IVANTI DATA PROCESSING ADDENDUM

This Ivanti Data Processing Addendum ("DPA") forms a part of the Ivanti End User License and Services Agreement ("Agreement") and is made and entered into as of the last signature date below (the "Effective Date") by and between the customer identified below or in the Agreement ("Controller") and the applicable Ivanti entity identified in this DPA ("Ivanti" or "Processor") (individually, a "Party"; collectively, the "Parties"). Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

RECITALS

WHEREAS, the Parties have entered into the Agreement.

WHEREAS, in the course of providing the Services to Controller pursuant to the Agreement, Processor may Process Personal Data on behalf of Controller;

WHEREAS, to ensure adequate safeguards with respect to the Processing of Personal Data provided by Controller to the Processor the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW, THEREFORE, in consideration of the foregoing premises and of the mutual promises and covenants set forth below, Controller and Processor hereby agree as follows:

AGREEMENT

1. DEFINITIONS

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data including but not limited to (a) the GDPR together with any transposing, implementing or supplemental legislation, and (b) the CCPA.

"Authorized Affiliate" means any of Controller's Affiliates which (a) are subject to the data protection laws and regulations of the European Economic Area and/or its member states, the United Kingdom, and Switzerland, (b) are subject to data protection laws and regulations outside of the European Economic Area and/or its Member States, Switzerland, and the United Kingdom (as applicable), and (c) permitted to use the Processor for Processing pursuant to the Agreement.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data. For the avoidance of doubt, the Party identified above as "Controller" is a Controller under this DPA.

"Data Breach" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed.

"Data Protection Authority" means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

"Data Subject" means a natural person to whom Personal Data relates.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Ivanti" means the entity identified below in the same geographic region as Customer:

- Ivanti, Inc., a Delaware corporation, in the Americas, except Brazil.
- Ivanti Comércio de Software Brasil Ltda, a Brazilian company, in Brazil.
- Ivanti Software K.K., a Japanese company, in Japan.
- Ivanti Software Technology (Beijing) Co., Ltd., a Chinese company, in China.

- Ivanti International Limited, an Irish company, for Wavelink and Naurtech branded products and services in Europe, the Middle East, Africa, and the Asia Pacific region.
- Ivanti UK Limited, a limited company registered in England and Wales, in all other locations.

"Personal Data" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or particular household. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Process" shall mean any operation or set of operations which is performed upon Personal Data by the or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

"Processor" means the entity which Processes Personal Data on behalf of the Controller. For the avoidance of doubt, the Party identified as "Processor" above is a Processor for this DPA.

"Services" means Processing of Personal Data by the Processor in connection with and for the purposes of the provision of the services to be provided by the Processor pursuant to the Agreement.

"Service Provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that process information on behalf of a Data Controller and to which the Data Controller discloses a Data Subject's Personal Data for a Business Purpose pursuant to a written contract, provided that the contract prohibits the Service Provider from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a Commercial Purpose other than providing the services specified in the contract with the Data Controller. The terms "Business Purpose" and "Commercial Purpose" have the same meaning as those terms are used in the CCPA. For the avoidance of doubt, Processor is a Service Provider.

"Sub-processor" means any entity which Processes Personal Data on behalf of the Processor.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that about the Processing of Personal Data, Controller is the Controller, Processor is the Processor or Service Provider. The subject matter, duration, purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.2 Controller's Obligations. Controller's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquires Personal Data and provides it to Processor.

2.3 Processor's Obligations. All Personal Data Processed by Processor pursuant to the Agreement is Confidential Information and Processor will Process Personal Data only in accordance with Controller's documented instructions set forth in Schedule 1 or as otherwise provided by Controller in writing. Processor will not sell the Personal Data Processed under this DPA and will not retain, use, or disclose Personal Data outside of the direct business relationship between Processor and Controller. Processor shall adhere to all Applicable Data Protection Laws with regard to Processing Personal Data. Where the Processor believes that compliance with any instructions by Controller would result in a violation of any Applicable Data Protection Law, the Processor shall notify Controller thereof in writing without delay. Processor shall make available to the Controller all information necessary to demonstrate Processor's compliance with its obligations under this DPA.

2.3.1. Assistance Requirements. Processor shall assist Controller with: compliance with Applicable Data Protection Laws; suspected and relevant Data Breaches; notifications to, or inquiries from a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and Controller's obligation to carry out data protection impact assessments and prior consultations with a Data Protection Authority.

3. NOTIFICATION OBLIGATIONS

3.1 Processor's Notification Obligations. Processor shall immediately notify Controller, in writing, of the following:

3.1.1 A Data Subject's request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;

3.1.2 Any request or complaint received from Controller's customers or employees;

3.1.3 Any question, complaint, investigation, or other inquiry from a Data Protection Authority;

3.1.4 Any request for disclosure of Personal Data that is related in any way to Processor's Processing of Personal Data under this DPA;

3.1.5 A Data Breach pursuant to the notification obligations set forth in Section 7.1; and

3.1.6 Where the Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed.

Processor will assist Controller in fulfilling Controller's obligations to respond to requests relating to paragraphs (3.1.1) - (3.1.6) above and will not respond to such requests without Controller's prior written consent unless Processor is required to respond by law.

4. CONFIDENTIALITY

4.1 Confidential Information. All Information provided to Processor pursuant to the Agreement is Confidential Information.

4.2 Processor's Personnel. Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of their respective employment relationship with such individuals.

4.3 Limitation of Access. Processor shall ensure that Processor's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Controller acknowledges and agrees that Processor and Processor's Affiliates may engage third-party Sub-processors in connection with the provision of the Services. Processor or Processor's Affiliate shall enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-processor. Controller hereby authorizes Processor to engage its current list of Sub-processors as listed at https://www.ivanti.com/company/legal/ivanti-subprocessors to Process Personal Data in accordance with this DPA. Controller will not directly communicate with Processor's Sub-processors about the Services, unless agreed to by Processor in Processor's sole discretion.

5.2 Notification of Changes to Sub-processors. Processor will inform Controller of any intended changes concerning the addition or replacement of Sub-processors by providing Controller with a mechanism to subscribe to notifications of new Sub-processors at https://www.ivanti.com/company/legal/ivanti-subprocessors. Processor will notify Controller of any intended changes concerning the addition or replacement of Sub-processors prior to its use of the Sub-processor.

5.3 Objection Right for New Sub-processors. Controller may reasonably object to Processor's use of a new Sub-processor by notifying Processor promptly in writing within fifteen (15) business days after receipt of Processor's notice. In the event Controller objects to a new Sub-processor, Processor will use reasonable efforts to make available to Controller a change in the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If Processor is unable to make available such change, Controller may terminate the applicable Agreement with respect to those Services which cannot be provided by Processor without the use of the objected-to new Sub-processor.

5.4 Liability for Acts of Sub-Processors. Processor shall be liable for the acts and omissions of its Sub-processors to the same extent Processor would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1 Protection of Personal Data. Processor shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or

unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data.

6.2 Audit Rights. Controller agrees its right to audit Processor may be satisfied by Processor presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Processor's data protection officer, the IT security department, data protection or quality auditors or other mutually agreed to third parties or certification by way of an IT security or data protection audit. To the extent it is not possible to satisfy an audit obligation mandated by applicable Data Protection Laws and Regulations through such attestations, reports or extracts, Controller, or Controller's designee, has the right to audit and inspect—at Controller's expense—Processor's premises, policies, procedures, and computerized systems to make sure Processor complies with the requirements in this DPA. Controller, or Controller's designee, will provide at least thirty (30) days notification before conducting an audit unless such audit is required due to a Data Breach involving Processor. Audits by Controller or Controller's designee will not violate Processor's confidentiality obligations with Processor's other clients. All audits will be conducted during normal business hours, at Processor's principal place of business or other Processor location(s) where Personal Data is accessed, processed or administered, and will not unreasonably interfere with Processor's day-to-day operations. Before the commencement of any such audit, Processor and Controller shall mutually agree upon the timing, scope, and duration of the audit. Controller may request a summary audit report(s) or audit Processor no more than once annually.

7. DATA BREACHES

7.1 Data Breach Notification. Processor shall notify Controller in writing without undue delay after becoming aware of a suspected Data Breach. In no event shall such notification be made more than 72 hours after Processor's discovery of the Data Breach.

7.2 Data Breach Management. Processor shall make reasonable efforts to identify the cause of such Data Breach and take those steps as Processor deems necessary and reasonable to remediate the cause of such a Data Breach to the extent the remediation is within Processors reasonable control.

8. TERMINATION

8.1 Termination. This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Agreement or (b) Processor's deletion or return of Personal Data. Controller shall further be entitled to terminate this DPA for cause if the Processor is, in the sole opinion of Controller, in a material or persistent breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within ten (10) days from the date of receipt by the Processor of a notice from Controller identifying the breach and requesting its remedy.

8.2 Return or Deletion of Data. Upon termination of this DPA, Processor will delete or return all existing copies of Personal Data unless applicable law requires continued retention of the Personal Data. Upon the request of Controller, the Processor shall confirm compliance with such obligations in writing and delete all existing copies. In instances where local law requires the Processor to retain Personal Data, Processor will protect the confidentiality, integrity, and accessibility of the Personal Data; will not actively Process the Personal Data; and will continue to comply with the terms of this DPA.

9. MECHANISMS FOR INTERNATIONAL TRANSFERS

1.1 **9.1 Transfers Outside of the EU.** In the course of the provision of Services under the DPA, it may be necessary for Controller to transfer Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland, or the United Kingdom, to Processor in a country that does not have an adequacy decision from the European Commission or is not located in the European Economic Area.

1.2 **9.1.1.** In relation to Personal Data that is subject to the GDPR (i) Processor will be deemed the "data importer" and Controller is the "data exporter"; (ii) the Module Two terms shall apply where Controller is a Data Controller and where Processor is a Data Processor; (iii) in Clause 7, the optional docking clause shall be deleted; (iv) in Clause 9 of Module Two, Option 2 shall apply and the list of Subprocessors and time period for notice of changes shall be as agreed under Section 5 of this DPA; (v) in Clause 11, the optional language

shall be deleted; (vi) in Clause 17, Option 1 shall apply and the Standard Contractual Clauses shall be governed by the member state where Controller is domiciled; (vii) in Clause 18(b), disputes shall be resolved before the courts of the member state where Controller is domiciled; (viii) Annex I and Annex II shall be deemed completed with the information set out in Schedule 1 of this DPA respectively; and (ix) if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict. For this section, the Standard Contractual Clauses from the Commission Implementing Decision (EU) 2021/914 are incorporated by reference and available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

1.3 **9.1.2.** In relation to Personal Data that is subject to UK Data Protection Laws, the International Data Transfer Agreement ("IDTA") shall apply with the following modifications: (i) the contact information about the parties to the Agreement is the contact information for the IDTA; (ii) Controller is the data exporter and Processor is the data importer; (iii) the laws that govern the IDTA and the location where legal claims can be made is England and Wales; (iv) the UK GDPR does not apply to the data importer's processing of transferred data; (v) the Parties do not use the additional security or commercial clauses from the IDTA; and (vi) the information in this DPA and Schedule 1 can be used for Tables 1-4. For this section, the Standard Contractual Clauses from the Information Commissioner's Office are incorporated by reference and available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

1.4 **9.1.3.** In relation to Personal Data that is subject to the Swiss DPA, the Standard Contractual Clauses referenced in Section 9.1.1 shall apply with the following modifications (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" shall be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

1.5 **9.2. Alternative Data Transfer Mechanisms.** The Parties acknowledge that the laws, rules and regulations relating to international data transfers are rapidly evolving. In the event that Controller adopts another mechanism authorized by applicable laws, rules or regulations to transfer Personal Data (each an "Alternative Data Transfer Mechanism"), the Parties agree to work together in good faith to implement any amendments to this Agreement necessary to implement the Alternative Data Transfer Mechanism.

2. 10. MISCELLANEOUS PROVISIONS

2.1 **10.1. Amendments.** This DPA may not be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of both parties.

2.2 **10.2 Governing Law.** This DPA shall be governed by the governing law set forth in the Agreement.

2.3

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

CONTROLLER:_____	**IVANTI**
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

2.4

2.5 List of Schedules:

2.6 Schedule 1: Description of the Processing

SCHEDULE 1

Description of the Processing

Ivanti Contact Information:

Ivanti

10377 South Jordan Gateway

Suite 110

South Jordan, Utah 84095

DPO Contact: privacy@ivanti.com

Subject-Matter

The subject-matter of the Processing:

Provision of IT software licensing, support services and implementation, whether on-premises or as a hosted SaaS solution, regarding the administration and facilitation of essential business processes in the field(s) of unified endpoint management, IT service management, IT asset management, security, reporting and analytics, and supply chain.

IT services include the use of software as an on-premise installation or a SaaS solution including installation of modules (including without limitation, incident, change, asset, configuration and release management modules); self-service and service catalogues; support and maintenance including, without limitation, remote access; and patches, app control, endpoint/mobile security and privilege management.

Processing Frequency:

Continuous.

Duration

Duration of the Processing:

As set forth in the Agreement.

Extent, Type and Purpose of the Processing

The extent, type and purpose of the Processing is as follows:

As set forth in the Agreement.

Data Subjects

Personal Data Processing may relate to the following categories of Data Subjects:

Customers, prospects; employees; suppliers; commercial representatives; contacts; contractors (including contingent workers); volunteer; temporary and casual workers; freelancers, agents, consultants and other professional respondents, and their respective dependents, beneficiaries and emergency contacts; perspective employees and temporary staff of customers; complainants, correspondents and enquirers; advisers, consultants and other professional experts; employees or contact persons of data exporter's prospects, customers, business partners and vendors; business

partners and vendors of data exporter (who are natural persons); and data exporter's users authorized by data exporter to use the software and related services.

Categories of Data

The Personal Data Processed may concern the following categories of data:

Customer data uploaded to the Services under Customer's services and accounts.

Technical and Organizational Measures

The following describes the technical and organizational security measures implemented by Processor:

Security Awareness Training

Processor has security awareness training which includes mandatory security training about the handling and securing of confidential information and sensitive information such as personally identifiable information, financial account information, and health information consistent with applicable law, and periodic security awareness communications and security courses that focus on end-user awareness.

Security Policies and Procedures

Processor has information security, use and management policies which dictate the actions of employees and contractors regarding appropriate use, access to and storage of confidential and sensitive information; restrict access to confidential and sensitive information to members of Processor's workforce who have a "need to know" such information; prevent terminated employees from accessing Processor's information post-termination; and impose disciplinary measures for failure to abide by such policies. System access to Processor resources denied unless specifically assessed and access granted. Processor performs background checks of its employees at time of hire, as permitted by law.

Physical and Environmental Access Controls

Processor limits physical access to its information systems and facilities using physical controls (e.g., coded pass access) that provide reasonable assurance that access to its data centers is limited to authorized individuals and employs camera or video surveillance systems at critical internal and external entry points. Processor applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

Logical Access Controls

Processor employs logging and monitoring technology to help detect and prevent unauthorized access attempts to its networks and production systems. Processor's monitoring includes a review of changes affecting systems' handling authentication, authorization, and auditing; privileged access to Processor's production systems.

Encryption Controls

Processor applies business-appropriate encryption controls across our products. Processor evaluates and applies in-transit and at-rest encryption utilizing industry best practices for ciphers. Best practices are utilized for the lifecycle management of encryption keys, including generation, storage, access control, and rotation.

Vulnerability Management

Processor regularly performs vulnerability scans and addresses detected vulnerabilities in accordance with their risk. Processor products are also subject to periodic vulnerability assessment and penetration testing.

Disaster Recovery and Back-up Controls

Processor performs periodic backups of production file systems and databases according to a defined schedule and maintains a formal disaster recovery plan for the production cloud data center, including regular testing.

Cyber Incident Response Plan

Processor employs an incident response plan to manage and minimize the effects of unplanned cyber events that includes procedures to be followed in the event of an actual or potential security breach, including: an internal incident response team with a response leader; an investigation team performing a root causes analysis and identifying affected parties; internal reporting and notification processes; documenting responsive actions and remediation plans; and a post-incident review of events.

Storage and Transmission Security

Processor employs technical security measures to guard against unauthorized access to Processor data that is being transmitted over a public electronic communications network or stored electronically.

Secure Disposal

Processor employs policies and procedures regarding the disposal of tangible and intangible property containing Processor data so that Processor data cannot be practicably read or reconstructed.

Risk Identification & Assessment

Processor employs a risk assessment program to help reasonably identify foreseeable internal and external risks to Processor's information resources and determine if existing controls, policies, and procedures are adequate to address the identified risks.

Vendor & Services Providers

Third-party service providers or vendors (collectively, "Suppliers") with access to Processor's confidential information are subject to risk assessments to gauge the sensitivity of Processor's information being shared. Suppliers will be expected to comply with any pertinent contract terms relating to the security of Processor data, as well as any applicable Processor policies or procedures. Periodically, Processor may ask a Supplier to re-evaluate its security posture to help ensure compliance.