TrustLayer

# Master Services Agreement

**Version:** 1.6

**Issued:** August 2026

# Master Services Agreement

## Operative Provisions:

This Master Services Agreement ("MSA") comprises the following modules*:

**Module A**: General Terms and

**Module B**: Terms for Unified Security Service ("USS") including Web Security ("WS"), Cloud Application Security ("CASB"), MFA powered by Entrust ("MFA"), Compliant Email Archive ("CEA"), Autonomous Security Engine ("ASE"), Posture Management ("SPM") and Security Awareness Training ("SAT").

and

**Module C**: Terms for Email Security ("EMS")

and

**Module D**: Terms for Support Services

and

**Module E:** Service Level Agreement ("SLA")

and

**Module F**: Terms for Managed Services

(*Modules B,C & F may or may not apply depending on the Service(s) purchased)

## Acceptance

By clicking "I ACCEPT" when logging in to the TrustLayer USS Portal: (a) for the first time and following acceptance of an Order by TrustLayer the Customer enters a contract with TrustLayer Limited for the selected Service(s) referred to in the relevant Modules from the Effective Date; and (b) on subsequent logins when there has been an update to the terms of the MSA the Customer accepts the variation to the Contract. All new revisions of the MSA prevail and supersede the terms of any previous versions. By clicking "I ACCEPT" you confirm that you have the requisite authority to act and are authorised by and on behalf of the Customer to enter into this binding Contract.

# Module A: General Terms

## 1. Introduction:

These Terms and Conditions (these "Terms") constitute a binding contract between TrustLayer and the Customer. These Terms, along with any other policies or documents referenced herein, govern the Customer's licensing and use of the relevant Service(s).

Unless expressly stated otherwise, this MSA applies to all Free Trials and NFR Licences. No Subscription Fees or automatic renewal provisions shall apply unless expressly agreed. TrustLayer may suspend, modify or terminate any Free Trial or NFR Licence at any time without liability. Free Trials and NFR Licences are provided on an "as is" and "as available" basis, are not subject to any SLA, service credits or warranties, and may not be used for production purposes unless expressly authorised by TrustLayer.

Subject to your acceptance of these Terms, you may use the Service(s), including the download or install of Software required to deliver the Service(s) subject to the terms of the relevant Modules. If you do not accept these Terms, or the terms of the Modules, you may not use the Service(s) or download, install (or otherwise obtain) Software required to deliver the Service(s). You are deemed to have accepted these Terms, and the terms of the Modules, when you proceed to use the Service(s) or download, install or use Software required to deliver the Service(s).

## 2. Interpretation:

Words defined in these Terms shall apply throughout the MSA, and shall have the following meanings:

| | |
|---|---|
| **Bulk Email Terms & Conditions** | means TrustLayer's Bulk Email Terms and Conditions applicable to EMS, as amended from time to time, made available to the Customer by TrustLayer online via the Product Help Portal https://help.clouduss.com/ems-knowledge-base/bulk-email-terms-and-conditions |
| **Business Day** | a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business. |
| **Change of Control** | shall be as defined in section 1124 of the Corporation Tax Act 2010. |
| **Confidential Information** | means any information disclosed by or on behalf of a party which is confidential by nature or which a reasonable person would understand to be confidential, |

| | |
|---|---|
| | including technical information, software, source and object code, security architecture, vulnerability information, product roadmaps, pricing, commercial information, business plans, customer information, Documentation and the results of any benchmarking or performance testing. |
| **Contract** | this contract between TrustLayer and the Customer, including all the modules. |
| **Customer** | means all customers purchasing Services from TrustLayer (either directly, via a reseller, or other authorized partner) described in the Modules or using our Services or by way of a Free Trial or NFR License. |
| **Customer Data** | the data (including Personal Data) inputted by the Customer, Users, or TrustLayer on the Customer's behalf for the purpose of using the Services or facilitating the Customer's use of the Services. |
| **Data Processing Agreement or "DPA"** | means TrustLayer's Data Processing Agreement, as amended from time to time, made available to Customers by TrustLayer online via its website or provided directly: https://trustlayer.co.uk/legal-policy/ |
| **Data Protection** | and Data Protection Legislation has the meaning given in the DPA. |
| **Documentation** | the documents made available to the Customer by TrustLayer online via https://www.trustlayer.co.uk or such other URL notified by TrustLayer to the Customer from time to time which sets out a description of the Services. |
| **Effective Date** | means the date on which the Customer purchases any Service(s) and/or the date of first use of the Service(s) whichever occurs soonest (excluding trial periods). |
| **Fair Usage Policy** | means TrustLayer's Fair Usage Policy applicable to WS and CASB, as amended from time to time, made available to the Customer by TrustLayer online via the Product Help Portal: https://help.clouduss.com/product-web-security/fair-usage-policy |
| **Free Trial** | a free of charge trial of the USS platform and Services which typically lasts for thirty (30) days. |
| **GDPR** | means (i) the General Data Protection Regulation (EU) 2016/679 ("EU GDPR") or (ii) the General Data Protection Regulation (EU) 2016/679 as applicable as part of United Kingdom domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended |

| | |
|---|---|
| | by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended) ("UK GDPR"), in each case as applicable to the processing of Personal Data. |
| **Intellectual Property Rights** | patents, rights to inventions, copyright and neighbouring and related rights, trademarks and service marks, business names and domain names, rights in get-up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets) and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world. |
| **Mailbox** | a mailbox is the storage location of electronic mail messages found on a remote server or downloaded to the user's device. Email client software typically organise messages into separate folders including inbox and sent items. |
| **Normal Business Hours** | 09:00am to 5:30pm UK-time, each Business Day |
| **Order** | an email, purchase order or other electronic order for one or more of the Services. |
| **Personal Data** | has the meaning set out in our Data Processing Agreement. |
| **Privacy Policy** | means TrustLayer's Privacy Policy, as amended from time to time, made available to Customers by TrustLayer online via its website: https://www.trustlayer.co.uk/privacy-policy/ |
| **Product Usage Policy** | means TrustLayer's Product Usage Policy, as amended from time to time, made available to the Customer by TrustLayer online via the Product Help Portal: https://help.clouduss.com/platform-general/understanding-product-usage |
| **Reseller** | means an authorised reseller of TrustLayer's Services. |
| **Services** | the Service(s) provided by TrustLayer to the Customer on these Terms, to include Email Security (EMS), Web Security (WS), Cloud Application Security (CASB), MFA powered by Entrust (MFA), Compliant Email Archive (CEA), Security Awareness Training (SAT) and Posture Management (SPM), as more particularly described in |

| | |
|---|---|
| | the Documentation. Other Services may be added by TrustLayer at any time. |
| **SLA** | TrustLayer's Service Level Agreement for providing support in relation to the Services contained in Module E. |
| **Software** | means any software forming part of, or included in, Services. |
| **Subscription(s)** | the subscriptions purchased by the Customer which enable the Customer to apply the applicable Service(s) to its Users in accordance with these Terms. |
| **Subscription Fees** | means the fees payable by the Customer to TrustLayer (whether or not through a Reseller) for the applicable Service(s), as notified/invoiced by TrustLayer. |
| **Term** | means the agreed contract length, as set out in the Order, with effect from the Effective Date. |
| **TrustLayer, "us" or "we"** | means TrustLayer Limited (Company No. 09091083), the registered office of which is at Belvedere House, Basing View, Basingstoke, Hampshire, RG21 4HG, United Kingdom. |
| **Users** | those employees, agents and independent contractors of the Customer, who the Customer wishes to be subject to the Services. |
| **Year** | means a 12-month period from the Effective Date. |
| **Virus** | any thing or device (including any software, code, file , program, script or agent) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or otherwise); or adversely affect the user experience. |

In this Contract, clause headings shall not affect its interpretation; a person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality); unless the context otherwise requires, words in the singular shall include the plural and, in the plural, include the singular; a reference to one gender shall include a reference to the other.

**3. The Contract:**

3.1. Any quotation given by TrustLayer shall be valid for thirty (30) calendar days from the date of the quotation (provided we have not previously withdrawn it) unless a different period is stated in writing on the quotation.

3.2. An Order constitutes an offer by you to license the relevant Service(s) in accordance with these Terms. An Order shall be deemed to be accepted by us, and the Contract shall come into existence, on confirmation of the Order to you or on first use of the Service(s) (whichever is soonest).

3.3. In the event of any conflict, the following order shall apply: (a) an Order accepted by TrustLayer, but only where that Order expressly identifies the provision of this MSA that it overrides; (b) the DPA solely in relation to the processing of Personal Data; (c) Module A; (d) the applicable Service Module; (e) the SLA; and (f) any incorporated policies or Documentation.

3.4. Any terms or conditions contained in or referenced by any Customer purchase order, procurement portal, acknowledgement or other Customer document shall have no effect and are expressly rejected, notwithstanding TrustLayer's acceptance or performance of such order.

**4. Use of TrustLayer Services:**

4.1. The Service(s) and Software are licensed to you in accordance with this MSA for internal business use by your organisation and you agree not to use the Service(s) / Software / Documentation for any resale purposes (unless you are a legal and authorised Reseller of our Services pursuant to a Reseller agreement executed between the parties or you are a legal and authorised sub-Reseller of our Services pursuant to a Distribution Agreement executed between us and the Distributor), or to provide any service to any third party (whether or not for reward).

4.2. TrustLayer warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this MSA.

4.3. In relation to Users, you undertake that the maximum number of Users that will be subject to the Service(s) / Software shall not exceed the number of Subscriptions you have purchased from time to time. If you exceed the number of Subscriptions purchased, you agree to pay additional Subscription Fees in respect of the additional Subscriptions / Users. Purchased quantities represent minimum

commitments and may not be reduced during the applicable Term unless expressly agreed by TrustLayer.

4.4. In respect of EMS and CEA, you undertake that the maximum number of Mailboxes that will be subject to the Service(s) / Software shall not exceed the number of Subscriptions you have purchased from time to time. If you exceed the number of Subscriptions purchased you agree to pay additional Subscription Fees in respect of the additional Mailboxes, backdated to the point of over-usage.

4.5. Please note that Disabled Mailboxes are chargeable. If you wish to avoid such charges, you are responsible for converting any Disabled Mailboxes to Shared Mailboxes.

4.6. In the event that a Mailbox is converted to a Shared Mailbox part way through a month you will be invoiced in respect of the entire month. There will be no charge thereafter.

4.7. TrustLayer may periodically verify actual usage against purchased Subscriptions. Where usage exceeds the purchased quantity, TrustLayer may invoice the additional quantity from the date on which the licensed quantity was first exceeded at the applicable contracted unit price or, where no applicable price has been agreed, TrustLayer's then-current price. TrustLayer's system records shall, absent manifest error, constitute the authoritative record of Customer's use of the Services.

4.8. You agree to be bound by the terms of our:

a. Product Usage Policy, as amended from time to time, which can be found at: https://help.clouduss.com/platform-general/understanding-product-usage;
b. Fair Usage Policy, as amended from time to time, which can be found at: https://help.clouduss.com/product-web-security/fair-usage-policy. Our Fair Usage Policy is only applicable to Customers purchasing CASB and WS; and
c. Bulk Email Terms and Conditions, as amended from time to time, which can be found at: https://help.clouduss.com/ems-knowledge-base/bulk-email-terms-and-conditions. Our Bulk Email Terms and Conditions are only applicable to Customers purchasing Email Security, and you acknowledge that TrustLayer will process the Personal Data of individuals at the Customer and their end users in accordance with the terms of our Privacy Policy, as amended from time to time, which can be found at: https://www.trustlayer.co.uk/privacy-policy/
d. Data Processing Agreement, as amended from time to time, which can be found at: https://trustlayer.co.uk/legal-policy/. Our DPA is applicable to all Customers.

4.9. You shall:

a. provide us with:

i. all necessary co-operation in relation to this MSA; and

ii. all necessary access to such information as may be required by us;

in order to provide the Service(s), including but not limited to Customer Data, security access information, and configuration services.

b. comply with all applicable laws and regulations with respect to your activities for which the Service(s) / Software / Documentation are provided; and

c. be responsible for setup and maintenance of accounts and Customer Data to ensure accurate usage reporting.

4.10. We shall be free to enter into similar agreements with third parties, or from independently developing, using, selling, or licensing documentation, products and/or services which are similar to those provided under this MSA.

4.11. The rights provided under this Clause 4 are granted to you only and shall not be considered granted to any subsidiary or holding company of you as the Customer.

**5. Restrictions:**

5.1. Except as expressly authorised under this MSA, or as permitted by any applicable law (which is incapable of exclusion by agreement between the parties), you undertake:

a. not to copy, frame, mirror or republish the Software or Documentation except where such copying is incidental to normal use of the Software nor access the Software in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the Services or to copy any ideas, features, functions or graphics of the Services or the data contained therein;

b. not to rent, sell, lease, sub-license, loan, pledge, translate, merge, transfer, assign, distribute, display, disclose, adapt, vary, modify or otherwise commercially exploit the Software or Documentation;

c. not to make alterations to, or modifications of, the whole or any part of the Software, nor permit the Software or any part of it to be combined with, or become incorporated in, any other programs;

d. not to attempt to circumvent or disable any restriction or entitlement mechanism that is present or embedded in the Software;

e. not to disassemble, decompile, reverse-engineer, create derivative works based on the whole or any part of the Software, nor otherwise attempt to derive any of the Software, source code or Documentation, nor attempt to do any such thing except

to the extent that (by virtue of section 296A of the Copyright, Designs and Patents Act 1988) such actions cannot be prohibited because they are essential for the purpose of achieving inter- operability of the Software with another software program, and provided that the information obtained by you during such activities:

i. is used only for the purpose of achieving inter-operability of the Software with another software program; and

ii. is not unnecessarily disclosed or communicated without our prior written consent to any third party and no passwords or log-in information is shared with third parties (without prior written consent); and

iii. is not used to create any software which is substantially similar to the Software;

f. not to publicly display or publicly perform the Software (without prior written consent);

g. to keep all copies of the Software secure and to maintain accurate and up-to-date records of the number and locations of all copies of the Software;

h. to use all reasonable endeavours to prevent any unauthorised access, or use of, the Software and/or Documentation and in the event of any such unauthorised access or use promptly notify us when you become aware of such unauthorised access or use;

i. to supervise and control use of the Software and ensure that the Software is used by your employees, agents and representatives in accordance with the USS terms (contained in Module B) and EMS terms (contained in Module C);

j. to include our copyright notice on all entire and partial copies you make of the Software on any medium;

k. not to provide or otherwise make available the Software in whole or in part (including but not limited to program listings, object and source program listings, object code and source code), in any form to any person other than your authorised users without prior written consent from us;

l. not to send, access, store, distribute or transmit any Viruses, or any material during the course of your use of the Software and Documents that is: (i) unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; (ii) facilitates illegal activity; (iii) depicts sexually explicit images; (iv) promotes unlawful violence; (v) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; (vi) is otherwise illegal or causes damage or injury to any person or property; or (vii) is morally distasteful, and we reserve the right, without prejudice or liability to our other rights to you, to disable your access to any material that breaches the provisions of this clause;

m. not to violate the privacy rights of any person. Do not collect or disclose any information about an identified or identifiable individual protected under Data Protection Legislation without a lawful basis, (including (where necessary) their consent). Do not co-operate or facilitate identity theft;

n. not to allow or permit access to any computer or communications system without authorization, including the computers used to provide the Services. Do not attempt to penetrate or disable any security system. Do not intentionally distribute a Virus, launch a denial of service attack, or in any other way attempt to interfere with the functioning of any computer, communications system or website. Do not attempt to access or otherwise interfere with the accounts of users of the Service or the Service itself;

o. not to use the Service in any way which may degrade or negatively influence the goodwill or reputation of TrustLayer, customers, partners or any other third party; and to comply with all applicable technology control, applicable laws, rules, export controls, regulations and all Data Protection Legislation.

5.2. We reserve the right to investigate the violation of this clause 5 or misuse of the Services. We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators or other appropriate third parties. Our reporting may include disclosing appropriate Customer and/or User information. We also may co-operate with appropriate law enforcement agencies, regulators or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing same related to alleged violations of the Clause. If you become aware of any violation of this clause, you agree to immediately notify us and provide us with assistance, as requested, to stop or remedy the violation.

**6. Fees and Payment:**

6.1. If the Customer is purchasing the Service(s) through a Reseller or Partner:

6.1.1. All Subscription Fees must be paid by you in accordance with the payment terms in your agreement with the Reseller.

6.1.2. In the event that the Reseller does not pay us the Subscription Fees due in respect of the Service(s) provided to you, we reserve the right to request proof that you have made payment in full to the Reseller in respect of the applicable Subscription Fees.

6.1.3. Failure to provide proof of payment within 14 days after being notified in writing to provide such proof in accordance with clause 6.1.2 above may result in the suspension, or termination, of the Service(s) provided to you.

6.1.4. In the event that we do not have end customer details, and these are not provided by the Reseller within 14 days of our request for them, we reserve the right to suspend, or terminate, the Service(s) provided to you, without any liability.

6.1.5. If you do not pay the Subscription Fees in full in cleared funds to the Reseller by the date specified by us, we reserve the right, by notice to you,

to require payment of the Subscription Fees direct to us immediately and to issue an invoice for such fees, on the basis that you have accepted the terms of this MSA and have thereby entered a Contract with us for the Service(s). In relation to such Contract, the minimum subscription Term will be 12 months from the date of our notice above, the Subscription Fees charged will be payable annually in advance and will be either (a) the Subscription Fees agreed by the Reseller with you or (b) our current retail price for such Services, as decided by us in our absolute discretion. Where this sub-clause applies, sub-clauses 6.2.3 and 6.2.4 will also apply.

6.2. If the Customer is purchasing directly:

6.2.1. Unless otherwise agreed, the Subscription Fees payable by you for the Service(s) shall be the price set out in the quotation and/or our invoice.

6.2.2. Subscription Fees are payable in advance and all invoices must be paid in full within thirty (30) days of the invoice date, free of deduction, set-off or counterclaim. If you are required by any applicable law to withhold any part of any amount payable to us, you shall at the time of payment of our invoice make an additional payment to us equal to the amount of such withholding.

6.2.3. You are responsible for all taxes, charges, levies, assessment and other fees of any kind imposed by governmental or other authority in respect of the purchase or implementation of the Service(s).

6.2.4. If any sum payable to us is not paid by the date on which it is due, then (without prejudice to any other available remedy) interest will accrue on the overdue amount at the statutory rate for the time being in force under the Late Payment of Commercial Debts (Interest) Act 1998 and we reserve the right in our discretion to suspend your rights to use the Service(s) and/or (without prejudice to any claim against the Customer) to terminate the Contract on written notice to the Customer. Where interest on any sum due accrues to us in accordance with this clause, any payment later received will be applied first in payment of the interest due, and secondly in reduction of the indebtedness. If you fail to pay our invoices within our payment terms, we reserve the right to instruct a Debt Collection Agency to recover the sums due and owing from you, together with compensation, the Agency's fees and any other costs and liabilities we have incurred in recovering the debt.

6.3. All invoices rendered in respect of additional Subscription Fees payable for over-usage (in accordance with clauses 4.3 and 4.4 above) will be subject to the same payment terms as detailed above in clauses 6.1 and 6.2 (as applicable).

6.4. Monthly Billing:

6.4.1. Unless otherwise agreed, the Subscription Fees payable by you for the Service(s) shall be the agreed price set out in the agreement and/or our invoice.

6.4.2. Monthly Fees are invoiced in arrears on or near the last day of the month and all invoices must be paid in full within thirty (30) days of the invoice date, free of deduction, set-off or counterclaim. If you are required by any applicable law to withhold any part of any amount payable to us, you shall at the time of payment of our invoice make an additional payment to us equal to the amount of such withholding.

6.4.3. Monthly Fees are based on actual usage for the preceding month and are billed in line with the Product Usage Policy.

6.4.4. Monthly Fees are charged in full for the month of termination.

6.4.5. You are responsible for all taxes, charges, levies, assessment and other fees of any kind imposed by governmental or other authority in respect of the purchase or implementation of the Service(s).

6.4.6. If any sum payable to us is not paid by the date on which it is due, then (without prejudice to any other available remedy) interest will accrue on the overdue amount at the statutory rate for the time being in force under the Late Payment of Commercial Debts (Interest) Act 1998 and we reserve the right in our discretion to suspend your rights to use the Service(s) and/or (without prejudice to any claim against the Customer) to terminate the Contract on written notice to the Customer. Where interest on any sum due accrues to us in accordance with this clause, any payment later received will be applied first in payment of the interest due, and secondly in reduction of the indebtedness. If you fail to pay our invoices within our payment terms, we reserve the right to instruct a Debt Collection Agency to recover the sums due and owing from you, together with compensation, the Agency's fees and any other costs and liabilities we have incurred in recovering the debt.

6.5. The Services are sophisticated software products designed to provide protection against a wide range of security risks. To this end it needs to inter-operate with other systems and products in many different configurations. In certain cases, this inter-operation may not be achieved straightaway, for technical reasons relating to the relevant systems and products or their technical/infrastructure environments. We will use our reasonable endeavours to achieve full inter-operation within a reasonable period. For the avoidance of doubt, all invoices are payable in accordance with these Terms even if the use, or full use, of the Service(s) is delayed whilst we do so.

## 7. Intellectual Property Rights

7.1. All Intellectual Property Rights (IPR) in and to the Service(s) belong, and shall continue to belong to TrustLayer. If you do not pay the Subscription Fees when demanded, without prejudice to our other rights and remedies, you will have no right or licence to use our IPR or Services.

7.2. You shall not do or authorise any third party to do any act which would or might invalidate or be inconsistent with any IPR of TrustLayer and shall not omit or authorise any third party to omit to do any act which, by its omission, would have that effect or character.

7.3. We make no representation or warranty as to the validity or enforceability of the IPR in the Service(s) nor as to whether the same infringe on any IPR of third parties.

7.4. You shall promptly give notice in writing to us in the event that you become aware of any infringement or suspected infringement of any IPR in or relating to the Service(s).

7.5. You acknowledge that you have no right to have access to the Service(s) / Software in source code form.

## 8. Confidentiality

8.1. Each party may be given access to Confidential Information from the other party in order to perform its obligations under this MSA. A party's Confidential Information shall not be deemed to include information that:

a. is or becomes publicly known other than through any act or omission of the receiving party;
b. was in the other party's lawful possession before the disclosure;
c. is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or
d. is independently developed by the receiving party, which independent development can be shown by written evidence.

8.2. Subject to clause 8.4, each party shall hold the other's Confidential Information in confidence and not make the other's Confidential Information available to any third party, nor use the other's Confidential Information for any purpose other than the provision and receipt of the Services.

8.3. A party may disclose Confidential Information to its officers, employees, professional advisers, consultants, investors, sub-contractors and contractors engaged by that party ("Representatives") who need to know such information for the purposes of exercising the party's rights or carrying out its obligations under or in connection with this MSA, on the basis that such party takes all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its Representatives in violation of this MSA, informs its Representatives of the confidential nature of information before it is disclosed, and procures that its Representatives comply with the confidentiality obligations of this Clause 8 as if they were the disclosing party. Each party shall be liable for the actions or omissions of its Representatives in relation to the Confidential Information as if they were the actions or omissions of that party.

8.4. A party may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction, provided that, to the extent it is legally permitted to do so, it gives the other party as much notice of such disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause 8.4, it takes into account the reasonable requests of the other party in relation to the content of such disclosure.

8.5. You acknowledge that details of the Services, and the results of any performance tests of the Services, constitute our Confidential Information.

8.6. We acknowledge that the Customer Data is the Confidential Information of the Customer.

8.7. The receiving party agrees that breach of this clause 8 may cause the disclosing party irreparable injury, for which monetary damages would not provide adequate compensation, and that, in addition to any other remedy, the disclosing party may be entitled to injunctive relief against such breach or threatened breach, without proving actual damage or posting a bond or other security.

8.8. Upon termination of the Agreement, the receiving party will return copies of all Confidential Information to the disclosing party or provide written confirmation of destruction.

8.9. The above provisions of this clause 8 shall survive termination of this Contract for a period of five (5) years thereafter, however arising.

## 9. Protection and processing of Personal Data

9.1. Each party agrees to be bound by, and shall comply with, its obligations under the provisions of our Data Protection Agreement ("DPA") in relation to any Personal Data that it processes under this MSA and the Service(s) provided. The DPA available at https://trustlayer.co.uk/legal-policy/ is incorporated into this Contract by reference as if set out in full herein.

9.2. TrustLayer may use third-party suppliers and infrastructure providers in providing the Services. Except to the extent expressly stated in this MSA or required by the DPA or applicable law, TrustLayer does not warrant and shall not be responsible for third-party products or services outside TrustLayer's reasonable control.

## 10. Limitation of liability and warranties:

10.1. The following provisions set out the entire financial liability of TrustLayer (including any liability for the acts or omissions of its employees, agents, sub-contractors, licensors, suppliers and sub-processors) to you in respect of:

a. any breach of the Contract howsoever arising; and

b. any representation, misrepresentation (whether innocent or negligent) statement or tortious act or omission (including without limitation negligence) or other legal or equitable claim arising under or in connection with the Contract.

10.2. Except as expressly and specifically provided in the Contract, all warranties, conditions and other terms implied by Statute or common law are, to the fullest extent permitted by law, excluded from the Contract. TrustLayer (including any employees, agents, sub-contractors, licensors, suppliers and sub-processors) make no representations, conditions or warranties regarding any third-party software or third-party service (including any third-party cloud service) with which the Services may inter-operate (including, without limitation, by way of an extension or a third-party integration).

10.3. Nothing in the Contract excludes the liability of TrustLayer:

a. for death or personal injury caused by TrustLayer's negligence or the negligence of its personnel, agents or sub-contractors; or

b. for fraud or fraudulent misrepresentation; or

c. any other liability which cannot lawfully be excluded or limited.

10.4. Other than in relation to any liability under clause 10.3, subject to clause 10.5, TrustLayer shall not in any circumstances be liable whether in tort (including for negligence or breach of statutory duty howsoever arising), contract, misrepresentation (whether innocent or negligent) or otherwise for:

a. loss of profits;
b. loss of business;
c. depletion of goodwill or similar losses;
d. loss of anticipated savings;
e. loss of goods;
f. loss of use;
g. loss, inaccuracy or corruption of data or information;
h. cost of procurement of substitute goods or services; or
i. any special, indirect, consequential or pure economic loss, costs, damages, charges or expenses.

10.5. Other than in relation to any liability under Clause 10.3, TrustLayer's total aggregate liability in contract, tort (including without limitation negligence or breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance (or non-performance) of the Contract and the Service(s) provided shall in all circumstances be limited to the Subscription Fees actually paid by you to us under the Contract in the twelve (12) months preceding the date on which the claim arose.

10.6. You acknowledge that the Service(s) and Software have not been developed to meet your individual requirements, and that it is therefore your responsibility to ensure that the facilities and functions of the Service(s)/Software as described by us meet your requirements.

10.7. You acknowledge that we do not warrant that your use of our Service(s) will be uninterrupted or error-free. We are not responsible for any delays, delivery failures, system downtime, failure of security mechanisms, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including email servers and the Internet, and you acknowledge that the Software and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

10.8. We use commercially reasonable measures to prevent any malware or unlawful content getting past our defences, including by using industry standard anti-malware software which is regularly updated, but we cannot guarantee, and do not warrant, that those efforts will be successful in all cases. Customer acknowledges that no cybersecurity service can detect, prevent or remediate all threats and that

the Services may generate false positives or false negatives and may not detect previously unknown, zero-day, obfuscated or otherwise evasive threats.

10.9. We shall have no liability, and you shall indemnify us and hold us harmless, for the consequences of any changes made by you, or by any third party who is not acting on our behalf, to the configuration of the Services / Software including any alteration of the default rules that are pre-set by us.

10.10. To the extent that any Service provides machine-generated, automated or artificial-intelligence-generated classifications, recommendations, summaries or remediation guidance, such outputs may contain errors or omissions and are provided for informational purposes. Customer remains responsible for reviewing outputs and deciding whether and how to act upon them.

10.11. The MSA sets out the full extent of our obligations and liabilities in respect of the supply of the Service(s) / Software / Documentation. Except as expressly stated in this MSA, there are no conditions, warranties, representations or other terms, express or implied, that are binding on us. Any condition, warranty, representation or other term concerning the supply of the Service(s) / Software / Documentation which might otherwise be implied into, or incorporated in, these Terms whether by statute, common law or otherwise, is excluded to the fullest extent permitted by law. The Parties agree that the limitations provided herein are essential and that you would not be permitted to use the Software absent the limitations.

10.12. Except as expressly and specifically provided in this MSA:

a. You assume sole responsibility for results obtained from the use of the Service(s) / Software / Documentation by you, and for conclusions drawn from such use. We shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to us by you in connection with the Service(s) / Software / Documentation, or any actions taken by us at your direction; and

b. the Service(s) / Software / Documentation are provided to you on an “as is” basis.

## 11. Indemnity

11.1. You shall defend, indemnify and hold harmless TrustLayer against claims, actions, proceedings, losses, damages, expenses and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with your use of the Service(s) / Software / Documentation, provided that:

a. we give you prompt notice of any such claim;

b. we provide reasonable co-operation to you in the defence and settlement of such claim, at your expense; and
c. you are given sole authority to defend or settle the claim.

11.2. Customer may not settle any indemnified claim in a manner that admits liability by TrustLayer, imposes obligations on TrustLayer or requires payment by TrustLayer without TrustLayer's prior written consent.

11.3. We shall defend you against any claim made against you that the Service(s) / Software / Documentation infringes any UK patent effective as of the Effective Date or any copyright or UK registered trade mark and shall indemnify you for any amounts awarded against you in judgment or settlement of such claims, provided that:
a. you give us prompt notice of any such claim;
b. you provide reasonable co-operation to us in the defence and settlement of such claim, at our expense; and
c. we are given sole authority to defend or settle the claim.

11.4. In the defence or settlement of any claim, we may procure the right for you to continue using the Service(s), replace or modify the Service(s) so that they become non-infringing or, if such remedies are not reasonably available, terminate the Service(s) on two (2) Business Days' notice to you without any additional liability or obligation to pay liquidated damages or other additional costs to you.

11.5. In no event shall TrustLayer, its employees, agents and sub-contractors be liable to you to the extent that the alleged infringement is based on:
a. a modification of the Service(s) / Software / Documentation by anyone other than us; or
b. your use of the Service(s) / Software / Documentation in a manner contrary to the instructions given to you by us; or
c. your use of the Service(s) / Software / Documentation after notice of the alleged or actual infringement from us or any appropriate authority.

11.6. The foregoing and clause 10 state your sole and exclusive rights and remedies, and our (including our employees', agents' and sub-contractors') entire obligations and liability, for infringement of any patent, copyright, trade mark, database right or right of confidentiality.

11.7. Customer retains all right, title and interest in Customer Data. Customer grants TrustLayer and its authorised subcontractors a worldwide, non-exclusive, royalty-free licence during the Term to host, reproduce, transmit, process and otherwise

use Customer Data solely to the extent necessary to provide, secure, support and administer the Services and otherwise perform TrustLayer's obligations under the Contract, subject always to the DPA in respect of Personal Data. Customer represents and warrants that it has all rights, permissions, authorisations and lawful bases necessary to provide Customer Data to TrustLayer and to instruct TrustLayer to process it in accordance with the Contract.

**12. Term, Renewal, and Termination:**

12.1. The Contract shall start upon the Effective Date and continue for the Term unless and until terminated in accordance with this MSA.

12.2. You agree that, for non-monthly billed customers, we have the right to, automatically and without notice, renew (each for a minimum period of twelve (12) months per renewal) and invoice any Subscription Fees upon expiration of the Term or then current renewal term ("Renewal Term"). The renewal start date will begin upon expiration of the previous Term or Renewal Term, and you will be responsible for the payment of all Subscription Fees to activate the renewal. Subscription Fees will be reviewed from time to time and may be subject to change. You will be notified of any price change within sixty (60) days prior to the expiration of your current term. In the event that you do not accept any price change, and the Parties are not able to reach a mutually agreeable adjustment to the Subscription Fees, you have the right to terminate the Contract upon thirty (30) days prior written notice from the expiration of the current term.

12.3. Unless terminated earlier in accordance with this MSA, the Contract shall continue until terminated by one party giving to the other notice in writing of at least thirty (30) days prior to expiration of the current term when the Contract will auto renew.

12.4. We can terminate the provision of the Service(s) immediately if you: commit a material breach of this MSA and/or become insolvent, cease trading, enter into liquidation or generally become unable to pay your debts within the meaning of Section 123 of the Insolvency Act 1986 or any analogous event occurs in any relevant jurisdiction.

12.5. TrustLayer may suspend all or part of the Services immediately where it reasonably believes that continued provision or use of the Services poses a security risk, may adversely affect TrustLayer, the Services or any other customer, may expose TrustLayer to legal or regulatory liability, is unlawful, breaches this MSA, or where suspension is reasonably necessary to protect the integrity, confidentiality or

availability of the Services. Where reasonably practicable, TrustLayer will notify the Customer of the reason for suspension. TrustLayer shall have no liability arising from a suspension properly made under this clause and, where the circumstances giving rise to suspension are attributable to the Customer, Subscription Fees shall continue to accrue.

12.6. Termination or suspension resulting from Customer's breach shall not relieve Customer of its obligation to pay Subscription Fees committed for the then-current Term, and all outstanding amounts shall become immediately due and payable.

12.7. Upon termination or expiry of the Contract for any reason: (a) the accrued rights of the parties as at termination or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination shall not be affected or prejudiced; and (b) you shall cease to have any right to access or use the Service(s).

12.8. The termination of the Contract shall not of itself give rise to any liability on the part of TrustLayer to pay any compensation to you for loss of profits or goodwill, to reimburse you for any costs relating to or resulting from such termination, or for any other loss or damage.

12.9. On termination of the Contract for any reason:

12.9.1. all rights granted under this MSA shall immediately terminate and you shall immediately cease all use of the Service(s), Software and/or any Documentation upon expiry of the current Term paid for;

12.9.2. each party shall return and make no further use of any equipment, property, Documentation and other items (and all copies of them) belonging to the other party;

12.9.3. Personal Data shall be returned or deleted following termination in accordance with the DPA. In relation to any other Customer Data, TrustLayer may delete such Customer Data following termination in accordance with its applicable data retention procedures unless the Customer has requested its return before deletion; and

12.9.4. any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this MSA which existed at or before the date of termination shall not be affected or prejudiced.

**13. Product End of Life:**

13.1. We reserve the right to discontinue or terminate any Service, or part of a Service, at any time by providing sixty (60) days' notice to you in writing (unless you are in material breach of the terms of this agreement whereupon we can terminate the Service with immediate effect).

13.2. The notice will provide details regarding the end-of-life process, access/use of the affected Service(s) during the notice period and any options for data migration.

13.3. We will make reasonable efforts to allow you to migrate your data to an alternative Service or provider during the notice period. It is your responsibility to ensure any data you wish to migrate is transferred before the termination date. After the end-of-life date, access may not be possible and any data not migrated may be deleted or otherwise disposed of in accordance with our data retention policy.

13.4. In the event of ending a Service, we will not be liable for any loss or damages incurred by you (in accordance with Clause 10 above). Your exclusive remedy will be limited to the refund of any pre-paid fees in respect of the terminated Service only, pro-rated for the period it was available. Please note that you have no right to terminate any other Service(s) purchased by you and any such Service(s) will continue for the remainder of your Term and will continue/renew in accordance with the terms of this Agreement.

13.5. TrustLayer may modify, enhance or replace elements of the Services from time to time, including underlying technologies and suppliers, provided that during a paid Term TrustLayer will not materially reduce the overall core functionality of a purchased Service except where reasonably necessary for security, legal or regulatory reasons or because an applicable third-party dependency is no longer reasonably available.

**14. Support:**

Standard Support will be provided to you by the Reseller, not us, unless approved in advance on a case-by-case basis. Additional chargeable support services may be delivered to you directly by us. Please see Module D for the Terms of our Support Services.

**15. Entire Agreement:**

This Contract constitutes the entire agreement between the parties concerning its subject matter and supersedes and extinguishes any previous understanding, promises, assurances, warranties, representations or agreement, express or implied, and prevails over any drafts, memoranda, letters or other communications. Each party confirms that it has not relied upon any representation or collateral warranty not recorded in this MSA inducing it to enter into the Contract.

**16. Assignment:**

16.1. You shall not, without our prior written consent, assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under the Contract.

16.2. We may at any time assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under the Contract.

**17. No partnership or agency:**

17.1. Nothing in the Contract is intended to, or shall be deemed to, establish any partnership or joint venture between the parties, constitute either party the agent of the other party, nor authorise either party to make or enter into any commitments for or on behalf of the other party except as expressly provided in the MSA.

17.2. Each party confirms it is acting on its own behalf and not for the benefit of any other person.

**18. Force majeure:**

Neither party shall in any circumstances be in breach of the MSA nor liable for delay in performing, or failure to perform, any of its obligations under the MSA if such delay or failure results from events, circumstances or causes beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes, failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors. In such circumstances the affected party shall be entitled to a reasonable extension of the time for performing such obligations.

**19. Variation:**

TrustLayer may update the MSA from time to time. Material changes will be notified to the Customer before they become effective. Continued use following the effective date constitutes acceptance, except where the parties have expressly agreed in an Order or other signed agreement that amendments require mutual written agreement.

**20. Severability:**

If any term or condition of this MSA is held void or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision shall be deemed deleted. Any modification to or deletion of a provision, or part provision, under this clause shall not affect the validity and enforceability of the rest of this MSA.

**21. Notices:**

Any notice given under the MSA shall be in writing and shall be delivered by hand or by commercial courier or by Royal Mail special delivery posted in the United Kingdom or by email. In the case of hand delivery, commercial courier or Royal Mail special delivery, delivery shall be deemed to take place on actual delivery (or on receipt by the sender of a notice that the addressee has "gone away" or refused to take delivery or any notice having similar effect). In respect of ordinary Royal Mail delivery, delivery shall be deemed to take place on the second Business Day after posting or at the time recorded by the delivery service. Email notices shall take effect on transmission (provided a non-delivery message is not generated) or, if this time falls outside Normal Business Hours, when business hours resume. Notices shall be delivered or posted to the addresses of the parties given above, email addresses appearing on a party's website or letter heading, or to any other United Kingdom address or email address notified in substitution on or after the Effective Date.

**22. Third Parties:**

A person who is not party to this MSA shall have no right to enforce any of its terms under the Contracts (Rights of Third Parties) Act 1999.

**23. Governing Law:**

This MSA and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) are governed by and construed in accordance with the laws of England and Wales.

**24. Jurisdiction:**

The parties irrevocably agree that the courts of England have exclusive jurisdiction to settle any disputes or claims arising out of or in connection with the MSA, the Contract, its subject matter or its formation (including non-contractual disputes or claims).

# Module B – Terms for Unified Security Service (USS) including Web Security (WS), Cloud Application Security (CASB), MFA powered by Entrust (MFA), Compliant Email Archive (CEA), Security Posture Management (SPM), Autonomous Security Engine (ASE) and Security Awareness Training (SAT)

PLEASE READ CAREFULLY BEFORE ORDERING SERVICE(S) or DOWNLOADING ANY SOFTWARE:

These terms ("USS Licence Terms") apply to the use of our Unified Security Service software that you are buying from us ("USS Software"); and any associated Documentation.

We license use of the USS Software and Documentation to you on the basis of these USS Licence Terms. We do not sell the Software or Documentation to you. We remain the owners of the Software and Documentation at all times.

IMPORTANT NOTICES:

BY CLICKING ON THE "ACCEPT" BUTTON OR BY USING THE USS SOFTWARE YOU AGREE TO THESE USS LICENCE TERMS. THE USS LICENCE TERMS INCLUDE, IN PARTICULAR, LIMITATIONS ON LIABILITY IN MODULE A CLAUSE 10.

IF YOU DO NOT AGREE TO THE USS LICENCE TERMS, BY EXPRESS OR IMPLIED ACCEPTANCE, WE WILL NOT LICENSE THE USS SOFTWARE AND DOCUMENTATION TO YOU AND YOU MUST DISCONTINUE THE ORDERING PROCESS.

THE PERSON WHO CLICKS ON THE "ACCEPT" BUTTON OR USES THE USS SOFTWARE IS EITHER ENTERING INTO THE USS TERMS WITH US ON THEIR OWN BEHALF OR ON BEHALF OF ANOTHER PERSON. IF ON BEHALF OF ANOTHER PERSON, THEY WARRANT THAT THEY HAVE BEEN DULY AUTHORISED TO DO SO.

THE USS LICENCE TERMS WILL APPLY TO YOUR USE OF THE USS SOFTWARE AND THE DOCUMENTATION IN ALL LICENSING OF THE USS SOFTWARE INCLUDING:

- THE ELEMENTS OF THE USS SOFTWARE THAT ARE HOSTED BY US
- THE ELEMENTS OF THE USS SOFTWARE THAT MAY BE INSTALLED ON ANY USER'S LAPTOP OR OTHER DEVICE
- THE ELEMENTS OF THE USS SOFTWARE THAT MAY BE INSTALLED AS A GATEWAY ON THE LICENSEE'S NETWORK

PLEASE NOTE THAT THE USS SOFTWARE IS A PRODUCT DESIGNED TO PROVIDE YOU WITH A PLATFORM INCORPORATING MULTIPLE SECURITY SERVICES. IT INCLUDES MEASURES THAT CAN INTERCEPT AND PREVENT DATA TRANSMISSIONS. THE CUSTOMER ACKNOWLEDGES THAT OPERATION OF THE SERVICES MAY REQUIRE TRUSTLAYER TO INSPECT, ANALYSE, INTERCEPT, BLOCK OR OTHERWISE PROCESS NETWORK, WEB, CLOUD APPLICATION OR EMAIL COMMUNICATIONS IN ACCORDANCE WITH CUSTOMER-CONFIGURED POLICIES. THE CUSTOMER AUTHORISES TRUSTLAYER TO UNDERTAKE SUCH ACTIVITIES TO THE EXTENT NECESSARY TO PROVIDE THE SERVICES AND REPRESENTS AND WARRANTS THAT IT HAS ALL RIGHTS, PERMISSIONS AND AUTHORISATIONS NECESSARY TO GIVE SUCH INSTRUCTION AND AUTHORISATION. BY ENTERING INTO THIS MSA OR BY USING THE USS SOFTWARE, AND SO ACCEPTING THE TERMS OF THIS MODULE, YOU GIVE THIS CONSENT.

IN ORDER TO OPTIMISE OUR SERVICE TO YOU, WE ALSO SHARE ANONYMIZED TELEMETRY INFORMATION (INCLUDING BUT NOT LIMITED TO DETECTION NAMES, FILE HASHES AND DEVICE CONTENT AND UNIQUE RANDOM ID DEVICES), BOTH IN REAL TIME AND PERIODICALLY, WITH OUR SERVICE PROVIDERS.

PLEASE NOTE THAT THE USS SOFTWARE ALLOWS THE ACTIVITIES OF EMPLOYEES AND OTHER USERS TO BE MONITORED. IN SOME JURISDICTIONS THIS MAY BE UNLAWFUL, OR MAY BE UNLAWFUL WITHOUT CONSENT. YOU ARE RESPONSIBLE FOR ENSURING THAT ALL SUCH MONITORING IS LAWFUL IN THE JURISDICTION(S) IN WHICH YOU USE IT.

IN ORDER TO FACILITATE ACCESS TO AND USE OF THE USS SOFTWARE, WE PROVIDE DEFAULT LISTS OF CATEGORIES (“CATEGORIES”). CATEGORIES ARE PROVIDED SOLELY FOR YOUR USE AND WE DO NOT APPROVE OR ENDORSE ANY CONTENT ACCESSED THROUGH ANY CATEGORIES. WE EXPRESSLY DISCLAIM ANY LIABILITY ARISING FROM OR RELATING TO THE USE OF CATEGORIES BY YOU.

**1. Grant of scope and license:**

1.1. In consideration of payment by you of the Subscription Fees and you agreeing to abide by the USS Licence Terms, we grant to you a non-exclusive, non-transferable licence to use the USS Software and the Documentation for the Term.

1.2. You may:

a. download and install the non-hosted components of our USS Software and use such components for your internal business purposes only and only by the number of Users agreed between you and us, or between you and a Reseller, and in respect of whom you have paid Subscription Fees;

b. use the hosted components of the USS Software via the Internet, again for your internal business purposes only and only by the number of Users agreed between you and us, or between you and a Reseller, and in respect of whom you have paid the Subscription Fees;

c. provided you comply with the restrictions in Module A clause 5, make one copy of the non- hosted USS Software components for back-up purposes only.

**2. Limited warranty:**

2.1. We warrant that:

a. the USS Software will, when properly used and on an operating system for which it is designed, perform substantially in accordance with its description on the TrustLayer website ("the Description"); and

b. that the Description correctly describes the operation of the USS Software in all material respects, for a period of thirty (30) days from the date of your first use of the USS Software ("Warranty Period").

2.2. If within the Warranty Period, you notify us in writing of any defect or fault in the USS Software as a result of which it fails to perform substantially in accordance with the Documentation, we will, at our sole option, either repair or replace the USS Software, provided that you make available all the information that may be necessary to help us to remedy the defect or fault, including sufficient information to enable us to recreate the defect or fault. Such correction or substitution constitutes your sole and exclusive remedy for any breach of the warranties set out in Clause 2.1.

2.3. The warranty does not apply:

a. if the defect or fault in the USS Software results from you, or any party other than us or our duly authorised contractors and agents, having altered or modified the USS Software;

b. if the defect or fault is caused by use of the USS Software contrary to our instructions; or

c. if the defect or fault in the USS Software results from you having used the USS Software in breach of the terms of this USS Licence.

2.4. We do not warrant that your use of the USS Software will be uninterrupted or error-free.

2.5. We are not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including email servers and the internet, and you acknowledge that the USS Software and/or Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

**3. Fair Usage – Web and CASB**

3.1. Web Security and CASB (inline mode) are licensed by number of users.

3.2. Below, the following terms are used:

a. Distinct user log entries: Number of unique usernames seen in log entries during a month.

b. Distinct device log entries: Number of unique MAC addresses seen in log entries without usernames during a month.

c. Distinct re-occurring device log entries: The subset of the unique MAC addresses that have been logged on at least 3 different days during a month.

d. Distinct guest device log entries: The subset of the unique MAC addresses that have been logged on up to 2 different days during a month.

3.3. Fixed policy

The number of distinct usernames must not exceed the number of purchased licenses during a month.

3.4. Fair usage policy 1:

a. The number of distinct re-occurring device log entries during a month must not add up to more than twice the number of licenses purchased.

b. This means that 1) On average, each user is allowed to have 2 devices using the service, and 2) Guest devices logging in at most twice during a month will not contribute to the calculation.

3.5. Fair usage policy 2 (“Guest logins”):
The number of distinct guest device log entries during a month must not add up to more than 5 times the number of licenses purchased. This means that on average, every license allows for 5 monthly guests.

# Module C – Terms for Email Security (EMS)

PLEASE READ CAREFULLY BEFORE ORDERING SERVICE(S) or DOWNLOADING ANY SOFTWARE:

These terms ("EMS Terms") apply to the use of our EMS software that you are buying from us ("EMS Software"); and any associated Documentation.

IMPORTANT NOTICES:
BY CLICKING ON THE "ACCEPT" BUTTON OR BY USING THE EMS SOFTWARE, YOU AGREE TO THESE EMS TERMS. THE EMS TERMS INCLUDE, IN PARTICULAR, LIMITATIONS ON LIABILITY IN MODULE A CLAUSE 10.

IF YOU DO NOT AGREE TO THESE EMS TERMS, BY EXPRESS OR IMPLIED ACCEPTANCE, WE WILL NOT LICENSE THE EMS SOFTWARE AND DOCUMENTATION TO YOU AND YOU MUST DISCONTINUE THE ORDERING PROCESS.

THE PERSON WHO CLICKS ON THE "ACCEPT" BUTTON OR USES THE EMS SOFTWARE IS EITHER ENTERING INTO THIS LICENSE WITH US ON THEIR OWN BEHALF OR ON BEHALF OF ANOTHER PERSON. IF ON BEHALF OF ANOTHER PERSON, THEY WARRANT THAT THEY HAVE BEEN DULY AUTHORISED TO DO SO.

PLEASE NOTE THAT THE EMS SOFTWARE IS A PRODUCT DESIGNED TO PROVIDE YOU WITH EMAIL SECURITY. IT INCLUDES MEASURES THAT CAN INTERCEPT AND PREVENT EMAIL AND DATA TRANSMISSIONS. THE CUSTOMER ACKNOWLEDGES THAT OPERATION OF THE SERVICES MAY REQUIRE TRUSTLAYER TO INSPECT, ANALYSE, INTERCEPT, BLOCK OR OTHERWISE PROCESS CUSTOMER EMAIL COMMUNICATIONS IN ACCORDANCE WITH CUSTOMER-CONFIGURED POLICIES. THE CUSTOMER AUTHORISES TRUSTLAYER TO UNDERTAKE SUCH ACTIVITIES TO THE EXTENT NECESSARY TO PROVIDE THE SERVICES AND REPRESENTS AND WARRANTS THAT IT HAS ALL RIGHTS, PERMISSIONS AND AUTHORISATIONS NECESSARY TO GIVE SUCH INSTRUCTION AND AUTHORISATION. BY CLICKING ON THE "ACCEPT" BUTTON OR BY USING THE EMS SOFTWARE AND SO ACCEPTING THE TERMS OF THIS MODULE, YOU GIVE THIS CONSENT.

IN ORDER TO OPTIMISE OUR SERVICE TO YOU, WE ALSO SHARE ANONYMIZED TELEMETRY INFORMATION (INCLUDING BUT NOT LIMITED TO DETECTION NAMES, FILE HASHES AND DEVICE CONTENT AND UNIQUE RANDOM ID DEVICES), BOTH IN REAL TIME AND PERIODICALLY, WITH OUR SERVICE PROVIDERS.

PLEASE NOTE THAT THE EMS SOFTWARE ALLOWS THE ACTIVITIES OF EMPLOYEES AND OTHER USERS TO BE MONITORED. IN SOME JURISDICTIONS THIS MAY BE UNLAWFUL, OR MAY BE UNLAWFUL WITHOUT CONSENT. YOU ARE RESPONSIBLE FOR ENSURING THAT ALL SUCH MONITORING IS LAWFUL IN THE JURISDICTION(S) IN WHICH YOU USE IT.

## 1. Grant of scope and Use:

1.1. In consideration of payment of the Subscription Fees and your compliance with these EMS Terms, we grant you a non-exclusive, non-transferable right during the Term to access and use the Email Security Service and associated Documentation for your internal business purposes, subject to the number of licensed Mailboxes and any other quantities specified in the applicable Order.

1.2. The EMS protects only email messages that are routed through, submitted to, or otherwise made available to the EMS using a supported configuration, including applicable MX records, mail connectors, APIs or other delivery methods described in the Documentation.

1.3. You are responsible for ensuring that your email systems and domains are correctly configured to route applicable email through the EMS and for maintaining all third-party permissions, connectors, credentials and configuration required for the EMS to operate.

## 2. Customer Configuration and Responsibilities

2.1. You are responsible for the configuration and operation of your email environment, including your domains, DNS records, mail servers, identity services and supported third-party email platforms.

2.2. You shall ensure that all information and configuration supplied to TrustLayer is accurate and kept up to date.

2.3. You remain responsible for rules, policies, safe lists, deny lists, exemptions, bypasses and other settings configured by you or on your behalf.

2.4. TrustLayer shall not be responsible for email which bypasses the EMS because of Customer configuration, third-party configuration, direct delivery or another route that does not pass through the EMS.

2.5. Where an EMS feature depends upon a third-party platform, API, connector or permission, you are responsible for obtaining and maintaining all rights, licences, permissions and access required for that integration.

## 3. Email Filtering and Quarantine

3.1. The EMS may inspect, analyse, classify, block, reject, quarantine, redirect or otherwise process email in accordance with Customer-configured policies, TrustLayer security controls and the functionality described in the Documentation.

3.2. You acknowledge that email-security classifications are automated and may result in false positives or false negatives. No email-security service can identify or prevent every malicious, unwanted or fraudulent message.

3.3. Where you release, allow, safe-list or otherwise permit delivery of an email or sender which the EMS has identified as potentially malicious, unwanted or suspicious, you accept responsibility for the consequences of that decision.

3.4. Quarantine and other EMS data shall be retained in accordance with the Documentation and DPA.

## 4. Email Delivery and Third-Party Services

4.1. TrustLayer will use commercially reasonable efforts to receive, process and deliver email submitted to the EMS, subject to the applicable SLA.

4.2. TrustLayer does not warrant that any particular email will be accepted or delivered by a recipient, recipient mail server or third-party email provider.

4.3. TrustLayer shall not be responsible for delays, rejection, non-delivery or other failures caused by circumstances outside its reasonable control, including:

a. Customer mail servers or configuration;
b. recipient mail servers or recipient policies;
c. DNS or domain configuration;
d. internet or telecommunications failures;
e. Microsoft, Google or other third-party email platforms;
f. third-party blocklists, reputation systems or filtering services;
g. invalid or unavailable recipient addresses; or
h. security policies or technical controls operated by third parties.

## 5. Outbound Email, Bulk Email and Service Protection

5.1. Use of the EMS for outbound email is subject to the Bulk Email Terms and Conditions incorporated into this MSA under Module A.

5.2. The EMS is not intended to operate as an unrestricted bulk email, marketing automation or high-volume mail delivery platform unless expressly agreed with TrustLayer.

5.3. TrustLayer may impose or modify reasonable sending limits, connection limits, message-size limits, recipient limits or other technical controls applicable to outbound email in accordance with the Bulk Email Terms, Documentation or applicable Order.

5.4. Where TrustLayer reasonably considers that Customer email traffic:

a. materially exceeds agreed or normal usage levels;
b. causes or risks causing material queueing, delay or degradation of the EMS;
c. adversely affects or risks adversely affecting another customer;
d. threatens the reputation or deliverability of TrustLayer infrastructure, sending IP addresses or the EMS;
e. results in material abuse or spam complaints;
f. creates a security risk; or
g. breaches the Bulk Email Terms or this MSA,

TrustLayer may rate-limit, throttle, defer, reroute, reject or block email traffic, including traffic from particular Mailboxes, senders or domains, or temporarily suspend outbound email processing to the extent reasonably necessary to protect the EMS.

5.5. TrustLayer may take action under clause 5.4 without prior notice where immediate action is reasonably necessary to protect the security, availability, integrity or reputation of the EMS or other customers. Where reasonably practicable, TrustLayer will notify you promptly of the action taken and the reason for it.

5.6. You shall not use, or permit the use of, the EMS in a manner that is reasonably likely to cause TrustLayer infrastructure, IP addresses, domains or services to be blocklisted, materially damage their sending reputation, or otherwise interfere with the ability of TrustLayer to provide email services to other customers.

## 6. Limited Service Warranty

6.1. TrustLayer warrants that, when correctly configured and used substantially in accordance with the Documentation, the EMS will perform in all material respects substantially in accordance with the Documentation.

6.2. If you notify TrustLayer of a material non-conformity, TrustLayer will use reasonable endeavours, at its option, to correct the non-conformity, provide a reasonable workaround or re-perform the affected element of the Service.

6.3. Clause 7.1 does not apply to any failure caused by:

a. Customer configuration or Customer systems;
b. use contrary to the Documentation;
c. a third-party system or service outside TrustLayer's reasonable control;
d. unsupported configurations; or
e. matters expressly excluded under Module A or Module E.

6.4. The remedies in this clause are subject to Module A clause 10 and do not create any Service Credit entitlement beyond Module E.

# Module D – Terms for Support Services

## 1. Standard Support (Level 1):

1.1. Standard Support (Level 1 Support) is provided online via the TrustLayer website. Online Customer support for TrustLayer services is available Monday to Friday, 9.00 am to 5.00pm UK time ("Standard Support Hours").

1.2. You can open a support ticket at: https://www.TrustLayer.co.uk/support/ . You will receive a case number by email which you can use to track the progress of your issue through to resolution.

1.3. Full details, and a Knowledge Base, are available at: www.TrustLayer.co.uk/support/

## 2. Extended Support Levels:

2.1. Level 2 Support

Level 2 Support is available Monday to Friday, 8.00am to 5.00pm UK time.
In addition to Online Support, Live Chat via the TrustLayer website is also available to customers that purchase Level 2 Support. Simply click the "Chat Now" button to connect to one of our technical support engineers.

Level 2 Support also includes telephone support Monday to Friday, 8.00am to 5.00pm UK time. To contact our Support Team please call:

From UK: 0845 230 9590 (select option 2)
Outside UK: +44 (0)845 230 9590 (select option 2)

2.2. Level 3 Support

Level 3 Support includes 24x7 telephone support. Customers that purchase Level 3 support have 24-hour access to our technical support engineers. Outside Level 2 telephone support hours customers should call the 24x7 telephone number provided when Level 3 Support was purchased.

## 3. Out-of-Hours Emergency Support

Level 1 and Level 2 Support customers can send an emergency email to support@trustlayer.co.uk outside of Standard Support Hours and someone will contact you as soon as possible. Please note, this service is restricted to Priority 1 Issues only which relate to a production outage with no reasonable workaround. Normal support channels should be used for non-critical requests.

## 4. Issue Levels

The following table provides a description of the different issue categories, based on their severity and impact, that TrustLayer uses to assign a priority to individual support cases.

| Category | Description |
|---|---|
| Priority 1 (Critical) | Infrastructure outage, service disruption, system not available and no workaround exists. |
| Priority 2 (Degraded) | The service is usable but degraded. Significant reduction experienced in system performance or unavailability of a specific function. Failure of one or more system functions making use of the systems difficult (e.g. service still running and operational, but not at full capacity). |
| Priority 3 (General) | A problem, which is outside of the expected operation of the service but causes only minor inconvenience to the customer, requests for information, service requests or feature requests. |

## 5. Response Times

TrustLayer will use commercially reasonable efforts to respond within the timescales below following the submission of a support request.

| Severity Level | Standard Support Target Response* |
|---|---|
| Priority 1 (Critical) | < 4 Business Hours (Email only) |
| Priority 2 (Degraded) | < 6 Business Hours (Email only) |
| Priority 3 (General) | Next Business Day (Email only) |

* 8AM to 12AM Monday to Friday

5.1. Please note that the Customer is responsible for notifying TrustLayer Support as soon as possible in the event of a critical or high service issue.

5.2. The USS platform status can be viewed by visiting https://status.clouduss.com which also offers the facility to subscribe to alerts and notifications. The page also details any scheduled maintenance which may affect the platform.

5.3. Response times are targets, not guaranteed resolution times.

# Module E – Service Level Agreement (SLA)

## 1. Introduction:

1.1. We are committed to providing top quality service levels in respect of all TrustLayer Services, to all Customers.

1.2. This service level agreement ("SLA") defines the framework for measuring the service levels offered to Customers and what they can expect from TrustLayer in respect of the reliability of the Service(s) provided, and our response times. Appendix 1 to 3 form part of this SLA and shall have effect as if set out in full in the body of this SLA. Any reference to this SLA includes Appendices 1 to 3.

1.3. This SLA only applies to Customers (defined as end users) and does not apply to any third parties including resellers or distributors.

## 2. Related Documents:

2.1. This SLA is subject to the Terms of the MSA and the applicable Modules, together with the current privacy policy which can be found at https://trustlayer.co.uk/privacy-policy

## 3. Eligibility:

3.1. Customers who subscribe to our Service(s) are subject to this SLA. This SLA only applies to Customers who have active accounts.

3.2 This SLA does not apply:

a. to trial or evaluation Customers;
b. where you have used the cloud service for a period of thirty (30) days or less;
c. where you are not up to date on payment of your Subscription Fees for the Service(s) at the time of a Claimed Outage;
d. where you have not paid your Subscription Fees for the Service(s) when due two (2) or more times in the previous twelve (12) calendar months;
e. where you have failed to report the unavailability in accordance with the procedure detailed below;
f. where the cloud service is incorrectly configured by you;
g. where you provide incorrect or inaccurate information to us;

h. where your applications, equipment or internet connection has failed;
i. where the Service(s) are not available due to system administration, commands or file transfers performed by you;
j. where you are misusing the Service(s) or are otherwise in violation of the MSA;
k. where there are problems with your, or a third party's, hardware or software, or problems caused by third parties who gain access to the cloud services using your accounts or equipment;
l. where there is a network unavailability outside of our controlled systems (servers, hardware, and associated software) that are responsible for delivering the cloud service;
m. where there are problems with your routing infrastructure (eg identity provider or secure web proxy of a third party);
n. for hosted email security, where an account is not configured to use two or more co-location sites (clusters);
o. where you have acted as an open relay or open proxy, or have been using the Service(s) to send spam or viruses, or are otherwise misusing the Service(s);
p. where the failure of meeting the terms of this SLA is based upon reasons beyond our reasonable control;
q. where there has been a violation by you, your personnel or anyone engaged by you of the Computer Misuse Act; or
r. when we are performing scheduled or routine maintenance of the Service(s), where you have been notified of the maintenance no less than five (5) Business Days in advance, or as otherwise set out below.

3.3 Please note that the administration portals are excluded from this SLA, and are not considered part of the core functionality of the Service(s).

**4. Service Details:**

4.1. The Services covered under this SLA are listed below:

a. Email Security Service ("EMS")
b. Web Security Service ("WS")
c. Cloud Application Security ("CASB")
d. Security Posture Management ("SPM")

Known all together as "the Services"

4.2. Scheduled downtime: If downtime is scheduled, for example for routine planned maintenance, then notices will be emailed to the technical contact configured in the account profile, at least five (5) Business Days in advance.

**5. Service Standards:**

The service availability for the Services listed in clause 4.1 above is 99% (unless otherwise stated in the appendices to this MSA).

**6. Service Credits:**

6.1. The following terms and definitions are used:

a. "Claimed Outage" means the period, measured in minutes, during which you claim a loss of service and/or the level of performance has failed to meet the monthly uptime commitment.
b. "Excluded Minutes" means the period of any outage that is attributed to one or more of the SLA Credit Exclusions (detailed in clause 3.2 and 3.3) during a Measurement Period.
c. "Measurement Period" means the month in which the Claimed Outage occurred.
d. "Verified Outage" means a Claimed Outage for a service that has been verified by us.

6.2. In the event of Service Unavailability, where we do not meet the monthly uptime percentage commitments for any calendar month detailed in clause 5 and the relevant appendices to this MSA, you will be eligible to receive Service Credits calculated and applied as follows:

6.2.1. following a claim submitted by you in accordance with clause 7 below, where we have verified the claim, we will credit your account with one (1) day's Service Credit for each two (2) full hours period of Service Unavailability ("Service Credits");

6.2.2. The issuance of Service Credits is subject to a maximum credit of five (5) days in any one calendar month.

6.3. Service Credits will be issued for all Services impacted by the Verified Outage as detailed in your claim. One claim cannot result in multiple Service Credits for different Services.

**7. Procedure to claim Service Credits**

7.1. In order to receive a Service Credit under this SLA, you must follow the procedures described below:

7.1.1. A Claimed Outage must be reported to our Technical Support Team within seven (7) calendar days following the end of the Claimed Outage; and

7.1.2. The report must include Service name(s), dates and times of the Claimed Outage, error messages received (if any), test reporting (if any), contact information and a full description of the interruption.

7.2. We will review the Claimed Outage against Verified Outage(s) within a reasonable time following receipt of the claim, using all information reasonably available in order to calculate the outage length, including analysis of service data immediately prior to the Claimed Outage. You will work with us, if requested, to verify the accuracy of the reports and information provided to us so we, acting reasonably, may confirm that the Claimed Outage occurred. An SLA Credit will be issued if the claim is determined to be valid by us. Our determination of the validity of claims is final. Your failure to provide the credit request and/or the information required above will disqualify you from receiving a Service Credit.

7.3. You agree to continue to make pay the Subscription Fees in full for Services while a Claimed Outage is being reviewed or a SLA Credit is being determined.

7.4. The SLA Credit will be applied against future charges only. SLA Credits may not be used to reduce the payments due in any term below zero.

**8. Remedies:**

The issuance of SLA Credits are your sole and exclusive remedy for any failure by us to satisfy the requirements set forth in this SLA.

**9. Amendment:**

We reserve the right to amend this SLA in accordance with Module A clause 19.

# Module F – Terms for Managed Services

## 1. Introduction:

1.1. These terms ("Managed Service Terms") apply where you purchase any of the TrustLayer Professional Services offerings ("Managed Service") such as Managed Web Security Rule Optimisation Service.

The Managed Service is provided in conjunction with the TrustLayer Services detailed in Module B, and is subject to these Managed Service Terms, Module A, Module B and any applicable Order.

The Managed Service comprises operational services performed by authorised TrustLayer personnel on your behalf, including the assessment, implementation, validation and documentation of configuration and policy changes within the TrustLayer Web Security platform.

The Managed Service is separate from Support Services under Module D and from any consultancy, project, implementation or incident response services that may be provided by TrustLayer from time to time.

IMPORTANT NOTICES

THE MANAGED SERVICE INVOLVES TRUSTLAYER PERSONNEL MAKING CHANGES TO THE CONFIGURATION OF YOUR WEB SECURITY ENVIRONMENT IN RELIANCE UPON INSTRUCTIONS AND APPROVALS PROVIDED BY YOU.

YOU REMAIN RESPONSIBLE FOR YOUR SECURITY POLICIES, THE BUSINESS, SECURITY, LEGAL AND COMPLIANCE APPROPRIATENESS OF EACH REQUESTED CHANGE, AND FOR END-TO-END TESTING OF YOUR ENVIRONMENT FOLLOWING IMPLEMENTATION.

THE MANAGED SERVICE TERMS INCLUDE, IN PARTICULAR, THE LIMITATIONS AND EXCLUSIONS OF LIABILITY CONTAINED IN MODULE A CLAUSE 10.

## 2. Definitions and Application

2.1. In this Module F:

Authorised Contact means an individual identified by you as being authorised to submit, approve or otherwise provide instructions in relation to Change Requests.

Change Request means a request submitted by or on behalf of you for TrustLayer to make a configuration, rule, policy or related operational change to the Web Security Service.

Managed Service Allowance means any quantity of Change Requests, hours, capacity or other usage allowance included within the Managed Service Fee.

Managed Service Hours means 09:00 to 17:00 UK time on each Business Day.

Managed Service Fee means the Subscription Fees payable for the Managed Service.

2.2. The Managed Service may only be purchased and used in conjunction with an active subscription to the TrustLayer Web Security Service.

2.3. These Managed Service Terms apply in addition to Module A and Module B. In the event of any conflict, Module A shall prevail except to the extent that an applicable Order expressly states otherwise.

2.4. For the avoidance of doubt, the Managed Service does not form part of the availability SLA in Module E and the service targets contained in this Module F do not give rise to Service Credits unless expressly stated otherwise in an Order.

## 3. Scope of the Managed Service

3.1. Subject to the applicable Order and any Managed Service Allowance, the Managed Service may include:

a. adding, modifying, or removing policies/rules in the CloudUSS Dashboard;
b. updating filtering rules based on Users, groups, devices, device types or operating systems;
c. adjusting SSL/TLS inspection policies and exception lists;
d. application and category-level control changes;
e. creating or modifying custom URL groups;
f. bypass and exception configuration;
g. Web Security agent profile configuration changes;
h. threat protection rule tuning;
i. URL or application unblock requests;

j. configuration of scheduled or ad-hoc activity reports;
k. MIME-type configuration;
l. reasonable post-change platform-level validation and functional checks; and
m. documentation of completed changes within TrustLayer's ticketing or change management systems and, where expressly agreed and reasonably practicable, within your nominated change management system.

3.2. Unless expressly included in an Order, the Managed Service does not include:
a. troubleshooting of non-policy-related connectivity or performance issues;
b. root cause analysis, forensic investigation, incident response or threat hunting;
c. design or redesign of your IT architecture or implementation;
d. major policy restructuring, bulk policy clean-up or mass rule migration;
e. development of third-party integrations, API scripts or automation;
f. capacity or performance tuning of your environment;
g. escalation to third-party vendors for matters unrelated to a Change Request;
h. rollout of agents, creation of deployment packages or enterprise onboarding;
i. software development or bespoke engineering;
j. penetration testing, vulnerability assessment or security certification; or
k. legal, regulatory, audit or compliance advice.

3.3. Activities outside the scope of the Managed Service may, where available, be provided as separately chargeable Professional Services.

3.4. TrustLayer may reasonably classify or reclassify a request as Support, Managed Services or Professional Services according to the nature, complexity and effort required to fulfil that request. TrustLayer shall not be obliged to commence any activity reclassified as chargeable Professional Services until any applicable additional fees have been agreed.

**4. Change Requests and Authorisation**

4.1. You shall identify and maintain an up-to-date list of Authorised Contacts.

4.2. TrustLayer may rely upon a Change Request, approval or other instruction received from an Authorised Contact through an agreed communication channel as being fully authorised by you. TrustLayer is not required to verify whether an Authorised Contact has obtained any further internal approval required by your organisation.

4.3. You are responsible for:
a. determining whether a requested change is appropriate for your business and security requirements;

b. obtaining all necessary internal, legal, regulatory, privacy, employment, security or other approvals;
c. ensuring the accuracy and completeness of all information contained in a Change Request; and
d. assessing the potential effect of the requested change upon your users, applications, systems and business processes.

4.4. TrustLayer's review or acceptance of a Change Request does not constitute approval of your security policy, business decision, legal position or compliance requirements and does not constitute a warranty that the requested configuration is suitable for your particular purposes.

4.5. Emergency authorisation

Where a Change Request is classified as an Emergency Change, TrustLayer may accept verbal approval from an Authorised Contact where obtaining written approval would cause unreasonable delay. TrustLayer may record that verbal approval within the relevant ticket or change record and may rely upon it as if the approval had been given in writing. You shall provide written confirmation of the instruction as soon as reasonably practicable following the Emergency Change.

## 5. Classification and Governance of Change Requests

5.1. TrustLayer may classify each Change Request, acting reasonably, as one of the following:

| Change Type | Description |
|---|---|
| Standard Change | Common, routine, or template-based change presenting a relatively low level of operational risk. |
| Moderate Change | Custom or moderately complex change requiring additional technical assessment or validation. |
| Emergency Change | Urgent change reasonably required to address an active or imminent security threat or material operational risk. |
| Planned Major Change | Multi-component, complex or higher-risk activity requiring an agreed implementation or maintenance window |

5.2. TrustLayer may reclassify a Change Request where its complexity, scope or risk becomes apparent after initial assessment.

5.3. TrustLayer may reject, defer or propose an alternative to a Change Request where TrustLayer reasonably considers that the Change Request:
a. introduces a material security or operational risk;
b. conflicts with supported platform functionality or technical limitations;

c. could adversely affect the stability, availability, security or performance of the Services or another customer;
d. requires access, information or authorisation that has not been provided;
e. falls outside the scope of the Managed Service;
f. requires significant investigation, design, development or Professional Services;
g. could cause TrustLayer to breach applicable law, regulation or third-party obligations;
h. exceeds the available Managed Service Allowance or available service capacity; or
i. cannot reasonably be completed within the requested timeframe.

5.4. TrustLayer will, where reasonably practicable, explain the reason for rejecting or deferring a Change Request and may recommend an alternative approach.

## 6. Assessment, Implementation and Validation

6.1. Pre-implementation assessment
TrustLayer will apply commercially reasonable change assessment procedures appropriate to the nature and risk of the relevant Change Request.
Such assessment may include consideration of:
a. operational and security risk;
b. potential service impact;
c. policy conflicts or duplication;
d. relevant technical dependencies;
e. reasonably apparent compliance considerations; and
f. the need for an implementation or maintenance window.

6.2. TrustLayer may require additional information, clarification, approval, testing or other action from you before implementing a Change Request.

6.3. Post-implementation validation
Following implementation, TrustLayer will undertake such reasonable platform-level validation as is appropriate to the Change Request, which may include:
a. basic functional validation;
b. policy application checks;
c. log confirmation where applicable; and
d. traffic inspection health checks where applicable.

6.4. TrustLayer's post-implementation validation is not intended to constitute and shall not replace full end-to-end testing of your environment.
You remain responsible for testing and verifying the effect of each Change Request upon your users, devices, networks, applications and business processes.

6.5. Unless otherwise agreed, a Change Request shall be considered completed when TrustLayer has implemented the requested change and notified you that its reasonable post-implementation validation has been completed.

## 7. Rollback and Remediation

7.1. Where reasonably practicable and appropriate to the Change Request, TrustLayer will identify an appropriate rollback or remediation approach before implementation.

7.2. TrustLayer may implement rollback or other remedial action where:

a. TrustLayer's post-change validation identifies a material issue;

b. you promptly report a material unintended consequence of the Change Request; or

c. TrustLayer reasonably considers that the change has materially destabilised the Service.

7.3. You acknowledge that it may not be technically possible to completely or immediately reverse every Change Request.

TrustLayer does not warrant that a Change Request can be rolled back where rollback is prevented or materially affected by:

a. changes subsequently made by you or a third party;

b. Customer or third-party systems;

c. a change to data, identity groups, applications or network infrastructure;

d. external technical dependencies; or

e. circumstances outside TrustLayer's reasonable control.

## 8. Customer-Directed Changes and Security Responsibility

8.1. You retain responsibility for determining the security policy and desired configuration of your environment.

8.2. Subject to Module A clause 10, where TrustLayer implements a Change Request substantially in accordance with an instruction approved by an Authorised Contact, TrustLayer shall not be responsible for any reduction in security coverage, access restriction, application incompatibility, loss of functionality, business interruption or other consequence arising from the content or intended effect of that approved Change Request.

8.3. Where TrustLayer advises you that a Change Request may reduce security protection or create a material security or operational risk and you nevertheless instruct TrustLayer to proceed, TrustLayer may:

a. refuse to implement the Change Request; or

b. implement the Change Request following your express confirmation that you wish to proceed.

Where paragraph (b) applies, you accept responsibility for the risks specifically identified to you by TrustLayer.

8.4. You acknowledge that no security configuration or security service can prevent or detect all threats and that changes to security policies may result in false positives, false negatives or unintended effects.

## 9. Service Targets

9.1. TrustLayer will use commercially reasonable efforts to meet the following service targets:

| Request Type | Initial Response Target | Completion Target |
|---|---|---|
| Standard Change | Within 8 business hours | Within 1 business day |
| Moderate Change | Within 8 business hours | Within 2 business days |
| Emergency Change | Within 4 business hours | Within 4 business hours, subject to approval and technical feasibility |
| Planned Major Change | Within 1 business day | In accordance with an agreed implementation window |

9.2. Unless expressly stated otherwise in the Order:

a. the service targets apply only during Managed Service Hours;

b. a Change Request received outside Managed Service Hours shall be deemed received at the start of the next Business Day;

c. the applicable response or completion period shall not begin until TrustLayer has received a sufficiently complete Change Request and all necessary authorisations;

d. target times shall be suspended while TrustLayer awaits information, approval, access, testing or another dependency from you or a third party;

e. the completion targets assume that the Change Request can be completed without material unforeseen technical issues; and

f. Planned Major Changes shall be subject to mutually agreed implementation windows.

9.3. The targets in clause 9.1 are service targets and not guaranteed completion times. Failure to meet a target does not constitute Service Unavailability under Module E and does not entitle you to a Service Credit, refund or other financial remedy unless expressly stated in an applicable Order.

9.4. Out-of-hours, weekend or public holiday Change Requests are not included unless expressly specified in the applicable Order and may be subject to additional fees.

9.5. An Emergency Change does not, of itself, entitle you to out-of-hours support or change execution.

**10. Customer Responsibilities**

10.1. You shall:

a. provide clear, complete and accurate information for each Change Request;

b. promptly provide all approvals, clarifications and decisions reasonably requested by TrustLayer;

c. maintain accurate details for Authorised Contacts and escalation contacts;

d. perform appropriate end-to-end testing following implementation;

e. notify TrustLayer of relevant network, infrastructure, identity-provider or architectural changes which may affect implementation;

f. maintain the identity and access structures upon which your security rules depend, including Active Directory groups, identity-provider attributes and other Customer-controlled identity information;

g. ensure the underlying Web Security deployment remains properly deployed, configured and supported;

h. provide reasonably requested traffic samples, logs or other diagnostic information required for assessment or validation; and

i. maintain appropriate internal change-management, security and compliance procedures.

10.2. TrustLayer shall not be responsible for delay, failure or additional work arising from your failure to comply with this clause.

**11. Service Dependencies**

11.1. The Managed Service depends upon the continuing availability and correct operation of the underlying Service and relevant Customer and third-party systems.

11.2. Dependencies may include:

a. connectivity between your environment and the TrustLayer platform;

b. identity providers and user/group structures;

c. Customer networks, devices and applications;

d. Customer-managed naming conventions and configuration information;

e. third-party cloud, identity, network and application services; and

f. information, logs and access supplied by you.

11.3. TrustLayer shall not be responsible for failure to meet a service target or for an unsuccessful Change Request to the extent caused by a dependency outside TrustLayer's reasonable control.

**12. Managed Service Allowance and Additional Services**

12.1. The applicable Order will specify a Managed Service Allowance, expressed as a number of service hours available to you throughout the Term.

12.2. Unless expressly described in an Order as unlimited, payment of a fixed Managed Service Fee does not entitle you to unlimited Change Requests or unlimited engineering resource.

12.3. Any included Managed Service Hours that are not used during the Term shall expire at the end of that period and shall not roll over, accumulate or carry forward into any subsequent Order. Unless otherwise specified in the Order, unused Managed Service capacity does not entitle you to any refund or Service Credit.

12.4. Where the Managed Service Allowance has been or is reasonably expected to be exceeded, TrustLayer may:

a. defer additional Change Requests until additional capacity becomes available;
b. offer additional Managed Service capacity for an additional fee; or
c. propose that the requested work be performed as Professional Services.

12.5. TrustLayer shall not be obliged to perform work exceeding the applicable Managed Service Allowance unless any applicable additional fees have been agreed.

12.6. TrustLayer's records of time spent providing the Managed Service shall, in the absence of manifest error, be conclusive for the purpose of determining use of the Included Managed Service Hours.

**13. Reporting and Audit Trail**

13.1. TrustLayer will maintain an appropriate audit trail of Change Requests, which may include:

a. Change Request records;
b. approvals;
c. implementation notes; and
d. post-change validation results.

13.2. Managed Service records shall be retained in accordance with TrustLayer's applicable retention policies and, to the extent they contain Personal Data, the DPA.

13.3. Any recommendations, security observations or compliance-related comments made by TrustLayer are provided for informational purposes only and do not constitute legal, audit, certification or regulatory advice or a warranty that you will achieve or maintain any certification, accreditation or regulatory compliance.

**14. Data Protection and Access**

14.1. The DPA applies to the processing of Personal Data in connection with the Managed Service.

14.2. You authorise appropriately authorised TrustLayer personnel to access and modify your Web Security configuration and to access relevant logs, policy information and other Customer Data to the extent reasonably necessary to:

a. assess Change Requests;
b. implement approved changes;
c. validate and troubleshoot those changes; and
d. document and report upon the Managed Service.

14.3. You shall ensure that you have all necessary authority and lawful bases to instruct TrustLayer to perform such activities.

**15. Term and Termination**

15.1. The Managed Service shall commence on the date specified in the applicable Order and continue for the Term specified in that Order, subject to Module A.

15.2. The Managed Service is dependent upon an active Product Subscription as defined in Module A. If your applicable Service Subscription expires or terminates, the Managed Service shall automatically terminate at the same time unless TrustLayer agrees otherwise in writing.

15.3. Termination or expiry of the Managed Service shall not, of itself:

a. terminate your Core Service Subscription; or
b. entitle you to terminate any other Service purchased from TrustLayer.

15.4. TrustLayer may suspend delivery of the Managed Service while the underlying Security Service is suspended or where TrustLayer does not have the access, information or authority reasonably required to provide the Managed Service.

**16. Managed Service Warranty**

16.1. TrustLayer will provide the Managed Service with reasonable skill and care.

16.2. Except as expressly set out in this Module F or elsewhere in the MSA:

a. TrustLayer does not warrant that any particular Change Request will achieve a particular business, operational, security or compliance outcome;

b. TrustLayer does not warrant that every requested Change Request will be technically feasible;

c. TrustLayer does not warrant uninterrupted or error-free operation following a Change Request; and

d. the limitations and exclusions in Module A clause 10 apply in full to the Managed Service.

# Appendix 1 - Email Security Service ("EMS")

## 1. Definitions:

The following terms are used:

- "Availability" or "Available" is defined as the delivery of email messages to and from your mail server.

- "Known Virus" is defined as a virus which has already been identified and a virus definition has been made available by one of the anti-virus services whose technology is used within our EMS, at least thirty (30) minutes before the time the email was processed by the EMS.

- "Service Unavailability" is defined as the inability of the EMS to receive and process email substantially in accordance with the published online documentation and measured during any given calendar month.

## 2. Availability:

Our EMS will be available 99% of the time.

## 3. Virus Detection:

3.1. We will detect and block 100% of Known Viruses contained in supported, unencrypted and otherwise scannable content processed through the relevant Service. This excludes links (URLs) inside email messages that take you to a website where viruses can be downloaded.

3.2. In the event that one or more Known Viruses in any calendar month passes through the EMS undetected and infects your systems, following a request submitted by you in accordance with the procedure detailed above in clause 7 of the SLA, we will credit you with one (1) day's Service Credit, subject to you providing evidence acceptable to us that the EMS failed to detect the Known Virus within seven (7) Business Days of the Virus infection, and the claim being approved.

3.3. The Virus Detection SLA for EMS will not apply if: (a) the virus was contained inside an email that could not be analysed by the EMS, such as encrypted email or a password protected file; (b) the Virus infection occurred because an email which had been identified as containing a Virus was released by us on your request, or released

by you through the administration portal; or (c) there is deliberate self-infection by you.

**4. SPAM Detection:**

4.1. Certain SPAM will be detected at a rate of 99.9% or above during each calendar month.

4.2. The SPAM detection rates do not apply to emails using a non-English or non-European language or emails sent to invalid mailboxes.

4.3. In the event that certain SPAM detection rates drop below 99.9% in any one (1) calendar month, following a request submitted by the Customer in accordance with the procedure detailed above in Clause 7 of the SLA, TrustLayer will credit the Customer with one (1) day's Service Credit if the claim is approved.

# Appendix 2 - Web Security Service ("WS")

## 1. Definitions:

The following terms are used:

- "Availability" or "Available" is defined as the ability to request, process and receive web content.

- "Known Virus" is defined as a virus which has already been identified and a virus definition has been made available by one of the anti-virus services whose technology is used within our WS, at least thirty (30) minutes before the time the web request was processed by the WS.

- "Service Unavailability" is defined as the inability of the WS to request, process and receive web content substantially in accordance with the published online documentation for the WS, and measured during any given calendar month.

## 2. Availability:

Our WS will be Available 99% of the time.

## 3. Virus Detection:

3.1. For Customers subscribing to the optional additional Gateway Anti-virus module we will detect and block 100% of Known Viruses contained in supported, unencrypted and otherwise scannable content processed through the relevant Service, subject to the exclusions below.

3.2. In the event that one or more Known Viruses in any calendar month passes through the WS undetected and infects your systems, following a request submitted by you in accordance with the procedure detailed above in clause 7 of the SLA, we will credit you with one (1) day's Service Credit, subject to you providing evidence acceptable to us that the WS failed to detect the Known Virus within seven (7) Business Days of the Virus infection and the claim being approved.

3.3. The Virus Detection SLA for WS will not apply if: (a) the virus was contained inside web content that could not be analysed by the WS - for example but not limited to a feature not being correctly deployed or configured that would have given the WS access to HTTPS encrypted content; (b) the Virus infection occurred because of a bypass rule configured by you; or (c) there is deliberate self-infection by you.

# Appendix 3 – Cloud Application Security ("CASB")

## 1. Definitions:

The following terms are used:

- "Availability" or "Available" is defined as the ability to request, process and receive cloud application content.

- "Known Virus" is defined as a virus which has already been identified and a virus definition has been made available by one of the anti-virus services whose technology is used within our CASB, at least thirty (30) minutes before the time the web request was processed by the CASB.

- "Service Unavailability" is defined as the inability of the CASB to request, process and receive cloud application content substantially in accordance with the published online documentation for the CASB, and measured during any given calendar month.

## 2. Availability:

Our CASB will be Available 99% of the time.

## 3. Virus Detection:

3.1. For Customers subscribing to the optional additional Gateway Anti-virus module we will detect and block 100% of Known Viruses contained in supported, unencrypted and otherwise scannable content processed through the relevant Service, subject to the exclusions below.

3.2. In the event that one or more Known Viruses in any calendar month passes through the CASB undetected and infects your systems, following a request submitted by you in accordance with the procedure detailed above in clause 7 of the SLA, we will credit you with one (1) day's Service Credit, subject to you providing evidence acceptable to us that the CASB failed to detect the Known Virus within seven (7) Business Days of the Virus infection and the claim being approved.

3.3. The Virus Detection SLA for CASB will not apply if: (a) the virus was contained inside cloud application content that could not be analysed by the CASB – for example but not limited to a feature not being correctly deployed or configured that would have given the CASB access to HTTPS encrypted content; (b) the Virus infection occurred because of a bypass rule configured by you; or (c) there is deliberate self-infection by you.