DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("DPA") forms part of the Ivanti End User License and Services Agreement (the "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 ("Customer" or "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.

1. **Definitions**. The following terms have the meanings set out below:

    a. **Affiliates**: Means any legal entity that controls, is controlled by or is under common control with Customer or Ivanti (as applicable); where 'control' refers to ownership of more than fifty percent (50%) of voting securities.

    b. **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 Information transmitted, stored, or otherwise Processed.

    c. **Data Protection Laws and Regulations**: Means all applicable privacy and security laws and regulations.

    d. **Data Protection Authority**: Means any representative or agent of the government who has the authority to enforce local data privacy and security laws.

    e. **Data Subject**: Means a natural person whose Information is Processed pursuant to this DPA.

    f. **Information**: Means all data Processed by Ivanti or Ivanti's Subprocessor pursuant to this DPA, including Personal Data and Sensitive Data.

    g. **Ivanti**: Means the entity identified below in the same geographic region as Customer:
        i. Ivanti, Inc., a Delaware corporation, in the Americas, except Brazil.
        ii. Ivanti Comércio de Software Brasil Ltda, a Brazilian company, in Brazil.
        iii. Ivanti Software K.K., a Japanese company, in Japan.
        iv. Ivanti Software Technology (Beijing) Co., Ltd., a Chinese company, in China.
        v. 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.
        vi. Ivanti UK Limited, a limited company registered in England and Wales, in all other locations.

    h. **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, particular consumer, or 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. A consumer is a natural person who is a California resident. A resident is every individual who is in California other than for a

temporary or transitory purpose, and every individual who is domiciled in California who is outside California for a temporary or transitory purpose.

i. **Process or Processing**: Means any operation or set of operations which is performed on Information or on sets of Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

j. **Sensitive Data**: Means any Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, or Information relating to criminal convictions and offences.

k. **Subprocessor**: Means any entity contracted by Ivanti to assist and/or support Ivanti's delivery of the Services under the Agreement and the DPA.

l. **Services**: Means Ivanti's provision of the Software and/or connected services (e.g. Professional Services, SaaS Offerings, Support and Maintenance Services, etc.).

2. **Term**. The term of this DPA (the "Term") shall commence on the Effective Date and continue until either Party terminates the DPA. Either Party may terminate this DPA for convenience thirty (30) days after providing written notice of termination.

3. **Roles of the Parties.** The Parties agree that Customer is the controller of the Personal Data and is solely responsible for determining purposes and means of the processing of Personal Data and its compliance with the Data Protection Laws and Regulations, including without limitation the lawfulness of any transfer of Personal Data to Ivanti and the instructions given to Ivanti concerning Ivanti's Processing of Personal Data. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer represents that it shall provide Data Subjects with all required notices and obtain any necessary consents required by applicable Data Protection Laws and Regulations prior to the transfer of any Personal Data to Ivanti. Customer shall provide adequate proof for having properly obtained all such necessary consents, authorizations and required permissions upon request. Customer shall keep the amount of Personal Data provided to Ivanti to the minimum necessary for the performance of the Services. Ivanti is the processor or service provider responsible for Processing Personal Data on behalf of the Customer. Customer acknowledges and consents that certain business operations necessary for the fulfilment of the Services hereunder may have been transferred or will be transferred in the future to one or more Ivanti Affiliates independently managing the provision of such services.

4. **Purpose of Processing**. Ivanti, Ivanti Affiliates, and its Subprocessors operating on behalf of Ivanti will collect, access, store, use or otherwise Process Personal Data to administrate the contractual relationship and to provide Customer with the Services.

5. **Nature of Processing**. Provision of IT services: Software licensing and implementation, whether on-premises or as a SaaS Offering, regarding the administration and facilitation of essential business processes in the field of:

    - Unified Endpoint Management;
    - IT service management (ITSM);
    - IT asset management (ITAM);
    - Security;
    - Reporting and Analytics; and,
    - Supply Chain.

    IT services include:

    - The use of software as an on-premise installation or a SaaS Offering 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.

    Additional details are set forth in the Documentation provided with the Software, subject to Agreement and any schedules or statements of work related thereto, or as further instructed by Customer for use of the Software and services.

6. **Categories of Information Involved**. Customer may submit Personal Data to the Software, Services, Ivanti websites and mobile applications, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

    - Application Use Data (e.g. log-files);
    - Identification data and employee master data (which may include title, name, address, telephone number, fax number, company address, email address);
    - Cookies and session information
    - Goods and services provided – products purchased, products shipped or downloaded, payments processed;
    - Internet protocol (IP) address and other computer identifiers;
    - Contact details (e.g. telephone, e-mail);
    - Contract master data and customer history (e.g. contractual relationship, interest in products or contracts);
    - Billing and payment data;
    - Planning and management data;
    - User-provided content; and
    - Other, as described in the Documentation or Agreement.

7. **Categories of Data Subjects Involved**. Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating 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 Customer's prospects, customers, business partners and vendors;
- Business partners and vendors of Customer (who are natural persons); and
- Customer's Users authorized by Customer to use the Software and related services.

8. **Rights of the Customer**. Customer agrees its right to audit Ivanti may be satisfied by Ivanti presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Ivanti'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, Customer may conduct an onsite audit of Ivanti's facilities used to provide the Services. All audits will be conducted during normal business hours, at Ivanti's principal place of business or other Ivanti location(s) where Personal Data is accessed, processed or administered, and will not unreasonably interfere with Ivanti's day-to-day operations. An audit will be conducted at Customer's sole cost and by a mutually agreed upon third party who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement, obligating it to maintain the confidentiality of all Ivanti Confidential Information and all audit findings. Before the commencement of any such on-site audit, Ivanti and Customer shall mutually agree upon the timing, scope, and duration of the audit. Customer may request a summary audit report(s) or audit Ivanti no more than once annually. Customer must provide at least six (6) weeks' prior written notice to Ivanti of a request for summary audit report(s) or request to audit. The scope of any audit will be limited to Ivanti's policies, procedures and controls relevant to the protection of Customer's Personal Data. Customer shall, at no charge, provide to Ivanti a full copy of all findings of the audit.

   Customer may not audit a Subprocessor without Ivanti's and Subprocessor's prior agreement. Customer agrees its requests to audit Subprocessors may be satisfied by Ivanti or Ivanti's Subprocessors presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Ivanti'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. Onsite audits at Subprocessors premises may be performed by Ivanti acting on behalf of Customer.

9. **Ivanti's Obligations**. Ivanti agrees and warrants that it will:

   a. Only Process Information in accordance with this DPA and Customer's documented instructions. Customer's initial instructions for the Processing of Personal Data are defined by this DPA, and any applicable order form or Statement of Work regarding the Software and Services. Subject to the terms of this DPA and with mutual agreement of the Parties, Customer may issue additional written instructions concerning the type, extent and procedure of Processing. Any changes of the subject matter of Processing and of procedures shall be agreed upon by the Parties in writing prior to becoming effective.

   b. Process Information in accordance with Data Protection Laws and Regulations. With regard to the GDPR, Ivanti—taking into account the nature of Processing and the Information available to Ivanti—will assist the Customer in ensuring compliance with Articles 32-37.

   c. If Information will transfer from the European Economic Area to a country outside the European Economic Area, the Parties will transfer the Personal Data using Ivanti's EU-U.S. Privacy Shield Certification.

   d. Not transfer Information to another organization without the Customer's documented approval.

   e. Not sale Personal Data to third parties for money or other valuable consideration.

   f. Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. In assessing the appropriate level of security, Ivanti shall weigh the risks presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed. A description of the technical and organizational security measures implemented by Ivanti are set forth in Schedule 1 attached hereto.

   g. Not use Subprocessors to Process Information received from Customer without documented approval from Customer. Customer hereby authorizes Ivanti to engage its current list of Subprocessors as listed at https://www.ivanti.com/company/legal/ivanti-subprocessors to Process Personal Data in accordance with this DPA. Ivanti will ensure each of its Subprocessors comply with the obligations in Section 9 (**Ivanti's Obligations**) and Section 10 (**Confidentiality**) of this DPA as if it were Ivanti. Ivanti will notify Customer of any intended changes concerning the addition or replacement of Subprocessors by providing Customer with a mechanism to subscribe to notifications of new Subprocessors at https://www.ivanti.com/company/legal/ivanti-subprocessors. If Customer reasonably objects to the addition of a new Subprocessors, Customer shall notify Ivanti in writing of its specific objections within fifteen (15) days of

receiving such notification. If Customer does not object within such period, the addition of the new Subprocessor and, if applicable, the accession to this DPA shall be considered accepted. If Customer objects to the addition of a new Subprocessor and Ivanti cannot accommodate Customer's objection, Customer may terminate the Services and Software in writing within fifteen (15) days of receiving Ivanti's notification of its inability to accommodate Customer's objection. Customer will not directly communicate with Ivanti's Subprocessors about the Services, unless agreed to by Ivanti in Ivanti's sole discretion.

h. Notify Customer when any law or legal requirement prevents Ivanti from fulfilling its obligations under this DPA, or from complying with Customer's instructions.

i. Maintain internal records of all Processing conducted on behalf of Customer. At a minimum, such records will list the categories of Information Ivanti Processes pursuant to this DPA and the methods used to reasonably preserve the confidentiality, integrity, and accessibility of such Information.

j. Make available to the Customer all information necessary to demonstrate Ivanti's compliance with its obligations under this DPA.

k. Immediately notify Customer, in writing, of the following:

   i. A Data Subject's request to access, rectify, erase, transport, object to, opt-out, or restrict Information Processed pursuant to this DPA;

   ii. Any request or complaint received from Customer's customers or employees;

   iii. Any question, complaint, investigation, or other inquiry from a Data Protection Authority; and

   iv. Any request for disclosure of Information from a public entity related in any way to Subprocessor's Processing of Information under this DPA.

   v. Ivanti will assist Customer in fulfilling its obligations to respond to requests referenced in paragraphs (i)-(iv) above.

   vi. Ivanti will not respond to requests referenced in paragraphs (i)-(iv) above without Customer's prior written consent unless Ivanti is required to respond by law.

l. Cooperate with Customer to comply with applicable Data Protection Laws and Regulations and this DPA.

m. Upon termination of this DPA or upon Customer's request to delete or return Information, Ivanti will delete or return existing copies of Information unless local law requires storage of the Information. In instances where local law requires Ivanti to store Information, Ivanti will protect the confidentiality, integrity, and accessibility of the Information; will not actively Process the Information anymore; and will continue to comply with this DPA.

n. Immediately inform Customer if, in its opinion, an instruction or request from the Customer infringes upon any applicable law or regulation. Ivanti will not execute such instructions until the instruction has been confirmed or modified by Customer.

o. Ivanti shall investigate potential Data Breaches, and after becoming aware of a Data Breach Ivanti shall notify Customer without undue delay and according to the relevant Data Protection Laws and Regulations.

p. If required by Data Protection Laws and Regulations, Ivanti shall appoint a data protection officer. Upon request, Ivanti will provide the contact details of the appointed person.

10. **Confidentiality**. All Information subject to this DPA is "Confidential Information". In connection with the performance of this DPA, either Party (each a "**Recipient**") may have access to or be provided with Confidential Information of the other Party (the "**Discloser**"). The Recipient shall use the Confidential Information of the Discloser solely in connection with the performance of this DPA. The Recipient shall limit its disclosure of the Confidential Information to Recipient's directors, officers, and employees that need such Information pursuant to this DPA. The Recipient is responsible for compliance with the terms and conditions of this DPA by its directors, officers, and employees. The Recipient will protect the Confidential Information from unauthorized use, access, or disclosure in the same manner as the Recipient protects its own confidential or proprietary Information of a similar nature but in any event with no less than reasonable care. The Recipient shall certify the destruction of all copies of the Discloser's Confidential Information upon request of the Discloser, with the exception that the Recipient may maintain one (1) copy of the Discloser's Confidential Information solely to the extent necessary for the Recipient to comply with laws or regulations applicable to such Recipient (and the Recipient shall destroy such retained Confidential Information of Discloser after the legal or regulatory retention purpose expires or otherwise no longer exists). The Recipient's obligations under this section shall continue for a period of two years after the expiration or termination of this DPA.

The Parties have caused their duly authorized representatives to execute this DPA as of the dates set forth below.

CUSTOMER:_____	IVANTI
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Schedule 1

Security Measures

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

Security Awareness Training

Ivanti 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.

Ivanti 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 Ivanti's workforce who have a "need to know" such information; prevent terminated employees from accessing Ivanti's information post-termination; and impose disciplinary measures for failure to abide by such policies. System access to Ivanti resources denied unless specifically assessed and access granted. Ivanti performs background checks of its employees at time of hire, as permitted by law.

Physical and Environmental Access Controls

Ivanti 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. Ivanti applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

Logical Access Controls

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

Vulnerability Management

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

Disaster Recovery and Back-up Controls

Ivanti 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

Ivanti 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

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

Secure Disposal

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

Risk Identification & Assessment

Ivanti employs a risk assessment program to help reasonably identify foreseeable internal and external risks to Ivanti'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 Ivanti's confidential information are subject to risk assessments to gauge the sensitivity of Ivanti's information being shared. Suppliers will be expected to comply with any pertinent contract terms relating to the security of Ivanti data, as well as any applicable Ivanti policies or procedures. Periodically, Ivanti may ask a Supplier to re-evaluate its security posture to help ensure compliance.