Master Services Agreement

Version: 2.2
Issued: December 2020

Master Services Agreement

Operative Provisions:

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

Module A – General Terms
and
Module B - Data Processing Requirements
and
Module C – Terms for Unified Security Service ("**USS**") including Web Security ("**WS**"), Cloud Application Security ("**CASB**"), Cloud Multi-Factor Authentication ("**Cloud MFA**"), MFA powered by IntelliTrust ("**MFA**"), Compliant Email Archive ("**CEMA**") and Autonomous Security Engine ("**ASE**").
[and]
Module D – Terms for Email Security ("**EMS**")
[and]
Module E – Terms for Support Services
and
Module F – Service Level Agreement ("**SLA**")

(*Modules C and D may or may not apply depending on the Service(s) purchased)

Acceptance

By clicking "I ACCEPT" when logging in to the Censornet USS Portal for the first time and following acceptance of an Order by Censornet the Customer enters a contract with Censornet for the selected Service(s) referred to in the relevant Modules from the Effective Date.

Module A – General Terms

Introduction:

These Terms and Conditions (these **"Terms"**) constitute a binding contract between Censornet 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).

These Terms apply to such Contract notwithstanding any provision of the respective Modules. These Terms apply to all Free Trials and NFR Licences, save for Clauses 2, 5 and 11.

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).

1. Interpretation:

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

"Bulk Email Terms and Conditions"	means Censornet's Bulk Email Terms and Conditions applicable to EMS, as amended from time to time, made available to the Customer by Censornet 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.
"**Censornet**", "**us**" or "**we**"	means Censornet Limited (Co. No. 05518629), the registered office of which is at Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT, UK;
"**Change of Control**"	shall be as defined in section 1124 of the Corporation Tax Act 2010.
"**Confidential Information**"	information that is proprietary or confidential disclosed by a party to the other party including commercial or technical know-how, technology, information pertaining to business operations, strategies, customers, pricing and marketing or is either clearly labelled as confidential or identified as Confidential Information.
"Contract"	the contract between Censornet and the Customer;
"Customer"	means all customers purchasing Services from Censornet described in the Modules or using our Services by way of a Free Trial or NFR License.
"**Customer Data**"	the data inputted by the Customer, Users, or Censornet on the Customer's behalf for the purpose of using the Services or facilitating the Customer's use of the Services.
"Data Protection Legislation"	the General Data Protection Regulation (EU) 2016/679, the General Data Protection Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the

	European Union, the Data Protection Act 2018 and any national implementing laws, regulations and secondary legislation, as replaced, amended or updated from time to time in the UK, and all applicable law relating to data protection and the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
"**Documentation**"	the documents made available to the Customer by Censornet online via https://www.censornet.com or such other web address notified by Censornet 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 Censornet's Fair Usage Policy applicable to WS and CASB, as amended from time to time, made available to the Customer by Censornet 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.
"Intellectual Property Rights"	patents, rights to inventions, copyright and

	neighbouring and related rights, trade marks 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**"	9.00 am to 5.30 pm local time, each Business Day.
"Order"	An email, purchase order or online order for one or more of the Services;
"Privacy Policy"	means Censornet's Privacy Policy, as amended from time to time, made available to Customers by Censornet online via its website https://www.censornet.com/privacy-policy/

"Product Usage Policy"	means Censornet's Product Usage Policy, as amended from time to time, made available to the Customer by Censornet online via the Product Help Portal https://help.clouduss.com/platform-general/understanding-product-usage
"Reseller"	means an authorised reseller of Censornet's Services.
"**Services**"	the Service(s) provided by Censornet to the Customer on these Terms, to include Email Security (EMS), Web Security (WS), Cloud Application Security (CASB), Cloud Multi-Factor Authentication (Cloud MFA), MFA powered by IntelliTrust (MFA), Compliant Email Archive (CEMA) and Autonomous Security Engine (ASE) as more particularly described in the Documentation.
"**SLA**"	Censornet's Service Level Agreement for providing support in relation to the Services contained in Module F.
"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 Censornet (whether or not through a Reseller) for the applicable Service(s), as notified/invoiced by Censornet;

"Term	means the agreed contract length, as set out in the Order, with effect from the Effective Date
"Users"	those employees, agents and independent contractors of the Customer, who the Customer wishes to be subject to the Services.
"**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, including worms, trojan horses, viruses, time bombs and other similar things or devices.
"Year"	means a 12-month period from the Effective Date.

1.2 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 genders; a reference to a statute or statutory provision is a

reference to it as amended, extended or re-enacted from time to time and a reference to writing or written includes e-mail.

2. The Contract:

2.1 Any quotation given by Censornet 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.

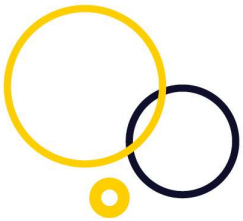
2.2 An Order constitutes an offer by you to license the relevant Service(s) in accordance with these Terms. An Order shall be deemed to be accepted by us, and the Contract shall come into existence, on confirmation of the Order to you or on first use of the Service(s) (whichever is soonest).

3. Use of Censornet Services:

3.1 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).

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

3.3 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.



3.4 In respect of EMS and CEMA, 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 oversuage.

3.5 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.

(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

(d) Privacy Policy, as amended from time to time, which can be found at: https://www.censornet.com/privacy-policy/.

3.6 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 its activities for which the Service(s) / Software / Documentation are provided; and

(c) be responsible for set up and maintenance of accounts and Customer Data to ensure accurate usage reporting.

3.7 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. Restrictions:

4.1 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;

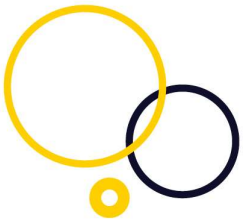
(f) not to publicly display or publicly perform the Software (without prior written consent);

(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 C) and EMS terms (contained in Module D);

(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 the privacy and/or Data Protection Legislation without written permission. 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 Censornet, customers, partners or any other third party; and

(p) to comply with all applicable technology control, applicable laws, rules, export controls, regulations and all privacy and data protection laws.

4.2 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.

4.3 We reserve the right to investigate the violation of this clause 4 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.

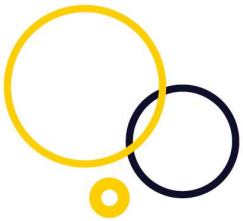
5. Fees and payment:

5.1 <u>If the Customer is purchasing the Service(s) through a Reseller</u>:

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

5.1.2 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.

5.1.3 Failure to provide proof of payment within 14 days after being notified in writing to provide such proof in accordance with clause 5.1.2 above may result in the suspension, or termination, of the Service(s) provided to you.



5.1.4 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.

5.2 If the Customer is purchasing directly:

5.2.1 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.

5.2.2 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.

5.2.3 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).

5.2.4 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.

5.3 All invoices rendered in respect of additional Subscription Fees payable for overusage (in accordance with clauses 3.3 and 3.4 above) will be subject to the same payment terms as detailed above in clauses 5.1 and 5.2 (as applicable).

5.4 Monthly Billing:

5.4.1 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.

5.4.2 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.

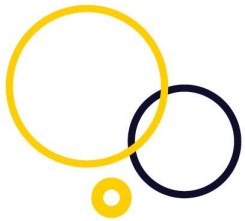
5.4.3 Monthly Fees are based on actual usage for the preceding month and are billed in line with the Product Usage Policy.

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

5.4.5 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).

5.4.6 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.

5.5 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.

6. Intellectual Property Rights:

6.1 All Intellectual Property Rights (IPR) in and to the Service(s) belong, and shall continue to belong, to Censornet.

6.2 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 Censornet 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.

6.3 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.

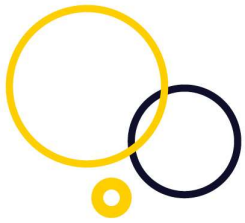
6.4 You shall promptly give notice in writing to us in the event that you become aware of any infringement or suspected infringement of any IPR in or relating to the Service(s).

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

7. Confidentiality:

7.1 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.

7.2 Subject to clause 7.4, 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.

7.3 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 7 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.

7.4 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 7.4, it takes into account the reasonable requests of the other party in relation to the content of such disclosure.

7.5 Neither party shall be responsible for any loss, destruction, alteration or disclosure of Confidential Information caused by any third party.

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

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

7.8 The receiving party agrees that breach of this clause 7 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.

7.9 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.

7.10 The above provisions of this clause 7 shall survive termination of this Contract for a period of five (5) years thereafter, however arising.

8. Protection and processing of personal data:

8.1 The parties acknowledge that for the purposes of the Data Protection Legislation, you are the controller and we are the processor.

8.2 You warrant that you have all necessary and appropriate consents and notices in place to enable the lawful transfer of Personal Data to Censornet for the duration and purposes of the Contract so that we may hold, use, process and transfer such Personal Data when providing the Service(s).

8.3 Each party shall comply with its obligations under the provisions of Module B and of the Data Protection Legislation in relation to any Personal Data that it processes under this MSA and the Service(s) provided.

8.4 You are responsible for informing all Users and third parties of such use and obtaining any necessary consents as may be required by the Data Protection Legislation.

9. Limitation of liability and warranties:

9.1 The following provisions set out the entire financial liability of Censornet (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) arising under or in connection with the Contract.

9.2 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. Censornet (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).

9.3 Nothing in the Contract excludes the liability of Censornet:

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

(b) for fraud or fraudulent misrepresentation.

9.4 Other than in relation to any liability under clause 9.3, subject to clause 9.5, Censornet 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 or corruption of data or information; or

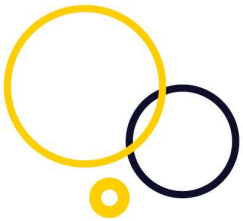
(h) any special, indirect, consequential or pure economic loss, costs, damages, charges or expenses.

9.5 Other than in relation to any liability under Clause 9.3, Censornet'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.

9.6 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.

9.7 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, 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.

9.8 We use our best efforts 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.

9.9 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.

9.10 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.

9.11 Except as expressly and specifically provided in this MSA:

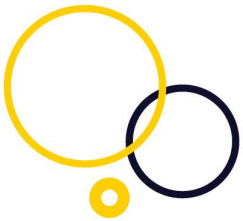
(a) you assume sole responsibility for results obtained from the use of the Service(s) / Software / Documentation by you, and for conclusions drawn from such use. We shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to us by you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

10. Indemnity:

10.1 You shall defend, indemnify and hold harmless Censornet 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.

10.2 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

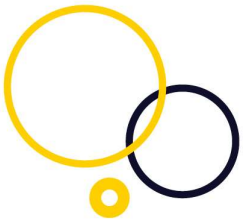
(c) we are given sole authority to defend or settle the claim.

10.3 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.

10.4 In no event shall Censornet, 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.

10.5 The foregoing and clause 9 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. Term, Renewal and Termination:

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

11.2 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.

11.3 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.

11.4 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.

11.5 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).

11.6 The termination of the Contract shall not of itself give rise to any liability on the part of Censornet 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.

11.7 On termination of the Contract for any reason:

11.7.1 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;

11.7.2 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;

11.7.3 We may destroy or otherwise dispose of any of your Data in our possession unless we receive no later than ten days after the effective date of the termination of the Service(s) a request not to do so. You shall pay all reasonable expenses incurred by Censornet in disposing of Customer Data; and

11.7.4 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.

12. 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 E for the Terms of our Support Services.

13. Entire agreement:

This agreement 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.

14. Assignment:

14.1 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.

14.2 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.

15. No partnership or agency:

15.1 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.

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

16. 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.

17. Waiver:

No failure or delay by a party to exercise any right or remedy provided under the MSA or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

18. Variation:

No variation of the Contract or MSA shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

19. 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.

20. 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.

21. Third Parties:

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

22. 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.

23. 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 - Data Processing Requirements

1. Definitions:

1.1 In this Module, unless the context otherwise requires, the following words and expressions have the following meanings:

"Agreement"	any agreement for the supply of Service(s) entered into by the parties whether forming part of the Contract which includes this Module or otherwise.
"Censornet Personnel"	means all directors, officers, employees, agents, consultants and contractors of Censornet and/or any sub-contractor engaged in the performance of its obligations under this Agreement.
"Controller"	has the meaning given in the GDPR.
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by Censornet under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement.
"Data Subject"	has the meaning given in the GDPR.
"Data Protection Officer"	has the meaning given in the GDPR.
"Data Protection Legislation"	the General Data Protection Regulation (EU) 2016/679, the General Data Protection Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the European Union, the Data Protection Act 2018 and any national implementing laws, regulations and secondary legislation, as replaced, amended or updated

	from time to time in the UK, and all applicable law relating to data protection and the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
"GDPR"	the General Data Protection Regulation (EU 2016/679) and the General Data Protection Regulation (EU 2016/679) as amended by any legislation arising out of the withdrawal of the UK from the European Union.
"Personal Data"	has the meaning set out in the GDPR and relates only to personal data, or any part of such personal data, of which the Customer is the Data Controller and in relation to which Censornet is providing Service(s) under the Contract.
"Processor" and "processing"	have the meaning set out in the GDPR.
"Sub-Processor"	any third party appointed to process Personal Data on behalf of Censornet related to this Agreement.
"SCCs"	means the model contract clauses set out in the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to data-processors established in third countries, under the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and any replacements or amendments to the SCCs from time to time.

2. Basis for Processing or Sharing:

2.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This Module is in addition to, and does not relieve, remove or replace, the parties obligations under the Data Protection Legislation.

2.2 The parties acknowledge that for the purposes of the Contract, the Customer is the Data Controller and Censornet is the Data Processor of any Personal Data.

2.2 The basis for processing and sharing Personal Data under this Agreement is in accordance with a lawful basis for processing Personal Data provided for by the Data Protection Legislation. The details of the data processing activities in relation to this Agreement are set out in Annex A.

3. Obligations of Censornet:

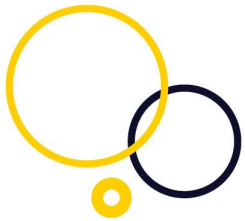
3.1 We shall only process any Personal Data on behalf of you in accordance with the written instructions provided by you and to the extent, and in such a manner as set out in Annex A. If we are required to do otherwise by law then we will promptly notify you of that legal requirement, where possible, before processing the Personal Data.

3.2 We shall provide all reasonable assistance to you in the preparation of any data protection impact assessment required prior to commencing any processing.

3.3 We will maintain complete and accurate records of any processing of Personal Data we carry out on your behalf.

3.4 If we receive any complaint, notice or communication which relates directly or indirectly to the processing or sharing of the Personal Data or to either party's compliance with the Data Protection Legislation, we shall promptly notify you and provide full co-operation and assistance in relation to any such complaint, notice or communication.

3.5 We shall ensure that we have in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and to protect against a Data Loss Event. The protective measures take account of:



3.5.1 the nature of the data to be protected;

3.5.2 the harm that might result from a Data Loss Event;

3.5.3 the state of technological development; and

3.5.3 the cost of implementing any measures.

3.6 We shall promptly inform you of a Data Loss Event or if any Personal Data becomes damaged, corrupted, or unusable. To the extent that we are responsible, we will restore such Personal Data at our own expense.

3.7 We shall notify you immediately if we become aware of any unauthorised or unlawful processing of Personal Data and in such circumstances shall comply with all your requests in dealing with the situation.

3.8 At your request, we shall provide you with a copy of all Personal Data held by us in the format and in the media reasonably specified by you.

3.9 Upon termination of the Agreement for any reason, we shall cease processing any Personal Data and shall return all Personal Data to you and any copies thereof, where requested, or shall securely destroy all Personal Data if instructed to do so by you and shall certify that this has been done, unless prevented from doing so by law.

4. Transfers outside the EEA:

4.1 Subject to clause 4.2, we shall not transfer any Personal Data outside of the European Economic Area ("**EEA**") unless your prior written consent has been obtained.

4.2 You acknowledge and consent to the transfer of Personal Data to the non-EEA Sub-Processors listed in Annex B.

4.3 In relation to the transfer of Personal Data that you transfer to us from the UK that we transfer to a non-EEA Sub-Processor located in third countries non benefiting from an adequacy decision (see list in Annex B), you hereby authorise us to (i) rely on their

BCR-processor instrument (if any) or (ii) enter into the SCCs in your name and on your behalf with any such non EEA Sub-Processors in relation to such transfer on the basis that:

4.3.1 you are the 'data exporter' and the non-EEA Sub-processor is the 'data importer';

4.3.2 where the SCCs contain modular options, the controller to processor transfer modules are selected;

4.3.3 the processing details applicable to the SCCs are as set out in Annex C and the applicable security measures are set out at Annex D; and

4.3.4 Where the SCCs are amended or replaced and we enter into such amended or replaced SCCs in your name and on your behalf with non-EEA Sub-processors pursuant to the authority granted in this clause 4.3, we will notify you of this.

4.4 In relation to the transfer of Personal Data that you transfer to us from the EEA, we agree to the terms of the SCCs (with you being the 'data exporter' and us being the 'data importer' under such SCCs) and we both agree that:

4.4.1 for the purposes of clauses 5(h) and 11 of the SCCs, you consent to the us appointing sub-processors in accordance with the provisions set out at clause 4.2 of this Agreement;

4.4.2 any rights to audit, pursuant to clauses 5(f) and 12(2) of the SCCs, will be exercised in accordance with clause 7 of this Agreement;

4.4.3 in the event of any conflict between the SCCs and the rest of this Agreement, the SCCs shall prevail; and

4.4.4 the details of the appendices applicable to the SCCs are as set out in Annex C and the security measures required are set out at Annex D.

The above shall cease to apply in the event that the European Commission issues an adequacy decision in relation to the United Kingdom under Article 45 of the GDPR.

5. Censornet's Personnel:

5.1 We shall ensure that access to the Personal Data is limited to those Censornet Personnel who need access to the Personal Data to meet our obligations under this Agreement.

5.2 We shall ensure that all Censornet Personnel:

5.2.1 are aware both of our duties and their personal duties and obligations under the Data Protection Legislation and this Contract;

5.2.2 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by you or as otherwise permitted by this Agreement;

5.2.3 are subject to appropriate confidentiality undertakings with us (or, if applicable, any Sub-Processor); and

5.2.4 have undertaken adequate training on the Data Protection Legislation relating to the use, care, protection and handling of Personal Data.

6. Rights of the Data Subject:

6.1 We shall notify the Customer immediately if we:

6.1.1 receive a request from a Data Subject for access to that person's Personal Data;

6.1.2 receive a request to rectify, block or erase any Personal Data;

6.1.3 receive a request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by Law; or

6.1.4 becomes aware of a Data Loss Event.

6.2 We shall provide you with full co-operation and assistance in relation to any request or event referred to in clause 6.1.

6.3 We shall promptly comply with any request from you requiring us to amend, transfer or delete the Personal Data.

6.4 We shall not disclose the Personal Data to any Data Subject or to a third party other than at your request or as provided for in this Module B.

6.5 We have designated a Data Protection Officer.

7. Rights of the Customer:

You are entitled, on giving us reasonable notice, to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data by us.

8. Warranties:

8.1 We warrant that:

8.1.1 we will process the Personal Data in compliance with the Data Protection Legislation and all other applicable laws, enactments, regulations, orders, standards and other similar instruments;

8.1.2 we will take such appropriate technical and organisational measures in order to ensure the safety and security of the Personal Data; and

8.1.3 we will take appropriate technical and organisational measures against the unauthorised or unlawful processing of Personal Data and against a Data Loss Event or destruction of, or damage to, Personal Data.

9. Appointment of Sub-Processors:

9.1 Subject to the terms of clause 4, we may only authorise a Sub-Processor to process the Personal Data provided that the Sub-Processor's contract is on terms which comply with Data Protection Legislation.

9.2 We shall remain fully liable to you for all acts or omissions of any Sub-Processor.

10. Review:

10.1 We may, at any time, revise this Module to ensure that it complies with any amendments to the Data Protection Legislation or any guidance issued by the Information Commissioner's Office. Any amendments to this Module will become effective upon you accepting the terms of the updated MSA online.

Annex A – Processing, Personal Data and Data Subjects

1. Introduction:

1.1 The Censornet Unified Security Service (USS) platform incorporates multiple security services that may be purchased separately or in any combination, at any time. Not all of the following information may therefore be applicable depending on the specific Service(s) purchased.

Service(s) include:

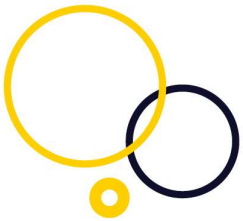
- Email Security (EMS)
- Compliant Email Archive (CEMA)
- Web Security (WS)
- Cloud Access Security Broker (CASB)
- Cloud Multi-Factor Authentication (Cloud MFA)
- Multi-Factor Authentication powered by IntelliTrust (MFA)
- Autonomous Security Engine (ASE) – an integral part of the USS platform

2. Unified Security Service (USS) Platform Security Measures:

2.1 We use world-class, highly accredited providers to deliver USS and associated services that include Amazon, IBM and Microsoft. Under GDPR these organisations would be considered Sub-processors.

2.2 In Europe specific data centre locations include London, Frankfurt, Dublin and Amsterdam.

2.3 USS log data is stored in a log database called LogDB. The region/location is specified at the time of account provisioning. You have a choice of London (UK), Frankfurt (EU), Dallas TX (US) or Dubai (UAE).



2.4 We offer a true multi-tenant environment with separate database schema for each customer. Customer log data in LogDB is isolated to a specific partition on IBM Endurance Storage Nodes (redundant network SANs) and encrypted at rest.

2.5 Log data in LogDB is archived after a specified retention period. This retention period is 90 days for WS and EMS and 365 days for CASB and Cloud MFA services.

2.6 Log data is archived to Amazon S3 storage in the same 'home' region where it lives for a further twelve (12) months and is then deleted. Log data in S3 is encrypted.

2.7 The only other service related data is policy/rule/configuration data that is held in a different database called CoreDB. The CoreDB master database (in Amsterdam) is currently replicated across 9 IBM locations worldwide to ensure rapid response times to user requests. Customers within Europe will be restricted by default to only using EU data centre locations. Use of data centres outside of Europe must be explicitly requested, either at the time of provisioning, or later.

2.8 All service-related data is handled in strict accordance with Data Protection Legislation.

3. Service Specific Security Measures:

3.1 Web Security (WS)

The WS service uses the USS infrastructure, notably two databases - LogDB and CoreDB - for log data and policy/rule/configuration data respectively - described in clause 2 of this Module B.

3.1.1 **WS Risks:**

- Although the use of https has increased dramatically a significant number of websites still use the unencrypted http protocol. Information sent in requests to and from those sites is therefore unencrypted in clear text and may be intercepted.
- WS is focused on protecting users from harmful, unlawful, offensive or inappropriate content. Harmful content includes web-borne malware a well as phishing sites designed to capture credentials or other confidential information.
- Viewing all of an individual user's web activity over time may enable the viewer to make assumptions or gain insight into the particular interests of

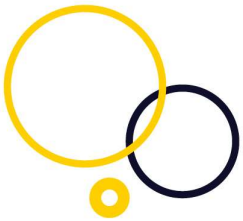
that user, or draw conclusions in respect of the user's political or religious beliefs.

3.1.2 **Scope of Risk:**

- Our staff could access log information that contains details of user's web browsing activity.
- Only a small number of our staff are involved in the administration of WS systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores web activity log data.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.1.3 **Input data that contains personal data – WS:**

- Input data for the WS service is comprised of all http and https web requests and associated metadata. Metadata includes Active Directory (**AD**) usernames, IP addresses and MAC addresses. Request information is sent securely using ICAP to the Censornet cloud and compared against customer configured policy to determine whether the URL is allowed or blocked. A final action is returned to the agent and/or gateway that results in the request being released to the target website, or blocked.
- Each ICAP server stores requests temporarily on disk in a transaction log. The servers maintain a transaction log for every LogDB partition that they are actively handling requests for. A new transaction log is written every 60 seconds and shipped to the appropriate LogDB server. The temporary log file is then deleted from the ICAP server.



3.1.4 **Output data that contains personal data – WS:**

- Output data from the WS service is comprised of log data relating to http and https web requests. Log information includes AD usernames, IP addresses and MAC addresses.
- Log data is held online in LogDB (in the specified 'home' region) for a period of 90 days and then archived. Archived log data is deleted after twelve (12) months (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.

3.2 Cloud Access Security Broker (CASB):

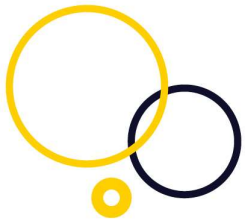
The CASB service uses the USS infrastructure, notably two databases - LogDB and CoreDB - for log data and policy/rule/configuration data respectively - described in clause 2 of this Module B.

3.2.1 **CASB Risks:**

- Although the use of https has increased dramatically a number of cloud applications still use the unencrypted http protocol. Information sent in requests to and from those applications is therefore unencrypted in clear text and may be intercepted.
- The Censornet CASB service in Inline Mode analyses all http and https requests made to the specific cloud applications included in the Cloud Application Catalog. The catalog comprises hundreds of business applications and thousands of user actions within those applications.
- The CASB service also includes an Application Programming Interface (**API**) Mode that uses and API Gateway and API Connectors to major cloud applications.

3.2.2 **Scope of Risk:**

- Our staff could access log information that contains details of user's cloud application activity.



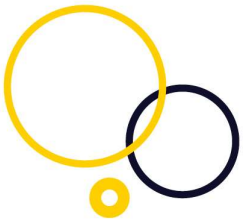
- Only a small number of our staff are involved in the administration of CASB systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores cloud application activity log data.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.2.3 **Input data that contains personal data – CASB:**

- Input data for the CASB service is comprised of all http and https cloud application requests and associated metadata. Metadata includes AD usernames, IP addresses, Real Names, MAC addresses, Email addresses and any captured application data. Request information is sent securely using ICAP to the Censornet cloud and compared against customer configured policy to determine whether the user action is allowed, blocked or logged. A final action is returned to the agent and/or gateway that results in the request being released to the target application or blocked (in Inline Mode).
- In Inline Mode each ICAP server stores requests temporarily on disk in a transaction log. The servers maintain a transaction log for every LogDB partition that they are actively handling requests for. A new transaction log is written every sixty (60) seconds and shipped to the appropriate LogDB server. The temporary log file is then deleted from the ICAP server.
- In API Mode events are written to a transaction file on the API Gateway and shipped every sixty (60) seconds to the appropriate LogDB server. The temporary log file is then deleted from the API Gateway.

3.2.4 **Output data that contains personal data – CASB:**

- Output data from the CASB service is comprised of log data relating to http and https cloud application requests. Log information includes AD



usernames, IP addresses Real Names, MAC addresses, Email addresses and any captured application data.

- Log data is held online in LogDB (in the specified 'home' region) for a period of 365 days and then archived. Archived log data is deleted after twelve (12) months (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.

3.3 Cloud Multi-factor Authentication (Cloud MFA):

The Cloud MFA service uses the USS infrastructure, notably two databases - LogDB and CoreDB - for log data and policy/rule/configuration data respectively - described in clause 2 of this Module B.

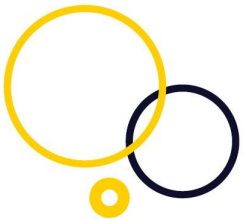
An additional copy of CoreDB is also replicated to Microsoft Azure (West Europe – Amsterdam) for failover and performance specifically for the MFA service.

With the exception of CoreDB, the majority of components within the Cloud MFA service only store data transiently whilst the user authenticates. Once authentication is complete (successful or failed) the data is deleted.

Lastly the service also includes the actual One Time Passcodes (**OTPs**) that are sent to users by SMS text message, email, using the Censornet mobile app, or a combination of these dispatch methods. For sensitive environments the Censornet app for iOS and Android provides full end-to-end encryption. OTPs are generated in real-time, are session specific to prevent phishing or man-in-the-middle attacks and are only valid for a short period of time.

3.3.1 **Cloud MFA Security Risks:**

- Cloud MFA presents the user with an additional challenge when authenticating to supported applications, services or systems to provide an additional level of identity assurance – and protection – beyond that offered by passwords alone.
- OTPs sent via configurable dispatch methods are highly secure and both generated in real-time and session specific. Even if an attacker were to



intercept an OTP they would be unusable outside of the session of the user that requested it.

- If organisations are concerned about the security of the OTP in transit, via SMS or email for example, then use of the Censornet mobile app is recommended as it offers true end-to-end encryption.

3.3.2 **Scope of Risk:**

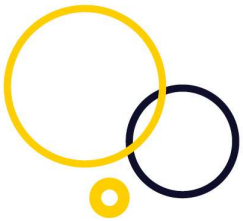
- Our staff could access log information that contains details of user's authentication (Cloud MFA) activity.
- Only a small number of our staff are involved in the administration of Cloud MFA systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores Cloud MFA activity log data.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.3.3 **Input data that contains personal data –Cloud MFA:**

- Input data for the Cloud MFA service is comprised of user authentication requests and associated metadata. Metadata includes Usernames, UPNs, Common Names (Real Names) and IP addresses.
- Requests are transiently held until authentication is complete (successful or failed) at which point all data is deleted.

3.3.4 **Output data that contains personal data –Cloud MFA:**

- Output data from the Cloud MFA service is comprised of authentication log data. Log information includes Usernames, UPNs, Common Names (Real Names) and IP addresses.
- Log data is held online in LogDB (in the specified 'home' region) for a period of 365 days and then archived. Archived log data is deleted after twelve (12)



months (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.

- The "Log Message Queue" keeps authentication log entries if the target LogDB is down. Otherwise entries are released as quickly as possible.
- "Auth Backend & Transmit" VMs keep transmission log entries (detailing what messages were sent to which phone numbers) for ninety (90) days. This data is only used for troubleshooting purposes.

3.4 MFA powered by IntelliTrust (MFA):

The MFA service uses the USS infrastructure, notably two databases - LogDB and CoreDB - for log data and policy/rule/configuration data respectively - described in clause 2 of this Module B.

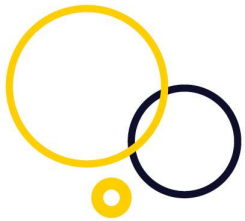
In addition an IntelliTrust database stores information to enable authentication requests to be processed resides on Amazon Web Services with locations in Frankfurt, Dublin and the US. The location of AuthDB is selected at the time of service provisioning.

With the exception of CoreDB, the majority of components within the MFA service only store data transiently whilst the user authenticates. Once authentication is complete (successful or failed) the data is deleted.

Lastly the service also includes the actual OTPs that are sent to users by SMS text message, email, using the Entrust Datacard IntelliTrust mobile app, or a combination of these dispatch methods. For sensitive environments the mobile app for iOS and Android provides full end-to-end encryption of Push Notifications. OTPs are generated in real-time and are only valid for a short period of time. Push Notifications are session specific to prevent phishing or man-in-the-middle attacks.

3.4.1 **MFA powered by IntelliTrust Security Risks:**

- MFA presents the user with an additional challenge when authenticating to supported applications, services or systems to provide an additional level of



identity assurance – and protection – beyond that offered by passwords alone.

- Push Notifications are highly secure and both generated in real-time and session specific.
- If organisations are concerned about the security of the OTP in transit, via SMS or email for example, then use of Push Notifications within the mobile app is recommended as it offers true end-to-end encryption.

3.4.2 **Scope of Risk:**

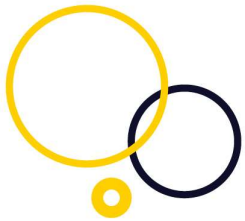
- Our staff could access log information that contains details of user's authentication (MFA) activity.
- Only a small number of our staff are involved in the administration of MFA systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores MFA activity log data.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.4.3 **Input data that contains personal data –MFA powered by IntelliTrust:**

- Input data for the MFA service is comprised of user authentication requests and associated metadata. Metadata includes Usernames, UPNs, Common Names (Real Names) and IP addresses.
- Requests are transiently held until authentication is complete (successful or failed) at which point all data is deleted.

3.4.4 **Output data that contains personal data –MFA powered by IntelliTrust:**

- Output data from the MFA service is comprised of authentication log data. Log information includes Usernames, UPNs, Common Names (Real Names) and IP addresses.



- Log data is held online in LogDB (in the specified 'home' region) for a period of 365 days and then archived. Archived log data is deleted after twelve (12) months (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.
- The IntelliTrust database stores log data online for 6 months in the specified data center (selected at provisioning time). Log data is then archived and deleted after thirty six (36) months. Archived data is stored on Amazon S3 stograge in the same data center as online log data.
- Internal system operation logs are only accessible to a small number of staff and used for troubleshooting only.

3.5 Email Security (EMS):

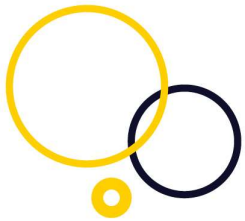
EMS from Censornet is a 100% cloud-based service that analyzes email traffic and removes unwanted or malicious messages.

The service scans all inbound (and outbound) messages for threats including malware and phishing attacks, and examines URLs embedded in messages protecting users from inappropriate or malicious web pages.

Organisations route email through Censornet's Cloud by changing their MX record.

We use world-class, highly accredited providers to deliver EMS that include Amazon, IBM and Microsoft. In Europe specific data centre locations include Frankfurt, Dublin and Amsterdam. Organizations choose which data centre or centres process their mail. In the UK data centre locations include London. In the US data centre locations include Wyoming, Texas and Virginia. In the UAE data centre locations include Dubai. Email messages flow through the infrastructure within the selected data centre(s) above and are checked for spam and viruses and other content. If the message is 'clean' it is logged and delivered to the customer's email server. The conversation with the customer's email server is also logged.

Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments.



Log data is stored in the same data centre that processes email traffic. Some log data may be replicated for reporting and visualization. The 'home' region selected at the time of account provisioning determines the location of this data.

During processing the message is written to disk. Once delivered to the customer's email server it is immediately deleted. This typically takes no more than a few seconds.

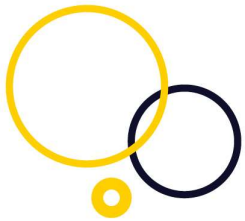
If a message is determined to be spam then the message may optionally be written to a quarantine where it is stored for thirty (30) days. Organization's may choose to delete spam rather than quarantine it. The quarantine is located specifically in the following data centres: Amsterdam (for UK and EU customers), Dallas TX (for US customers) and Dubai (for UAE customers).

3.5.1 **Email Risks:**

- It should be noted that email is generally sent unencrypted in clear text and routes through numerous network providers, systems and servers between sender(s) and recipient(s). Each of these providers, systems and servers may have a copy of the complete email message.
- The use of Transport Layer Security (**TLS**) to encrypt server to server transmission of email is becoming increasingly used. There is the option within EMS to use TLS for outbound email with specific domains that support it.
- For sensitive messages, including messages containing personal data, the use of a separate email encryption solution is recommended.
- It should be further noted that Censornet EMS only covers email sent or received externally. Internal messages sent between users is not processed by Censornet.

3.5.2 **Scope of Risk:**

- Our staff could access the message body (including file attachments) of email messages sent or received externally - if they are not encrypted - for the short time that they are written to disk and processed in the Censornet Cloud.



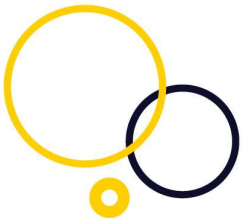
- Only a small number of our staff are involved in administration of EMS systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that processes and temporarily stores email messages.
- The same small number of our staff could access spam messages that are stored in a quarantine if the service is configured to quarantine messages determined to be spam.
- All service-related data is handled in strict accordance with Data Protection Legislation.

3.5.3 **Input data that contains personal data – EMS:**

- Input data for the EMS service is comprised of inbound and outbound email messages sent or received externally to or from the organization. Email messages are sent unencrypted in clear text unless a separate email encryption solution is used or TLS is enforced for outbound email sent to a specified domain.
- Email messages are stored, typically for a few seconds, during analysis and deleted immediately once delivered to your email server.

3.5.4 **Output data that contains personal data – EMS:**

- Output data from the EMS service is comprised of log data relating to inbound and outbound email messages sent or received externally. Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments.
- Depending on the configuration of the service output data may also include complete email messages that are determined during analysis to be spam messages, if the service is configured to quarantine spam emails rather than delete them. Quarantined messages are stored for thirty (30) days and then deleted.



- Log data is held online for ninety (90) days and then archived. Archived log data is deleted after twelve (12) months (but may be downloaded on demand by customers at any time prior to deletion).

3.6 Email Backup (Archiving) & Emergency Inbox:

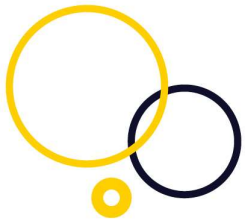
Email Backup (Archiving) and Emergency Inbox are optional additional services that may be purchased alongside EMS.

3.6.1 **Email Backup (Archiving)**

- Email Backup (Archiving) stores copies of complete email messages for a specified period of time up to seven (7) years. A portal provides the ability to search messages by time, sender, recipient, subject and keyword(s).
- All inbound messages processed by EMS are backed up to two Microsoft Azure Blob Storage instances. Messages are stored as full .EML files containing all email headers and body, including any file attachments. If outbound email is also routed through Censornet outbound messages will also be stored.
- For customers located in the UK and Europe the Microsoft Azure instances are West Europe (Netherlands) and Northern Europe (Ireland).
- Data stored on Azure Blob Storage is encrypted at rest.

3.6.2 **Emergency Inbox**

- This service provides an 'Emergency Inbox' for users in the event that the primary email service (or email server) fails.
- In the event of an email outage users can log into a web portal and view (read) and reply to messages. Users can also compose new email messages.
- The Emergency Inbox is built on the Email Backup (Archive) described in 3.6.1 above.



3.7 Compliant Email Archive (CEMA):

Compliant Email Archiving is an optional additional service that can be purchased separately or combined with the Email Security (EMS) service.

The Compliant Email Archiving service stores copies of journaled email messages securely. Emails are transferred into the archive either via SMTP from the customer's mail server, or collected via a polling process from a dedicated journal mailbox on the on premise mail server via Exchange Web Services (EWS), or via IMAP connections.

Mail servers supported include Office 365 Exchange Online, Exchange 2007/10/13/16/19, and Lotus Domino.

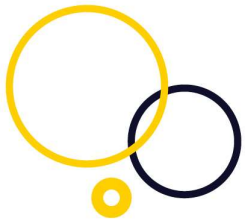
Every archived message is given a unique ID, digitally fingerprinted, encrypted, compressed, timestamped, fully indexed and written to the storage system. All messages at rest are encrypted using 256-bit Advanced Encryption Standard (AES-256)

Data is stored in separate storage repository buckets per tenant / customer. Storage used is Amazon S3 storage buckets within the Frankfurt data center.

Each tenant repository can have its own unique encryption key for the archived data. By default each tenant will use the Global Encryption key which is set up during account creation.

By default, the solution keeps the emails indefinitely. Specific retention periods are available on request.

A secure https portal provides the ability to search the archived messages by date, sender, recipient, keywords in the body and/or attachments. Access to the portal can be within Outlook via a web enabled folder or through any mainstream web browser.



The following pre-defined user roles are available:

- Standard / Basic (LDAP) Users – access to their own nominated email addresses
- Privileged Users – eDiscovery users who can access all/subset of the archived emails, with comprehensive audit trails showing which emails have been searched for and opened
- Data Guardian Users – Date Guardian users have access to audit trails and are able to review Privileged User searches
- Privileged & Delete Users – similar to Privileged Users, with the extended functionality to be able to delete emails from the archive in an audited manner (for example within a 'Right To Be Forgotten' process)
- Administrators – no access to search the archive but can administer accounts and basic settings.

The archiving platform is delivered as a high availability clustered environment layered with Kubernetes and Zookeeper to seamlessly orchestrate archiving activity at very high scale.

The environment is load balanced enabling for load to be shared across the environment.

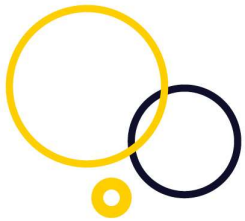
3.7.1 **Scope of Risk**

- Only a small number of our staff are involved in administration of CEMA systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that processes and stores email messages.
- Our staff could access the message body (including file attachments) of email messages received - if they are errored and not encrypted - for the short time they reside in the error queue prior to being processed into the Censornet Archive Cloud.

- All service-related data is handled in strict accordance with Data Protection Legislation.

3.8 Autonomous Security Engine (ASE):

The Autonomous Security Engine is an integral part of the Censornet USS platform that shares security state data, security event data, and threat objects across some or all services. Threats seen by one service are proactively managed and blocked by other services to prevent attacks in real-time.



4. Common security considerations across all Services:

4.1 External communication connections:

4.1.1 Infrastructure elements associated with delivery of USS and individual services resides within the data centres described above. Our staff have remote access to these environments but all connections are protected using Secure Sockets Layer (**SSL**) encryption (Remote Desktop Protocol and PowerShell), or over Secure Sockets Shell.

4.1.2 Connections to the environments are tightly restricted and only allowed from a list of static IP addresses.

4.2 Authorization and access control:

4.2.1 Access to production systems and associated data is strictly limited to our staff that require that access to perform their role. This includes a small number of staff involved in administration of systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons. No other Censornet staff have any access to the infrastructure.

4.2.2 The Censornet Joiners Movers Leavers process ensures that authorizations are reviewed whenever an employee joins, changes role, or leaves employment.

4.2.3 In addition to passwords other forms of access control are used extensively throughout the environment – including two-factor authentication, wherever it is available, to protect user accounts.

4.3 Control of rejected access attempts:

4.3.1 All login attempts – both successful and unsuccessful – are logged. All two-factor authentication events – both successful and unsuccessful – are logged.

4.3.2 Wherever possible user accounts are locked out for thirty (30) minutes if more than 3 unsuccessful login attempts are identified.

4.4 **Logging:**

4.4.1 All User – and particularly privileged (admin) user activity – carried out by our staff on systems and servers is logged.

4.4.2 All User activity within the admin interface and Censornet Unified Security Service portal is also logged. Log data is held for thirty (30) days and then deleted.

4.5 **Home offices:**

4.5.1 A small number of our staff have company provided PCs that are configured to use Cisco VPNs for remote access to infrastructure to enable them to troubleshoot and resolve service issues or to assist customers out of hours. The use of home or private PCs is strictly prohibited.

4.5.2 All connections are protected using SSL encryption.

4.6 **Locations for processing:**

4.6.1 Censornet has the following office locations within the UK:

- Basingstoke
- Bristol
- Lerwick, Shetland

ANNEX B - Sub-processors

As at the date of this Agreement, we use the following Sub-processors:

Amazon EC2: Amazon Web Services Inc, 410 Terry Ave North, Seattle, WA, 98109-5210, USA. The Supplier has selected either a specific EU/ESS Datacenter location, or a EU/ESS region (eg Western Europe, Northern Europe) depending on the Sub-Processor options provided at the time of provisioning the systems.

ApriorIT: (VRSoft LTD) Headquarters - 34B Kniazia Volodymyra Velykoho St., Dnipro, 49000, Ukraine.

Datadog, Inc.: Headquarters - 620 8th Avenue, 45th Floor, New York, NY 10018, USA.

Entrust DataCard Corp: 1187 Park Place, Minneapolis, MN 55379, USA.

Functional Software, Inc. dba Sentry: 132 Hawthorne Street, San Francisco, CA 94107, USA.

IBM Cloud: Corporate headquarters - IBM Corporation, 1 New Orchard Road, Armonk, New York 10504-1722, USA. The Supplier has selected either a specific EU/ESS Datacenter location, or a EU/ESS region (eg Western Europe, Northern Europe) depending on the Sub-Processor options provided at the time of provisioning the systems.

Lastline Inc.: 203 Redwood Shores Parkway, Suite 500, Redwood City, CA 94065, USA. *Please note this Sub-processor is only used if the 'Sandbox Level 2' add on is purchased/used with EMS.*

Microsoft Azure: Microsoft Ireland Operations Ltd, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland. The Supplier has selected either a

specific EU/ESS Datacenter location, or a EU/ESS region (eg Western Europe, Northern Europe) depending on the Sub-Processor options provided at the time of provisioning the systems.

SendGrid, Inc. (part of Twilio): 1801 California Street, Suite 500, Denver, Colorado 80202, USA.

Sorry App Limited: Building 1, Old Station Business Park, Petworth, West Sussex, UK, GU28 0JF. Please *note this Sub-processor is only used if Customers subscribe to system status updates/notifications.*

Twilio Inc.: 375 Beale Street, Suite 300, San Francisco, CA 94105, USA. *Please note this Sub-processor is only used if MFA is enabled on portal (USS) logins.*

Vade Secure Inc.: 180 Sansome Street, Floor 2 – San Francisco, CA 94104, USA. *Please note this Sub-processor is only used if Email Security is purchased/used.*

ANNEX C – Processing Details

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- Customers, Clients and Prospects (including their staff)

Categories of data

The personal data transferred concern the following categories of data (please specify):

- Basic personal data (for example street name and building number or name (address), postal code, city, country, mobile phone number, first name, last name, initials, email address, domain and related data);
- Authentication data (for example user name, password, audit trail);
- Contact information (for example addresses, email, phone numbers, website address);
- Device identification / Unique identification numbers (for example IP addresses, MAC addresses, logical tag);
- Commercial Information (subscription (license) information, purchase history, payment history);
- Location data (for example, geo-location network data);
- Email activity (inbound and outbound email messages, including attachments);
- Internet activity (for example browsing activity, cloud application activity);
- Any other personal data identified in Article 4 of the GDPR.

Summary of Data Processed (input / output data) by Service:

Service	Input Data	Output Data
Web Security (WS)	• All http and https web requests and associated metadata	• Log data relating to http and https web requests. Log information includes

	• Metadata includes Active Directory (AD) usernames, IP addresses and MAC addresses	AD usernames, IP addresses and MAC addresses
Cloud Application Security (CASB)	• All http and https cloud application requests and associated metadata • Metadata includes AD usernames, IP addresses, Real Names, MAC addresses, Email addresses and any captured application data	• Log data relating to http and https cloud application requests. Log information includes AD usernames, IP addresses Real Names, MAC addresses, Email addresses and any captured application data.
Cloud MFA (Cloud MFA)	• User authentication requests and associated metadata. Metadata includes Usernames, UPNs, Common Names (Real Names) and IP addresses • Mobile phone numbers	• Authentication log data. Log information includes Usernames, UPNs, Common Names (Real Names) and IP addresses
MFA Powered by IntelliTrust (MFA)	• User authentication requests and associated metadata. Metadata includes Usernames, UPNs, Common Names (Real Names) and IP addresses • Mobile phone numbers	• Authentication log data. Log information includes Usernames, UPNs, Common Names (Real Names) and IP addresses
Email Security (EMS)	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization	• Log data relating to inbound and outbound email messages sent or received externally. Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments
Email Back Up Emergency Inbox Compliant Email Archive (CEMA)	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- None

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Data processing operations are summarised as:

- Receiving data, including collection and recording
- Holding data, including storage, organisation and structuring
- Updating data, including adaptation, alignment and combination
- Computer processing of Personal Data, including data transmission, data retrieval, data access, and network access to allow data transfer if required
- Protecting data, including restricting, encrypting, and security testing.

Censornet and Censornet's Sub-processors will use and otherwise process Personal Data only in accordance with and as described in the Master Services Agreement (MSA) and for Censornet's legitimate business operations related to delivery of the Services to Customers.

<u>Processing to Provide Services</u>

A Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Ongoing improvement (making improvements to performance, productivity, reliability, protection offered, and security).

Processing for Censornet's Legitimate Business Operations

"Censornet's legitimate business operations" consist of the following, each as related to delivery of the Services to Customers: (1) billing and account management; (2) internal reporting and business planning (e.g., forecasting, revenue, capacity planning, product strategy); (3) combatting fraud, cybercrime, or cyberattacks that may affect Censornet; (4) financial reporting and compliance with legal obligations.

ANNEX D – Security Measures

Description of the technical and organisational security measures implemented by the data importer:

Censornet:

The data importer has implemented and will maintain appropriate technical and organisational measures, internal controls, and information security measures intended to protect Customer Data and Personal Data, as defined in this MSA, against accidental loss, destruction, or alteration; unauthorised disclosure or access; or unlawful destruction. The technical and organisational measures set forth in Annex A of Module B of this MSA are hereby incorporated into this Annex D.

Censornet's Sub-processors:

The Sub-processors detailed in Annex B of Module B of this MSA all implement and maintain appropriate technical and organisational measures. Details of each Sub-processors' security measures can be found at: https://help.clouduss.com/legal/sccs .

Module C – Terms for Unified Security Service (USS) including Web Security (WS), Cloud Application Security (CASB), Cloud Multi-Factor Authentication (Cloud MFA), MFA powered by IntelliTrust (MFA), Compliant Email Archive (CEMA) and Autonomous Security Engine (ASE)

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 9.

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. IT IS IMPORTANT THAT YOU UNDERSTAND AND GIVE YOUR CONSENT TO SUCH INTERCEPTION WHICH, BUT FOR THIS CONSENT, WOULD BE IN BREACH OF THE COMPUTER MISUSE ACT 1990. 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 and scope of licence:

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 4, make one copy of the non-hosted USS Software components for back-up purposes only.

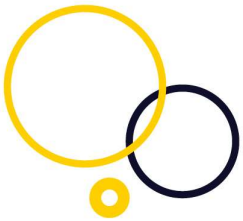
2. Limited warranty:

2.1 We warrant that:

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

(b) that the Description correctly describes the operation of the USS Software in all material respects, for a period of ninety (90) 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. Web Security AV / Gateway Anti-malware ("WS AV")

3.1 This Clause 3 ("WS AV Terms") governs use of the Bitdefender software distributed by Censornet as an optional add-on to the WS Agent and Gateway software.

3.2 Limited License:

3.2.1 Subject to the WS AV Terms, Censornet grants to you a non-transferable, non-sublicensable, non-exclusive license to use the object code form of the software for your own use, but only in accordance with the technical specification documentation generally made available with the software and these WS AV Terms. "Software" shall also include any documentation and any support and maintenance releases of the same software provided to you.

3.2.2 You are not allowed to create derivate technologies or to use to offer services derived from the software.

3.3 Application Software:

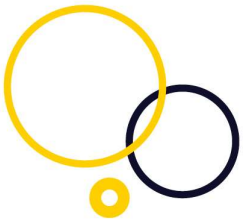
You may install and use the software, on as many computers as necessary with the limitation imposed by the total number of licensed Users. You may make one additional copy for back-up purpose.

3.4 Restrictions:

3.4.1 You shall not (and shall not allow any third party to): (a) decompile, disassemble, or otherwise reverse engineer the software or attempt to reconstruct or discover any source code, underlying ideas, algorithms, file formats or programming interfaces of the software by any means whatsoever (except and only to the extent that applicable law prohibits or restricts reverse engineering restrictions, and then only with prior written notice to the respective owners;); (b) distribute, sell, sublicense, rent, lease or use the software (or any portion thereof) for time sharing, hosting, provision of services or like purposes; (c) remove any product identification, proprietary, copyright or other notices contained in the software; (d) modify or create a derivative work of any part of the software; or (e) publicly disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the software. You may not permit third parties to benefit from the use or functionality of software, except as and only to the extent explicitly permitted by the licensing terms, governing use of the third party software.

3.5 Ownership:

3.5.1 Notwithstanding anything to the contrary contained herein, except for the limited license rights expressly provided herein, Censornet and its suppliers have and will retain all rights, title and interest (including, without limitation, all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the software and all copies, modifications and derivative works thereof. You acknowledge that you are obtaining only a limited license right to the software and that irrespective of any use of the words "purchase", "sale" or like terms hereunder no ownership rights are being conveyed to you under these WS AV Terms or otherwise. You acknowledge that Bitdefender has a substantial interest in the software and that Bitdefender is a third party



beneficiary to these WS AV Terms, with the understanding that rights, titles and interest in and to certain third party software identified are owned by their respective owners.

3.5.2 If requested, you shall certify in writing the number of Censornet Agents and/or Gateways you are using. You agree that no more than once annually your use of the software may be audited by Censornet or Bitdefender (or an independent auditor working on such party's behalf) during normal business hours upon reasonable advance written notice for the purpose of verifying your compliance with these WS AV Terms.

3.6 Confidentiality:

3.6.1 You acknowledge that, you may obtain information relating to the software or Bitdefender, including, but not limited to, any code, technology, know-how, ideas, algorithms, testing procedures, structure, interfaces, specifications, documentation, bugs, problem reports, analysis and performance information, and other technical, business, product, and data. You shall not disclose such confidential information to any third party or use it for any purpose other than the use of the software as licensed under these WS AV Terms.

3.7 Warranty Disclaimer:

THE SOFTWARE IS PROVIDED "AS IS" AND NO WARRANTIES ARE MADE TO ANY PERSON OR ENTITY WITH RESPECT TO THE SOFTWARE OR ANY SERVICES AND CENSORNET DISCLAIMS ON ITS OWN BEHALF AND THAT OF ITS LICENSORS, INCLUDING BITDEFENDER, ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

3.8 Limitation of Damages and Remedies:

3.8.1 IN NO EVENT SHALL CENSORNET OR ITS LICENSORS BE LIABLE UNDER CONTRACT, TORT, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE SOFTWARE. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, THE TOTAL LIABILITY OWING TO YOU, INCLUDING BUT NOT LIMITED TO DAMAGES OR LIABILITY ARISING OUT OF CONTRACT, TORT, BREACH OF WARRANTY, INFRINGEMENT OR OTHERWISE, SHALL NOT IN ANY EVENT EXCEED THE FEES PAID BY YOU WITH RESPECT TO THE SOFTWARE. NEITHER CENSORNET NOR ITS LICENSORS SHALL BE LIABLE FOR

LOSS OR INACCURACY OF DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, SYSTEM DOWNTIME, FAILURE OF SECURITY MECHANISMS, GOODWILL, PROFITS OR OTHER BUSINESS LOSS, REGARDLESS OF LEGAL THEORY, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.8.2 THE PARTIES AGREE THAT THE LIMITATIONS OF THIS SECTION ARE ESSENTIAL AND THAT YOU WOULD NOT BE PERMITTED TO USE THE SOFTWARE ABSENT THE TERMS OF THIS SECTION. THIS SECTION SHALL SURVIVE AND APPLY EVEN IF ANY REMEDY SPECIFIED IN THESE WS AV TERMS SHALL BE FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

3.8.3 THIS SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

3.9 Export Compliance

You acknowledge that the software may be subject to export restrictions by the United States government and import restrictions by certain foreign governments. You shall not and shall not allow any third-party to remove or export from the United States or allow the export or re-export of any part of the software or any direct product thereof: (i) into (or to a national or resident of) any embargoed or terrorist-supporting country; (ii) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals; (iii) to any country to which such export or re-export is restricted or prohibited, or as to which the United States government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval; or (iv) otherwise in violation of any export or import restrictions, laws or regulations of any United States or foreign agency or authority. You agree to the foregoing and warrant that you are not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list. The software

is further restricted from being used for the design or development of nuclear, chemical, or biological weapons or missile technology, or for terrorist activity, without the prior permission of the United States government.

3.10 Government Users:

The software is commercial computer software. If the user or licensee of the software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by these WS AV Terms in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The software was developed fully at private expense. All other use is prohibited.

3.11 Termination and Survival:

Upon any termination of these WS AV Terms, you shall immediately cease use of the software and remove all software from your systems. The terms set forth in the sections entitled Restrictions, Ownership, Confidentiality, Warranty Disclaimer, Limitation of Damages and Remedies shall survive any termination of these WS AV Terms.

4. Fair Usage – Cloud MFA:

4.1 The Cloud MFA service includes the option to send OTPs via text message (SMS). The cost of sending passcodes over SMS is included in the Subscription Fees for the Cloud MFA service but is subject to this section. This is to ensure that your use of SMS is not excessive and kept within reasonable and sensible limits.

4.2 The maximum usage per month is equivalent to four (4) OTPs per user per day.

4.3 If you exceed this limit we reserve the right to apply an additional charge to cover the amount by which you exceeded the allowance.

4.4 We complete periodic checks on SMS usage throughout the Term and will inform you if your usage appears higher than average, before any additional charges are incurred, and discuss alternatives to sending OTPs over SMS (for example through use of the Censornet MFA app for iOS and Android devices).

5. Fair Usage – Web and CASB

5.1 Web Security and CASB (Inline Mode) are licensed by number of users.

5.2 Below, the following terms are used:

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

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

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.

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.

5.3 Fixed policy:

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

5.4 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.

5.5 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 D – 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 ESS 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 9.

IF YOU 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. IT IS IMPORTANT THAT YOU UNDERSTAND AND GIVE YOUR CONSENT TO SUCH INTERCEPTION WHICH, BUT FOR THIS CONSENT, WOULD BE IN BREACH OF THE COMPUTER MISUSE ACT 1990. 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 and scope of licence:

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

Module E – Terms for Support Services

1. Standard Support (Level 1):

1.1 Standard Support (Level 1 Support) is provided online via the Censornet website. Online Customer support for Censornet services is available Monday to Friday, 8.00 am to 5.00pm UK time ("**Standard Support Hours**").

1.2 You can open a support ticket at: https://www.censornet.com/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: https://www.censornet.com/support/.

2. Extended Support Levels:

2.1 Level 2 Support

2.1.1 Level 2 Support is available Monday to Friday, 8.00am to 5.00pm UK time. In addition to Online Support, Live Chat via the Censornet 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.

2.1.2 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:

3.1 Level 1 and Level 2 Support customers can send an emergency support email to: support@censornet.com 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 (see below). Normal support channels should be used for non-critical requests. Please see below for details of how Censornet classifies the support tickets received.

4. Issue Levels:

4.1 The following table provides a description of the different issue categories, based on their severity and impact, that Censornet 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 (High)	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 (Medium)	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:

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

Severity Level	Hours (GMT)	Standard Support Target Response
Priority 1 (Critical)	8 AM – 12 AM*	< 4 Business Hours email only
Priority 2 Degraded (High)	8 AM – 12 AM*	< 6 Business Hours email only
Priority 3 General (Medium)	8 AM – 12 AM*	Next Business Day (NBD) email only

*Monday to Friday

5.2 Please note that the Customer is responsible for notifying Censornet support as soon as possible in the event of a critical or high service issue.

Module F – Service Level Agreement (SLA)

1. Introduction:

1.1 We are committed to providing top quality service levels in respect of all Censornet 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 Censornet in respect of the reliability of the Service(s) provided, and our response times. Appendix 1 to 4 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 4.

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 our current privacy policy which can be found at https://www.censornet.com/privacy-policy/

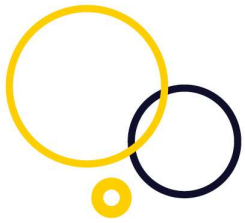
2.2 We reserve the right to amend any of these documents at any time without notice.

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:

- to trial or evaluation Customers;
- where you have used the cloud service for a period of thirty (30) days or less;
- where you are not up to date on payment of your Subscription Fees for the Service(s) at the time of the Claimed Outage;



- 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;
- where you have failed to report the unavailability in accordance with the procedure detailed below;
- where the cloud service is incorrectly configured by you;
- where you provide incorrect or inaccurate information to us;
- where your applications, equipment or internet connection has failed;
- where the Service(s) are not available due to system administration, commands or file transfers performed by you;
- where you are misusing the Service(s) or are otherwise in violation of the MSA;
- 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;
- where there is a network unavailability outside of our controlled systems (servers, hardware, and associated software) that are responsible for delivering the cloud service;
- where there are problems with your routing infrastructure (eg identity provider or secure web proxy of a third party);
- for hosted email security, where an account is not configured to use two or more co-location sites (clusters);
- 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);
- where the failure of meeting the terms of this SLA is based upon reasons beyond our reasonable control;
- where there has been a violation by you, your personnel or anyone engaged by you of the Computer Misuse Act; or
- 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:

- Email Security Service ("**EMS**")
- Web Security Service ("**WS**")
- Cloud Application Security ("**CASB**")
- Multi-Factor Authentication ("**Cloud MFA**")
- MFA powered by IntelliTrust ("**MFA**")

Known all together as "**the Services**".

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

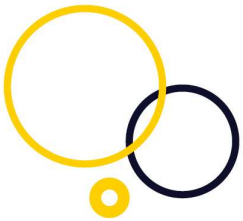
5. Service Standards:

5.1 The service availability for the Services listed in clause 4.1 above is **99.999%** (unless otherwise stated in the appendices to this MSA).

6. Service Credits:

6.1 The following terms and definitions are used:

"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.



"**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.

"Measurement Period" means the month in which the Claimed Outage occurred.

"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 5.1 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:

8.1 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:

9.1 We reserve the right to amend or cancel this SLA from time to time, in its sole discretion, with or without notice.

Appendix 1 - Email Security Service ("EMS")

1. Definitions:

1.1 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:

2.1 Our EMS will be Available 99.999% of the time.

3. Virus Detection:

3.1 We will protect you from infection by 100% of all Known Viruses contained inside email that has passed through the EMS. 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, Censornet will credit the Customer with one (1) day's Service Credit if the claim is approved.

Appendix 2 - Web Security Service ("WS")

1. Definitions:

1.1 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.

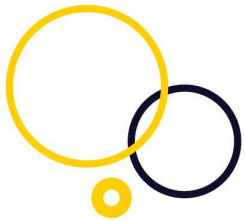
2. Availability:

2.1 Our WS will be Available 99.999% of the time.

3. Virus Detection:

3.1 For Customers subscribing to the optional additional Gateway Anti-virus module we will protect you from infection by 100% of all Known Viruses contained inside web content that has passed through our Cloud Gateway deployed as part of the WS.

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 SSL 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:

1.1 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.

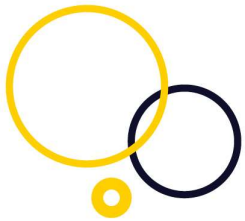
2. Availability:

2.1 Our CASB will be Available 99.999% of the time.

3. Virus Detection:

3.1 For Customers subscribing to the optional additional Gateway Anti-virus module we will protect you from infection by 100% of all Known Viruses contained inside cloud application content that has passed through our Cloud Gateway deployed as part of the CASB.

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 SSL 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 4 – Multi-factor Authentication ("Cloud MFA")

1. Definitions:

1.1 The following terms are used:

"**Availability**" or **"Available"**is defined as the ability to receive and process requests and generate and dispatch One Time Passcodes (OTPs) for user authentication to MFA protected services, systems and applications.

"**Service Unavailability**" is defined as the inability of the MFA to receive and process requests and generate and dispatch OTPs substantially in accordance with the published online Documentation for the MFA, and measured during any given calendar month. Service Unavailability does not include failures of networks or systems (servers, hardware and associated software) outside of our control that are involved in the delivery of OTPs (including but not limited to CPaaS providers used for OTP delivery by SMS or Email Service Providers used for delivery of OTPs by email).

2. Availability:

2.1 Our Cloud MFA service will be Available 99.999% of the time.

Appendix 5 – Multi-factor Authentication powered by IntelliTrust ("MFA")

1. Definitions:

1.1 The following terms are used:

"**Availability**" or **"Available"** is defined as the ability to use the service to authenticate user identity in order to gain access to protected services, systems and applications.

"**Service Unavailability**" is defined as a state during which authorized users are unable to use the Cloud Components to authenticate user identity in order to gain access to protected services, systems and applications. Service Unavailability does not include any unavailability that results from: (a) suspension or termination of the Service pursuant to the terms of the Agreement, (b) factors outside of our reasonable control, including without limitation, any force majeure event, internet accessibility problem beyond our ISP environment, network, software, equipment or other technology, (c) the licensed software hosted by you, and (d) any maintenance window for scheduled routine system maintenance.

2. Availability:

2.1 Our MFA powered by IntelliTrust service will be Available at least 99.9% during each calendar month.