Infoblox Professional Services

Domain Mitigation Services (Light)
Terms and Conditions

GENERAL: These Additional Terms and Conditions supplement ("**Additional Terms**") and are incorporated into the Professional Services Addendum set forth at https://www.infoblox.com/company/legal/infoblox-professional-services-addendum (the "**PS Addendum**") with respect to the "Infoblox Threat Defense Quickstart Package" Service. In the event of a conflict between the Professional Services Addendum and these Additional Terms, these Additional Terms shall control only with respect to the Service described below. Any terms not defined in the Additional Terms will have the meaning set forth in the Professional Services Addendum or the Master Purchasing Agreement, set forth at: https://www.infoblox.com/company/legal/master-purchasing-agreement.

1. Definitions

a. "Covered Products" means Customer's installed base of Infoblox DDI family of products (including products for DNS, DHCP, and IPAM), as purchased by Customer. The Services in this document are sold separately and are provided by separate Professional Services resources.

b. "Customer" means the Product user purchasing the Services. If Customer is a service provider purchasing the Services in support of an end customer, then "Customer" refers only to the service provider business unit personnel providing services to the specific end customer associated with the underlying Services.

2. Description of Services

2.1 Project Logistics

Infoblox will perform the Services outlined in the "Project Scope" section for the Customer on a fixed price basis.

Work Hours and Location:
As defined in these Terms and Conditions, the standard workday consists of eight (8) work hours. Infoblox personnel will carry out their tasks remotely.

Customer Responsibilities and Change Orders:
The Customer is responsible for promptly fulfilling the responsibilities outlined in these Terms and Conditions. Infoblox will not be held accountable for any delays resulting from the Customer's failure to provide timely access, facilities, cooperation, or necessary information as requested. Any Customer delays, modifications to the approach or Services described in these Terms and Conditions, including the division of migration evolution(s), will necessitate a Change Order.

2.2 Project Scope

The following Services will be performed as part of these Terms and Conditions:

DOMAIN MITIGATION SERVICES

Infoblox will provide Customer with up to twenty (20) Domain Mitigation Site Takedowns for the Term defined in these Terms and Conditions.

A Domain Mitigation Site Takedown will be initiated using the following two options:

- Customer sends an email to deactivatenow@infoblox.com with the URL(s) of the suspicious domain(s).
- Infoblox Domain Mitigation Services to proactively identify suspicious Customer lookalike domain(s). Infoblox shall reach out to the Customer with the details on the lookalike domain(s) and request permission in writing (via email) to perform Domain Mitigation Services on these domain(s).

The Domain Mitigation Site Takedown will consist of the following activities:

Task #	Description
1	Infoblox shall analyze and make commercially reasonable efforts to shut down domestic and international suspicious or lookalike websites, and email accounts designed to perpetrate fraud or disseminate malware that in the opinion of Infoblox: ● Falsely purport to be the Customer ● Falsely purport to be an authorized agent or partner of the Customer ● Falsely assert to conduct business on behalf of the Customer and/or ● Unlawfully display or misuse Customer logos in violation of the Lanham Act (Also known as the Trademark Act)
2	Infoblox shall contact the fraudulent domain's Internet Service Providers, Registrars, hosting companies, and domain name registrants with a request to remove the suspicious domain. Infoblox shall also work with other parties as needed to perform these activities.
3	Infoblox shall provide the following to the Customer: ● Infoblox point of contact details. ● A monthly statistical analysis report that outlines the number of takedowns during the month: ○ Date and time of self-identification of site. ○ Date and time of authorization by Customer to commence takedown of site. ○ Date and time of resolution. ○ Complete URL of site. ○ Status of attack. ○ History of all activity related to takedown efforts. ○ Uptime in minutes. ● Infoblox shall provide the takedown case information and after-action report if requested.

DOMAIN MITIGATION SITE TAKEDOWN SCHEDULE

Infoblox shall maintain a cumulative average domestic administrative shutdown time of forty-eight (48) hours or less from for all Customer reported and self-identified websites/domains, excluding Content Removal and Trademark Cases, that have been authorized by the Customer for takedown. If the domestic administrative phishing shutdown time exceeds forty-eight (48) hours from initial contact with Infoblox, it will not count towards the purchased volume of mitigations. Europe, Middle East, Africa, and Asia Internet Service Providers are not bound to this SLA. Domestic is defined as US only. If the international administrative phishing shutdown time exceeds seventy-two (72) hours from initial contact with Infoblox, it will not count towards the purchased volume of mitigations. International is defined as Canada, Mexico, South America, Europe, Middle East, Africa, and Asia

Domain Mitigation Site Takedowns will be initiated* in accordance with the schedule below.

* Initiated is defined as when Infoblox initiates communications with parties capable of appropriately removing the suspicious site. These parties, henceforth referred to as Responsible Parties will include, but are not limited to: Internet Service Providers, Registrars, hosting companies, domain name registrants, foreign CERTS, etc.

- Business Day (M-F, 0800-1900 US Eastern Time)—within fifteen (15) minutes from the time the site is reported by the Customer to Infoblox by sending an email to deactivatenow@infoblox.com or authorized in writing for takedown by the Customer for lookalike sites identified by Infoblox.
- After-Hours (M-F, 1901-0759 US Eastern Time/Saturday/Sunday)—Infoblox initiation* will begin on the next business day following Customer submission to Infoblox by sending an email to deactivatenow@infoblox.com.
- Site Takedown activities will unless otherwise instructed in writing by the Customer start at the initiated time for sites identified by Infoblox. Authorization by the Customer will occur via e-mail. Takedown activities will conclude when either of the following occurs:
    a. The site is no longer available for viewing over the Internet and/or the malicious contents are no longer retrievable by victims.
    b. When Infoblox exhausted all reasonably commercial performed activities to mitigate the fraudulent domain, but the Responsible Parties could not remove the domain from the Internet.

  Site Takedown activities time includes a monitoring period of 30 days after Takedown conclusion time. If any site reactivates within this timeframe's incident time, Infoblox will continue the mitigation process. The Customer will not be charged for the reactivation.
- Infoblox shall continuously monitor all deactivated sites at intervals for a period of 30 days after deactivation; and shall take steps to take down any such site that resurfaces. Infoblox shall notify Customer via email of any sites reactivation if illicit content comes back online.

- Infoblox shall provide Customer on a monthly basis with a report, as per Infoblox standard format, of requested takedown attack information: time of receipt, time of deactivation, cumulative shutdown time, notes of all activities and current status.

2.3 Out of scope activities

Any activity not outlined in section 2.2 is out of scope.

3. Roles and Responsibilities

3.1 Infoblox Responsibilities

- Infoblox shall cooperate with law enforcement agencies as requested by providing law enforcement officials with all necessary information/evidence/data that was collected during the course of the domain mitigation services activities. Infoblox shall notify Customer contacts of any requests for data/sites involving Customer domain mitigation requests.
- All sites identified by Infoblox shall be subject to a written Mitigation Authorization by the Customer before commencement of a mitigation is initiated.
- All phishing sites the Customer reported and authorized for mitigation will be reviewed and verified by Infoblox as fraudulent sites and may be subject to additional verification. Verification may be requested by Infoblox if needed information is not provided by the Customer or content doesn't appear available. In this case, Infoblox shall call Customer contacts or send email notifications that the site is pending mitigation activity within 30 minutes of receiving Customer mitigation request, subject to the schedule outlined in section 2.2.
- Infoblox shall notify the Customer via email of Infoblox-identified sites.

3.2 Customer Responsibilities

- Customer shall provide all available context for authorized mitigations.
- Customer will provide a branded authorization letter to validate the relational authority of Infoblox to contact providers on their behalf.
- The Customer shall have the ability to electronically notify and authorize a Mitigation of a site. This can be done via email to deactivatenow@infoblox.com.
- Customer shall promptly provide any images / logos so Infoblox can document the Customer's associated images and use that in any content removal / trademark related processes.
- Customer shall promptly provide registered trademarks for submission on any trademark related removals. This includes the mark registration numbers and where the marks were registered.

4. Assumptions

Domain Takedown activities on multiple sites on the same domain/subdomain and/or IP will be considered one takedown. Examples include:

- one IP but multiple domains = 1 takedown
- one domain but multiple subfolders = 1 takedown
- one URL but multiple forms = 1 takedown
- one URL redirecting to one landing page = 2 takedowns

- **General Assumptions**
  - Infoblox understands that Customer's services should not be disrupted during identified periods of time; Infoblox will perform the services in a manner designed to avoid such disruption.
  - All non-public information provided by Customer during this engagement is considered confidential, including documentation data, information and conversations associated with the Services.

5. Term

These Terms and Conditions, including for the purpose of clarity the fees will expire within twelve (12) calendar months from the Customer Purchase Order Date (the "Term"), or upon consumption of the 20 Domain Mitigation Site Takedowns, whichever is earlier.

6. Fees and Payment Terms

The project's fees and payment terms are specified in the quote provided to the Customer (where Customer purchased the Services directly from Infoblox), or the quote provided by the Reseller / Distributor to Customer (where Customer purchased the Services from the Reseller / Distributor).

Fees Table

Payment Milestone	Invoice Amount
Upon receipt of Purchase Order	100% of Purchase Order amount

In the case where the Customer purchased Services from a Reseller or Distributor, Infoblox acknowledges that the Customer has made payment or will make payment to the Reseller or Distributor in advance, as per the agreement between Customer and Reseller or Distributor, as applicable.

Infoblox will invoice the Reseller or Distributor (as applicable), in advance, within thirty (30) calendar days of receiving the Purchase Order.

If Customer purchased the Services directly from Infoblox, Infoblox will invoice the Customer for the Services based on the Fees table above, within thirty (30) calendar days of receiving the Purchase Order.

Payment Schedule:

Payments shall be made within thirty (30) business days after receipt of invoice.

Refund and Credit:

Except in the event of termination for Infoblox's material breach, fees are not subject to refund or credit.

Change Order Process:

Any request for services outside the scope of these Terms and Conditions will be documented in a Change Order executed by both parties. The Reseller and Infoblox will agree upon changes in services or costs before executing additional work beyond the defined scope of these Terms and Conditions.

7. Change Management Process

If either party wishes to make changes to these Terms and Conditions, including but not limited to modifying the scope of work, assumptions, dependencies, or fees, such changes will only be effective upon mutual approval and execution of a "Change Order" describing the specific scope changes, possible changes to project timeline, and possible changes to project cost.

Infoblox will have no obligation to provide Services pursuant to a Change Order unless all parties to these Terms and Conditions have executed and signed a Change Order. This ensures that any modifications to these Terms and Conditions are documented and agreed upon by both parties, providing clarity and formalizing the changes to be implemented.

Any requests for services outside the scope of these Terms and Conditions will be documented in a Change Order agreed upon by both parties. A Change Order must be executed before performing such services or incurring costs beyond the scope of these Terms and Conditions.