Software as a Service Addendum

This Software as a Service Addendum ("**Addendum**") is made between you, the Customer ("**Customer**" or "**You**") and Provider and is made part of the agreement ("**Agreement**") between you and the Provider that references this Addendum. Defined terms used in this Addendum that are not otherwise defined herein shall have the meaning set forth in the Agreement.

1. **Definitions.** Capitalized terms not defined in context or in the Agreement shall have the meanings assigned to them below:

(a) "***Appropriate Safeguards***" shall mean appropriate safeguards pursuant to Art. 46 GDPR, such as binding corporate rules or standard data protection clauses adopted by the EU Commission, like the Standard Contractual Clauses defined below.

(b) "***Controller***", "***Data Subject***", "***Personal Data***", '***processing***", "***Personal Data Breach***", ***"Processor***", ***"Supervisory Authority***" shall have the meaning set forth in Article 4 of the GDPR.

(c) "***Customer Personal Data***" shall mean Personal Data that Customer provides to Provider (in Provider's capacity as a Processor) through Customer's use of SaaS Software.

(d) ***"Data Protection Laws"*** means all laws and regulations, including laws and regulations of the European Union such as the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the ***"GDPR***"), and, as the case may be, of any other country which has implemented data protection principles similar to the GDPR and has been recognized by the European Commission as providing an adequate level of protection, applicable to the processing of Personal Data.

(e) ***"SaaS Environment"*** means the systems to which Customer is provided access in connection with its use of the SaaS Software.

(f) ***"Standard Contractual Clauses"*** means the unchanged standard contractual clauses, published by the European Commission (available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914), reference 2021/914 or any subsequent final version thereof, which shall automatically apply.

(g) "***Sub-processor***" means Provider Affiliates and third parties engaged by Provider or Provider's Affiliates in connection with the SaaS Software and which process Personal Data in accordance with this Addendum.

2. **SaaS Provisions.**

(a) **Data.** Customer may store data on the SaaS Environment. Customer is solely responsible for collecting, inputting, validating and updating all Customer data stored in the SaaS Environment. Customer represents and warrants that it has obtained all rights, authorizations and consents necessary to use and transfer all Customer and/or third-party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents or authorizations from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other location for access by the SaaS Software, Customer will be deemed to have given its consent and/or authorization for access by Provider.

(b) **Conduct.** When using the SaaS Software, Customer shall not: (i) use the SaaS Software in breach of applicable law and in particular Customer will not transmit any content or data that is unlawful or infringes any intellectual property rights of third parties; (ii) circumvent or endanger the operation or security of the SaaS Software or attempt to probe, scan or test the vulnerability of the SaaS Software, the SaaS Environment, or a system, account or network of Provider or any of Provider's customers or suppliers; (iii) transmit unsolicited bulk or commercial messages; or (iv) intentionally distribute worms, Trojan horses, viruses, corrupted files or any similar items. Customer shall cooperate with Provider's reasonable investigation of SaaS Environment outages, security issues, and any suspected breach of this Section, and shall, at its expense, defend Provider and its Affiliates from any claim, suit, or action by a third party (a ***"Third Party Claim"***) alleging harm to such third party caused by Customer's breach of any of the provisions of this Section. Additionally, Customer shall pay any judgments or settlements reached in connection with the Third Party Claim as well as Provider's costs of responding to the Third Party Claim.

(c) **Suspension.** Provider can temporarily limit or suspend Customer's access to the SaaS Software to prevent damages, if it is sufficiently probable that the continued use of the SaaS Software may result in harm to the SaaS Software, other Provider customers, or the rights of third parties in such a way that immediate action is required to avoid damages or Customer is in breach of the *Conduct* section above. Provider will notify Customer of the limitation or suspension without undue delay. If circumstances allow, Customer shall be informed in advance in writing or by email. Provider will limit the suspension or limitation in time and scope as reasonably possible under the circumstances and will promptly restore access, and notify Customer of the restoration, when the issue causing the suspension or limitation has been resolved.

(d) **Availability.** Provider will make commercially reasonable efforts to make the SaaS Software available twenty-four hours a day, seven days a week except for scheduled maintenance, the installation of updates, those factors that are beyond the reasonable control of Provider, Customer's failure to meet any minimum system requirements communicated to Customer by Provider, and any breach of the Agreement or this Addendum by Customer that impacts the availability of the SaaS Software. Provider shall provide reasonable advance notice to Customer of any scheduled maintenance.

3. SaaS Security.

(a) **General Security Policies**. Provider takes the security and confidentiality of our Customer's data (including Personal Data) seriously. Provider is committed to maintaining and improving its information security practices and minimizing exposure to security risks. To that end, details on Provider's information security practices, data breach response policies, technical and organizational measures, and software development security practices are available at: www.oneidentity.com/legal/security.aspx (collectively "***Security Site***"). Customer agrees that Provider may modify its Security Site so long as it does not materially decrease the overall level of protection provided.

(b) **Data Center Security and Locations**. Provider uses commercial hosting providers to host the SaaS Environment. The applicable hosting provider for the SaaS Environment will be identified as a Sub-Processor. Provider will only use hosting providers that meet industry standard security requirements and undergo independent assessments of their security procedures such as Service Organization Control (SOC) audits, SSAE 18 audits, and/or ISO certifications. Provider shall provide copies of the hosting providers' certifications upon request. Customer will be provided the option of selecting which geographic region the SaaS Environment will be hosted in upon initial configuration of the SaaS Software. Once selected, Provider shall not change the geographic region without Customer's prior consent.

(c) **Data Secrecy.** Provider will only use personnel who are informed of the confidential nature of data deemed "confidential" under the Agreement, including specifically the Customer Personal Data, to process any such data. Provider will require all Provider personnel supporting the SaaS Software in accordance with this Addendum and the Agreement to execute confidentiality agreements relating to the protection of data, including Customer Personal Data. Provider shall ensure that such confidentiality obligations survive the termination of employment for any such personnel. Provider will regularly train individuals having access to data, including Customer Personal Data in data security and data privacy requirements and principles.

(d) **Limited Processing and Disclosure.** Provider may process and disclose data, including Customer Personal Data (i) to affiliated entities, for purposes consistent with the Agreement and in accordance with the terms of this Addendum or (ii) as required by Union or Member State law to which the processor is subject, including in response to a subpoena, judicial or administrative order; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4. Cooperation. Except as prohibited by law or contract, Provider shall, upon Customer's request, reasonably cooperate with Customer on Data Subject requests and will promptly notify Customer if Provider receives a request from a Data Subject whose data has been provided under this Agreement either (a) requesting the right to access to, correct, amend or delete that Data Subject's Personal Data; (b) opposing the processing of her or his Personal Data under this Agreement; and/or (c) wishing to exercise her or his right to portability or to be forgotten under GDPR. Provider shall not respond to such Data Subject's request without Customer's prior written approval, except in order to confirm that such request is properly directed to Customer.

5. Audit Rights. Upon Customer's request and subject to the confidentiality obligations of the Agreement, Provider will make available to Customer information reasonably necessary to demonstrate its compliance with the obligations under this Addendum and allow for and contribute to audits, including inspections, conducted by Customer (or its third party auditor), at Customer's expense, in relation to the Processing of the Personal Data by Provider.

6. International Data Transfers. Where the provision of the SaaS Software and associated services involves the transfer of Personal Data, that is either subject to GDPR or to applicable Data Protection Laws, to a country or countries that are not recognized by the European Commission under Article 45 of GDPR as countr[ies] providing adequate data protection ("***Third Country***") and where any required adequacy means under GDPR or applicable Data Protection Laws can be met by entering into the Standard Contractual Clauses, then Provider (or a Provider Affiliate on its behalf) has entered into the Standard Contractual Clauses with each Sub-processor as the data importer. Module 3 (Processor to Processor) of the Standard Contractual Clauses shall apply to such transfers. For all purposes relating to such transfers the Appendix to this Addendum shall also constitute the Appendix to the Standard Contractual Clauses.

7. Sub-processors.

(a) Customer acknowledges and agrees that Provider may retain Sub-processors in connection with the provisioning of the SaaS Software.

(b) Provider shall execute the appropriate written agreements with Sub-processors in accordance with the provisions of this Addendum and the instructions herein between Customer and Provider. The same data protection obligations as set out in this Addendum shall be imposed on any Sub-processors.

(c) Provider is responsible for any breaches of this Addendum to the extent caused by Sub-processors retained by Provider.

(d) Provider maintains lists of Sub-processors per product available to Customer at https://support.oneidentity.com/subprocessor. At least ten (10) business days before authorizing any new Sub-processor to access Personal Data, Provider will update the list of Sub-processors and provide Customer with a mechanism to obtain notice of that update. Where Provider is Processor, the following terms apply:

(i) If Customer does not approve of a new Sub-processor, then Customer may terminate any subscription for the affected SaaS Software without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval.

(ii) After termination as described immediately above, Customer shall remain obligated to make all payments required under any Order or other contractual obligation and shall not be entitled to any refund or return of payment from the Partner and/or Provider.

8. **Personal Data Breach Notification.** In addition to the obligations set forth in the Security Site, Provider will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Provider may provide such information in phases as it becomes available. Provider agrees to make good faith efforts to identify the cause of such Personal Data Breach and take such steps as Provider deems necessary and reasonable in order to remediate the cause of the Personal Data Breach to the extent the remediation is within Provider's reasonable control.

9. **Return and Deletion of Customer Personal Data.**

(a) Customer shall notify Provider at least 30 (thirty) days before the expiration or earlier termination of the SaaS Term for any reason of its intent to have the Customer Personal Data returned to Customer or deleted. If requested to return Customer Personal Data, Provider shall return Customer Personal Data to the extent allowed by applicable law in a commonly used format.

(b) Unless Customer requests Customer Personal Data be returned, following termination of the SaaS Term, Provider shall delete Customer Personal Data held by Provider except to the extent necessary to allow Provider to comply with legal or regulatory orders or requirements.

10. **Data Protection Impact Assessment.** Provider shall provide Customer with reasonable cooperation and assistance as needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the SaaS Software.

APPENDIX
TO THE ADDENDUM

This Appendix forms part of the Addendum.

ANNEX I

A. LIST OF PARTIES

The Agreement between Customer as the controller and Provider as the Processor contains a description of all the required information, such as:

- name, address, contact person's name,
- position and contact details,
- activities relevant to the data transferred under these Clauses, and
- signature and date.

B. DESCRIPTION OF PROCESSING

1. Categories of data subjects whose personal data is processed

Unless provided otherwise by Customer, processed Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the SaaS Software.

2. Categories of personal data processed

Customer determines the categories of data per its use of the SaaS Software. The personal data processed typically concern the following categories of data:

- Employment details (which may include company name and address, job title, grade, demographic and location data) relating to employees of Customer or other third parties whose personal information is provided by or on behalf of Customer;
- System information relating to Customer systems, or systems provided to Provider by Customer and related to the services purchased under this Agreement and required for the provisioning of the SaaS Software (which may include user ID and password, computer and domain name, the IP address, GUID number or location of the computer or other device being used).

Customer Personal Data processed hereunder may concern past, present and prospective, business partners or other individuals related to such business partners.

3. Sensitive data processed (if applicable)

Special categories of personal data (as defined in Article 9 GDPR) must not be provided by Customer unless identified on a case by case basis and then only to the extent that the parties agree that such special categories of data are to be covered by the SaaS Software.

4. The frequency of the processing (e.g. whether the data is processed on a one-off or continuous basis).

Continuously for the duration of the use of the SaaS Software.

5. Nature of the processing

Provision of services as purchased by Customer.

6. Purpose(s) of the data transfer and further processing

The Customer Personal Data processed by Provider will be subject to the following basic processing activities:

- use of Customer Personal Data to provide access to and benefits of the SaaS Software pursuant to the Agreement and to provide assistance and technical support to Customer at Customer's request and in accordance with Customer's specific requirements, as appropriate, all in accordance with the instructions described below;
- storage of Customer Personal Data in data centers (multi-tenant architecture);
- back up and restoration of Customer Personal Data stored in the SaaS Software;
- computer processing of Customer Personal Data, including data transmission, data retrieval, data access.
- communication to Customer's users;
- release, development and upload of any fixes or upgrades to the SaaS Software;
- network access to allow Personal Data transfer;

- monitoring, troubleshooting and administering the underlying SaaS Software infrastructure and database;
- security monitoring, network-based intrusion detection support, penetration testing;
- execution of instructions of Customer in accordance with the Agreement and this Addendum; and
- as necessary to respond to and address requests and demands of Data Subjects as appropriate and in accordance with the instructions described immediately below.

Provider may use anonymized data (which is not Customer Personal Data but may be derived from Customer Personal Data) for purposes related to product improvement and development of new Provider products and services.

Further details of what the Product does, how it handles Personal Data and the data storage location are indicated in the applicable Product Documentation and Security Guide.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The aforementioned personal data shall be processed during Customer's use of SaaS Software pursuant to the Agreement and subject to Section 9 of this Addendum.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

In respect of the Standard Contractual Clauses, transfers to Sub-processors shall be on the same basis as set out in this Addendum.

9. Instructions, Customer and Provider Commitments.

Any description of processing in the Agreement, this Addendum and any related SaaS Software Documentation of Provider shall be considered as instructions by Customer and Provider. Provider will follow written and documented instructions received from Customer with respect to Customer Personal Data unless in Provider's opinion such instructions (1) are legally prohibited or likely to result in a violation of applicable Data Protection Law, (2) require material changes to Provider's SaaS Software, and/or (3) are inconsistent with the terms of the Agreement or Provider's Documentation relating to the SaaS Software sold hereunder. In any such case, Provider shall immediately inform Customer of its inability to follow such instructions.

ANNEX II - Statement of Technical and Organizational Measures

Provider will use the appropriate technical and organizational measures set out at the Security Site (as defined in Section 3(a) of the Addendum) in Provider's processing of Customer Personal Data hereunder. Customer agrees that Provider may modify the measures taken in protecting Customer Personal Data so long as it does not materially decrease the overall level of data protection agreed herein.