to settle any disputes (including non-contractual disputes) arising out of or in connection with the Orders and Agreements, and the Parties hereby submit to the exclusive jurisdiction of the English courts.

SCHEDULE 1: SUBJECT MATTER AND DETAILS OF PROCESSING

12.1 **Subject matter**: Vorboss Services provided to Customer, including compute, storage and content delivery on the Vorboss network.

12.2 **Duration of Processing**: As per clause 10.

12.3 **Purpose of Processing**: For the Authorised Purposes (as defined above).

12.4 **Categories of Personal Data**: As per clauses 1.1 and 1.2.

12.5 **Data Subjects**: Data Subjects include individuals about whom Customer Personal Data is provided to Vorboss.

SCHEDULE 2: SECURITY MEASURES

13.1 Vorboss takes security extremely seriously and maintains security policies and procedures that are assessed and regularly audited against ISO 27001 and covering all areas related to Processing Customer Data.

13.2 **Physical Access Control:** All Customer Data storage locations are monitored with CCTV and physical access controlled through a restricted list of named individuals.

13.3 **Data and Administrative Access:** Authentication, credential management, and privilege control systems restrict administrative access to systems to a limited number of authorised personnel.

13.4 Vorboss further has specific policies, within scope of its ISO 27001 certification, addressing the following areas:

(A) **Removable Devices Policy** defining requirements, encryption standards and limitations on use.

(B) **Disposal of Media and Equipment Policy** detailing the process for securely wiping, degaussing and physically destroying (as applicable) media and equipment after use.

(C) **Use of Cryptographic Controls Policy** setting out encryption usage, PKI, and transport encryption.

(D) **Password Policy** governing the generation, strength, storage and rotation of passwords, PINs and cryptographic private keys.

(E) **Backup and Antivirus Policy** dictating the usage of antivirus and anti-malware protection and detailing backup policy.

(F) **Information Security Events, Reporting and Investigation Procedure** detailing the process to be followed upon discovery of any actual or perceived system weaknesses or breaches.

vorboss

Vorboss Limited - Supplier Service Specific Terms
Managed Security Service (Lot 3 - Cloud Support)

1. Definitions and Interpretation

1.1. Any capitalised terms not defined herein shall have the meaning given to them in the Call-Off Contract.

1.2. In these Supplier Service Specific Terms, the following terms shall have the following meanings:

"**EULA**" means the third party end user licence agreement, customer agreement or equivalent document applicable to the Buyer's use of any third party software or services made available to the Buyer pursuant to an Order Form or as set out in the Supplier Licence Terms;

"**Mean Time To Respond**" has the meaning given in Clause 2.3 below; and

"**Services**" has the meaning set out in the CCS General Terms, but in relation to these Supplier Service Specific Terms means the Managed Security Service set out in a Call-Off Contract.

2. Supplier SLA

2.1. Other than to the extent stated otherwise in a Call-Off Contract, the service levels set out below shall be indicative targets only.

Operational Service Levels

Service Area	Coverage	P1	P2	P3	P4
MDR – Core	24x7x365	Mean Time to Respond **15 mins**	Mean Time to Respond **15 mins**	Mean Time to Respond **60 mins**	Mean time to Respond **60 mins**
MDR – Advanced	24x7x365	Mean Time to Respond **15 mins**	Mean Time to Respond **15 mins**	Mean Time to Respond **60 mins**	Mean time to Respond **60 mins**
Vulnerability & Patch Management	Business hours (as agreed)	Critical patching: **2 Working Days**	High patching: **10 Working Days**	Medium patching: **30 days**	N/A

2.2. In relation to Managed Detection & Response (Core) and Managed Detection & Response (Advanced) Services, the Supplier shall use reasonable endeavours to ensure that Mean Time to Respond shall be the same or less than the time set out in the table above.

2.3. The Mean Time to Respond period shall (i) commence immediately upon the detection of a security event by the Supplier's security information and event management (SIEM) system (Microsoft Sentinel), and (ii) cease upon notification being made to the Buyer of the security event in the manner agreed in the relevant Call-Off Contract.

2.4. In relation to Vulnerability and Patch Management, the Supplier operates and scores the criticality of patching on the basis of the Common Vulnerability Scoring System ("**CVSS**"), under which:

(a) a "Critical Patch" shall mean a CVSS score of 9.0 – 10.0;

(b) a "High Patch" shall mean a CVSS score of 7.0 – 8.9; and

(c) a "Medium Patch" shall mean a CVSS score of 4.0 – 6.9.

2.5. The Supplier and the Buyer shall agree appropriate definitions of "P1", "P2", "P3" and "P4" (to reflect the nature of the Buyer's business) in the Order Form or during Buyer onboarding.

3. Supplier Licence Terms

3.1. To the extent that the Buyer requires access to any third party software or services as part of the Services, the Call-off Contract shall state whether such software or services shall be purchased by the Buyer directly from the relevant third party supplier, or by the Supplier on behalf the Buyer.

3.2. If the Supplier provisions software on behalf of the Buyer, such software is licensed (not sold) to the Buyer, and is licensed or sublicensed to the Buyer (on a non-exclusive, non-transferable basis) by the Supplier solely on the terms of and for the purpose set out in the Call-Off Contract (including any EULA referenced below or incorporated into an Order Form). Buyer shall only be entitled to use such software for its internal purpose of receiving the benefit of the Services and shall have no right to sublicense the use of such software other than where expressly set out in the Call-Off Contract or applicable EULA.

3.3. The Buyer acknowledges that the nature of the Services for each Call-Off Contract may differ dependent on third-party restrictions, Buyer Systems or other Buyer requirements ("**Bespoke Requirements**"), and that therefore further additional licences may be required. The Buyer acknowledges that any such Bespoke Requirements do not form part of the Supplier's core Managed Security Service offering and that any additional Supplier Licence Terms or EULAs required to accommodate such Bespoke Requirements shall be contained in an agreed Order Form.

3.4. The following EULAs are generally applicable to the Managed Security Services and form part of the Supplier Licence Terms applicable to any Call-Off Contract, only where stated in the relevant Call-Off Contract:

(a) **Proofpoint** - https://www.proofpoint.com/us/customer-agreement

(b) **Qualys** - https://cdn2.qualys.com/docs/mktg/qualys-master-cloud-services-agreement.pdf

3.5. In relation to Microsoft products, the Buyer acknowledges that it must agree to the Microsoft Customer Agreement located at https://www.microsoft.com/licensing/docs/customeragreement (Geography: United Kingdom; Language: English (UK); Purchase Channel: CSP Partner; Audience: Commercial).