Minimum Security Requirement for Vendors/ Third Parties in Agreements

These security requirements apply to vendors and third parties that have access to sensitive systems, data, and applications. Some vendors may not have access to systems or applications but access to working areas (e.g. facilities maintenance) and therefore be subject to a subset of these requirements.

- **Non-disclosure agreements.** These agreements shall be in place with all third parties prior to sharing confidential data.
- **Background Checks.** Prior to granting access to confidential data all employees working on behalf of the third party shall be subject to a criminal background check. Results should be evaluated to assure there are no reasonable indication that such employee presents a risk for misuse or threat to Infoblox's confidential data.
- **Security Certifications.** Third party must have appropriate certifications or other designation in relationship to data security and privacy such as ISO 27001: 2013 or SOC 2 Type II.
- **Right to Audit.** Infoblox has the right to audit all third-party vendors at least annually and any time for due cause. These audits can include onsite visits, documentation requests, or use of security questionnaires.
- **Disaster Recovery and Business Continuity.** Disaster recovery and Business Continuity processes shall be established to ensure the ongoing availability of business processes involving access to or use of Infoblox data. Recovery Time Objectives must be appropriate to minimize impact to services provided under this Agreement.
- **Protection of Data.** Proper protections must be put in place to safeguard Infoblox data in place to prevent unauthorized access, alteration, disclosure, or misuse of confidential information processed, stored or transmitted by the third party.
- **Data Destruction.** All confidential data must be wiped from systems/servers when the system is retired. The wipe method must conform to the U.S. Department of Defense standards for data destruction. Removable media must be encrypted if it is used to transfer confidential information. Removable media must be destroyed or returned to Infoblox upon termination or expiration of the Services Agreement.
- **Workstation/ Laptop Encryption.** All workstations, laptops, personal devices, and portable devices (as applicable) that process or store confidential data must be encrypted. As used herein, the term "encryption" or "encrypted" refers to data that has been secured consistent with Federal Information Processing Standards (FIPS) 140-2, and/or the National Institute of Standards and Technology (NIST) publications regarding cryptographic standards.
- **Encryption at Rest and In Transit.** All data at rest and in transmission must be encrypted using an industry standard product and algorithm. Encryption levels shall be maintained at the same level required for PCI certification as published by the Payment Card Industry Council.
- **A Security program in Place that Includes the Following:**
    - **Documented security policies.** All third parties shall have documented security policies based on Industry standards (e.g. ISO 27001:2013 or NIST 800-53).
    - **Secure Configuration**. All third parties must implement system hardening and secure configuration standards (e.g. CIS Benchmarks).
    - **Antivirus.** All endpoints and servers must have a commercial anti-virus software with a minimum daily automatic update of signatures or approved Next Generation antivirus.
    - **Patch Management.** All endpoints and servers must have security patches applied regularly. Critical security patches must be applied within 48 hours of release.
    - **Intrusion Detection.** All systems that are accessible via the Internet or store or transmit any data shall be protected by a suitable intrusion detection and/or prevention system

- **Vulnerability Management.** All servers and applications must be regularly scanned for vulnerabilities, including missing patches, outdated versions of software, and certificate issues. Scans may be run by appropriate internal staff. The vendor must maintain an appropriate vulnerability management program to remediate issues.
- **Penetration Testing.** Internet-facing systems and applications must undergo third-party penetration testing at least annually to identify vulnerabilities, and remediation of all critical or high-risk vulnerabilities must be completed in a timely manner.
- **Security Incident Response.** Third parties must maintain a comprehensive incident response plan for handling security incidents, incident escalation, breach notification, and corrective action plans. This plan must be regularly tested.
- **Information Security Training and Awareness Program**. All persons with access to Infoblox data must be trained on security policies and procedures prior to giving access to Infoblox data. Security and privacy training must be done on an annual basis and results documented. A program of ongoing security awareness must be demonstrated.
- **Access Control.** Role-based access controls will be implemented for all user permissions, enforcing the principle of least privilege.
- **User audit.** Regular audits shall be performed to ensure that terminated users no longer have access to the system and that users who change job roles do not retain permissions which are no longer needed.
- **Log Review.** All systems processing and/or storing Infoblox data shall have a routine procedure in place to review system logs for unauthorized access.
- **Risk Management.** Third party must complete a Third-Party Risk Assessment Questionnaire to provide additional information about the security environment. Any identified gaps will have negotiated remediation deadlines. Also, a risk management program must be implemented which enabled the vendor to prioritize its risks.
- **User IDs and Password Controls**. All authorized users must be issued a unique username. Passwords shall be at least eight characters in length and composed of characters from at least three of the following four groups from the standard keyboard: upper case letters (A-Z), lower case letters (a-z), Arabic numerals (0-9), and non-alphanumeric characters (punctuation symbols). Further, passwords shall not be shared or stored in readable format on a computer, and must be changed at least every 90 days, or immediately if revealed or compromised.
- **Multi- factor Authentication.** Access over the Internet to systems processing Infoblox data must be protected by Multi-factor authentication, such as a one-time passcode.