Data Processing Agreement

This Data Processing Agreement ("DPA") is incorporated into, and forms part of, the Master Purchase Agreement, Quote, Purchase Order, Statement of Work, and/ or other contractual documents (individually and collectively, the "Agreement") between Infoblox Inc. ("Infoblox") and your company ("Customer").

1. Scope, Order of Precedence, and Term

(a) This DPA applies when Personal Data is processed in connection with the Services.

(b) In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the parties use an international transfer mechanism and there is a conflict between the international transfer mechanism and this DPA, the international transfer mechanism will prevail.

(c) The effective date of this DPA is the date of the Agreement, or the date that Customer first begins using Infoblox Products or Services, whichever is earlier. This DPA is coterminous with the Agreement, except for obligations that survive past termination as specified below.

2. Definitions

In this DPA, the following terms have the meanings set forth below. In the event of a conflict between the definitions in this DPA and any applicable Data Protection Law, the definition provided by the Law in question will control. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

"Affiliate" means (i) for Customer, any entity that directly or indirectly Controls, is Controlled by, or is under common Control with Customer and (ii) for Infoblox, any entity that is Controlled by Infoblox Inc.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing Personal Data (also, Customer).

"Customer Data" means any data, file attachments, text, images, reports, personal information, or other content that is uploaded or submitted to an online Service by Customer or Users and is Processed by Infoblox on behalf of Customer.

"Data Protection Laws" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

"Data Subject" means a living, natural person who is or can be identified directly or indirectly by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

“EU Data Protection Law” means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the “GDPR“); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom (“UK“) any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union).

“Parties” or “Party” means Customer and/or Infoblox as applicable.

“Personal Data” means any information relating to an identified or identifiable natural person 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.

“Processor” means a natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of a Controller.

“Professional Service” means consulting, implementation, or training services for Products and Services as described in a Purchase Order or Statement of Work.

“Security Breach” means any accidental, unauthorized, or unlawful breach of security that leads to the destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed or otherwise controlled by Infoblox.

“Security Incident” means a security event that does not lead to the destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed or otherwise controlled by Infoblox.

“SCCs” means the Standard Contractual Clauses approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

“Services” means the support and maintenance services, Professional Services, Software as a Service, and any other online service or application provided or controlled by Infoblox and made available for Customer’s use online and specified in an applicable Purchase Order.

“Subprocessor” means any individual or entity (including any third party but excluding Infoblox) appointed by or on behalf of Infoblox to process Personal Data pursuant to the Agreement.

“Supervisory Authority” means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR.

“Technical and Organizational Measures” or “TOMs” means the functions, processes, controls, systems, procedures, and measures that Infoblox implements to promote secure processing and storage of Personal Data, address and prevent data breaches, and facilitate compliance with relevant Data Protection Laws. See Annex II.

“User” means any individual authorized or invited by Customer or another User to access and use the Services under the terms of the Agreement.

“UK International Data Transfer Addendum” means the template addendum issued by the Information Commissioner’s Office (ICO) for the transfer of personal data from the UK to countries not covered by an adequacy decision.

3. Roles and Responsibilities

(a) Role of the Parties. The parties agree and understand that Section 3 will apply to them according to their role as indicated in applicable Data Protection Laws.

(b) Controller

(i) Controller is responsible for the accuracy of Customer Data and the legality of the means by which it acquires Customer data.

(ii) Controller’s instructions to process Customer Data will comply with all applicable Data Protection Laws and be duly authorized, with all necessary rights, permissions, and authorizations secured.

(c) Processor

(i) Processor, and any person who is authorized by it, will process Customer Data only: (a) as instructed by Customer or as initiated by Users via a Service; (b) only to the extent necessary to provide Services or to prevent or address technical issues with a Service; (c) to prevent or address violations of the Agreement or this DPA; (d) to comply with Customer’s instructions to the extent they are consistent with the terms of the Agreement and applicable law; (e) to comply with appropriate obligations of confidentiality; and/ or (f) in accordance with the rights and duties attached to the Customer Data.

(ii) Processor will not disclose Customer Data to a third party for monetary or other consideration except as otherwise permitted under this DPA or the Agreement.

(d) Customer Responsibilities. Customer shall:

(i) be responsible for its secure use of the Services (including account authentication and configuration, securing data when in transit to and from the Services, and any appropriate backup and encryption steps);

(ii) implement appropriate TOMs relating to its use of the Services in a manner which enables Customer to comply with applicable laws and regulations and maintain appropriate security, protection, deletion and backup of Personal Data; and

(iii) control the type and substance of Customer Data, set User permissions to access Customer Data, and be responsible for reviewing and evaluating whether the documented functionality of the Services meets Customer’s required security and privacy obligations.

4. Subprocessing

(i) Use of Subprocessors. Customer hereby permits Infoblox to engage Subprocessors to process Customer Data and approves of the Supplier Affiliates and third parties listed in https://support.infoblox.com/s/article/Infoblox-Subprocessors as Subprocessors.

(ii) Such Subprocessors will treat all Customer Data as confidential and will be permitted to access Customer Data only to deliver the services that Infoblox has retained them to provide in connection with the services, and they are prohibited from using Customer Data for any other purpose.

(iii) Infoblox will: (a) enter into a written agreement with each Subprocessor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the services provided by such Subprocessor; (b) Restrict the Subprocessor's access to Customer Data only to what is necessary to maintain or provide the services to Customer; and (c) remain responsible for such Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of such Subprocessor that cause Infoblox to breach any of its obligations under this DPA.

(b) Liability for Subprocessors. Each party will be liable for the acts and omissions of its Subprocessors to the same extent it would be liable if performing the services of the Subprocessor directly under the DPA.

(c) Objection to Subprocessors. Customer agrees to register and subscribe to https://support.infoblox.com/s/article/Infoblox-Subprocessors to be notified of any new or updated Subprocessor, including details of the Processing to be undertaken by the Subprocessor.

(i) In the event that Customer reasonably objects within 14 days to a Subprocessor and notifies Infoblox in writing, Infoblox will notify Customer of any available alternatives to change the Services or receive the Services from an alternate Subprocessor, together with any applicable charges or changes to terms, but only to the extent that qualified alternatives are available.

(ii) If an alternative Subprocessor that is acceptable to Customer is not available within a reasonable time or adds unproportionate monetary burden or amount of work for Infoblox, then Customer may terminate the Services which cannot be provided by Infoblox without the objectionable Subprocessor; provided that Customer shall not receive a refund of any prepaid fees for such Services due to the termination. Infoblox will work with Customer in good faith to make available a change in the provision of the Services which avoids the use of that proposed Subprocessor.

5. Data Subject Rights

(a) Data Subject Rights. As part of the Services, Infoblox may provide Customer with a number of self-service features that Customer may use to retrieve, correct, delete or restrict the use of Customer Data, which Customer may use to assist it in connection with its obligations under Data Protection Laws with respect to responding to requests from Data Subjects via Customer's account. In addition, Infoblox will, taking into account the nature of the processing, provide reasonable assistance to Customer to the extent possible to enable Customer to comply with its data protection obligations with respect to Data Subject rights under Data Protection Laws.

(b) If Customer does not have access to such Personal Data through its use of the Services to respond to such request, Infoblox will provide Customer with commercially reasonable cooperation and assistance in relation to responding to a Data Subject's request for access to that individual's Personal Data to the extent legally permitted. The Customer will be responsible for any costs arising from Infoblox's provision of such assistance.

(c) In the event that any such request is made to Infoblox directly, Infoblox will not respond to such communication except as necessary (for example, to direct the Data Subject to contact Customer or if legally required) without Customer's prior authorization. If Infoblox is required to respond to such a request, Infoblox will promptly notify Customer and provide Customer with a copy of the request unless Infoblox is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) will restrict or prevent Infoblox from responding to any Data Subject or Supervisory Authority requests in relation to Personal Data for which Infoblox is a Controller.

6. Cooperation

(a) Data Protection Impact Assessment. To the extent required under applicable Data Protection Laws, and under strict confidentiality, Infoblox will (taking into account the nature of the processing and the information available to Infoblox) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with Supervisory Authorities as required by Data Protection Laws.

(b) Legal Disclosure Requests. Infoblox is obligated not to disclose Personal Data except: (1) as Customer directs; (2) as described in this Agreement; or (3) as required by law.
Infoblox will not intentionally disclose Personal Data to law enforcement, other governmental authority, or other persons ("Requesting Body") unless the Infoblox receives a civil or criminal subpoena, warrant, or other official and written request which:
(i) is issued by a Requesting Body with the authority and jurisdiction to demand the disclosure, and
(ii) is, in the reasonable judgment of Infoblox, legally binding on Infoblox and requires Infoblox to disclose Personal Data in response thereto ("Disclosure Request").

If Infoblox is contacted with a Disclosure Request, Infoblox will:
(i) attempt to redirect the Requesting Body to request that Personal Data directly from the Customer instead,
(ii) promptly notify the Customer and provide a copy of the Disclosure Request unless legally prohibited from doing so,
(iii) review the Disclosure Request to determine whether it is valid and if Infoblox has a legal requirement to disclose Personal Data, and
(iv) assert its legal rights, including to resist and narrow the demand by fully taking all available remedies possible, and/or seek a stay from enforcement of the Disclosure Request.

In the event Infoblox is notified by the Requesting Body issuing a Disclosure Request that Infoblox is prohibited by law from giving notice to the Customer of the Disclosure Request, Infoblox will use best efforts to relieve itself of any such prohibition so that it may fully disclose such Disclosure Request to the Customer and coordinate with the Customer in responding to the Disclosure Request solely to the extent possible without incurring additional or outside legal fees or expenses.

In any case, Infoblox will provide notice to the Customer of the Disclosure Request immediately or as soon as legally permissible. Infoblox will notify the Customer of a Disclosure Request by contacting the indicated contact person.

Infoblox will only provide Personal Data if, and to the extent that, it is necessary and proportionate to comply with a Disclosure Request. Unless specifically requested by the Requesting Body, Infoblox will not provide any Requesting Body: (a) direct, indirect, blanket, or unfettered access to Personal Data; (b) platform encryption keys used to secure Data or the ability to break such encryption; or (c) access to Data if Processor is aware that the Data is to be used for purposes other than those stated in the third party's request.

In support of the above, Processor may provide Customer's basic contact information to the third party. The Parties agree that they will enter into additional agreements regarding additional protections measures regarding transfer of Data to third countries as required by local or European data protection authorities.

The parties recognize that Processor has sole discretion over its approach to adhering to the above and shall not be in breach of this section unless Customer is able to demonstrate willful misconduct or gross negligence.

Under no circumstances is Processor expected to incur additional legal fees or expenses in excess of $1,000 in meeting its obligations under subsections of this paragraph. If permitted under applicable law, Infoblox will provide Customer with an estimate of any additional legal fees and/or expenses and provide the Customer with the opportunity to pay for such fees and/or expenses.

(c) Audits.

(i) Infoblox will respond to all reasonable requests for information made by Customer to confirm Infoblox's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to security-compliance@infoblox.com provided that Customer will not exercise this right more than once per calendar year.

(ii) Once per year, upon Customer's written request and on a confidential basis, Infoblox will, within a reasonable time following such request, make available to Customer (or Customer's independent third party auditor that is not a competitor of Infoblox) information regarding Infoblox's compliance with the obligations set forth in the DPA, which may be in the form of third party audit reports and certifications, to the extent that Infoblox has such current reports or certifications and generally makes them available to customers.

(iii) Customer agrees that it will provide at least 30 days written notice for any audit activities. Before the commencement of any audit, Infoblox and the Customer will agree upon the scope, purpose, timing, and duration of the audit.

(iv) Customer will reimburse Infoblox for any time expended and expenses incurred for any audit at Infoblox's standard Professional Services rates.

7. Data Transfers and Exports

(a) The Parties acknowledge and agree that the Processing of Customer Data by Infoblox may involve an international transfer of Customer Data from Customer to Infoblox ("International Transfer").

(b) Standard Contractual Clauses. With respect to any International Transfer from the European Economic Area or the United Kingdom that would be prohibited by applicable Data Protection Laws in the absence of a lawful data transfer mechanism, the Parties agree that the SCCs issued by the European Commission under the GDPR on June 4, 2021, as may be amended, replaced, or supplemented from time to time, will be in effect between the Parties. For transfers of Personal Data from the United Kingdom to countries not covered by an adequacy decision by the Information Commissioner's Office (ICO), the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum") will apply.

(c) The SCCs will apply to Customer Data that is transferred outside the European Economic Area ("EEA"), either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

(d) The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if Infoblox has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

8. Security

(a) Infoblox will not assess the type or substance of Customer Data to identify whether it contains Customer Data or is subject to any specific legal requirements.

(b) Infoblox has implemented and maintains appropriate TOMs that are designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of Customer Data in accordance with Infoblox's security standards described as the Technical and Organizational Measures.

(c) For any Services for which Infoblox obtains third party certifications or audits, upon request, Infoblox will provide a copy of Infoblox's most recent third party certification or audit as applicable, which Infoblox generally makes available to its customers at the time of the request.

(d) Updates to TOMs. Customer is responsible for reviewing the information made available by Infoblox relating to data security and for making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the TOMs may change through the adoption of new or enhanced security technologies and development and as a result Infoblox may update or modify the TOMs from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

(e) Security Breach Response. Customer agrees and acknowledges that Infoblox's notification of or response to a Security Breach will not be construed as an acknowledgment by Infoblox of any fault or liability with respect to the Security Incident.

(f) Upon becoming aware of a Security Breach that results in unlawful exposure, destruction, or loss of access that is likely to affect the rights and freedoms of data subjects, Infoblox will: (a) notify Customer without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Breach; (b) provide timely information relating to the Security Breach as it becomes known or as is reasonably requested by Customer; and (c) investigate and, as necessary, take appropriate steps to mitigate or remediate in accordance with Infoblox's security policies and procedures.

9. General

(a) Modification to the DPA Terms. The parties agree to mutually determine and execute appropriate modifications to the terms of this DPA which do not materially alter the economics or allocation of risk established by the Agreement: (i) if required to do so by a Supervisory Authority or other government or regulatory entity [with appropriate jurisdiction]; (ii) if necessary to comply with Data Protection Law; or (iii) to implement or adhere to revised SCCs or the UK International Data Transfer Addendum which may be issued under Data Protection Law.

(b) Waiver. Unless otherwise expressly stated herein, this DPA may be modified only by a written agreement executed by an authorized representative of each Party. The waiver of any breach of this DPA will be effective only if in writing, and no such waiver will operate or be construed as a waiver of any subsequent breach.

(c) Relationship with the Agreement. Any claims brought under this DPA will be subject to the terms and conditions of the Agreement.

(i) This DPA will remain in effect for as long as Infoblox carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 9(d) below).

(ii) This DPA will replace any existing data processing agreement or similar document that the Parties may have previously entered into in connection with the Services.

(d) Return or Deletion of Data.

(i) Upon termination or expiration of the Agreement, Infoblox will (at Customer's written request) delete or return to Customer all Personal Data in Infoblox's possession or control. The Customer acknowledges that Infoblox may retain deidentified or anonymized data for research purposes.

(ii) This requirement will not apply to the extent Infoblox is required by applicable law to retain some or all the Customer Data or to Customer Data Infoblox has archived in its backup systems. In this case, Infoblox will archive the data and implement reasonable measures to prevent the Personal Data from any further processing and eventually delete in accordance with Infoblox's retention and deletion policies, unless otherwise required by applicable law.

(e) Severability. If any provision of this DPA is held to be unenforceable, then that provision is to be construed either by modifying it to the minimum extent necessary to make it enforceable (if permitted by law) or disregarding it (if not permitted by law), and the rest of this DPA is to remain in effect as written. Notwithstanding the foregoing, if modifying or disregarding the unenforceable provision would result in failure of an essential purpose of this DPA, the entire DPA will be considered null and void.

(f) Notices. Unless otherwise expressly stated herein, the parties will provide notices under this DPA in accordance with the Agreement, provided that all such notices may be sent via email.

(g) Governing Law and Jurisdiction. Unless prohibited by Data Protection Laws, this DPA is governed by the laws stipulated in the Agreement and the Parties to this DPA hereby submit to the choice of jurisdiction and venue stipulated in the Agreement, if any, with respect to any dispute arising under this DPA.

(h) Enforcement. Regardless of whether Customer or its Affiliate(s) or a third party is a Controller of Customer Data, unless otherwise required by law: (a) only Customer will have any right to enforce any of the terms of this DPA against Infoblox; and (b) Infoblox's obligations under this DPA, including any applicable notifications, will be to only Customer.

10. Limitation of Liability

(a) Each Party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) will be subject to the exclusions and limitations of liability set forth in the Agreement to the extent permissible by applicable law.

(b) Any claims made against Infoblox or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) will be brought solely by the Customer entity that is a party to the Agreement.

(c) Variations in Data Protection Laws. If any variation is required to this DPA as a result of a change in or subsequently applicable Data Protection Law, then either Party may provide written notice to the other Party of that change in law. The Parties will then discuss and negotiate in good faith any variations to this DPA necessary to address such changes, with a view to agreeing and implementing those or alternative variations as soon as practicable, provided that such variations are reasonable with regard to the functionality and performance of the Services and Infoblox's business operations.

(d) Reservation of Rights. Notwithstanding anything to the contrary in this DPA: (a) Infoblox reserves the right to withhold information the disclosure of which would pose a security risk to Infoblox or its customers or is prohibited by applicable law or contractual obligation; and (b) Infoblox's notifications, responses, or provision of information or cooperation under this DPA are not an acknowledgement by Infoblox of any fault or liability.

Infoblox Inc. **Customer: _____**

Signature: _____	Signature:_____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Email: _____	Email:_____

Last updated October 2024