DYNATRACE SUPPLIER SECURITY POLICY

A. Introduction

1. This document sets forth minimum physical, technical, and organizational security requirements for Suppliers that provide products or services to Dynatrace. Suppliers must know the requirements in this document and ensure compliance by entities working on their behalf (*e.g.*, contractors, processors, and sub-processors).

2. Dynatrace may update this document from time to time. Suppliers must stay informed of any changes. The most current version is available online and is effective when posted.

B. Definitions and Scope

1. Dynatrace Information: any information, content, materials, or data, including personal data, that is provided, generated, or made available by or on behalf of Dynatrace.

2. Supplier: any third party, firm, or individual (collectively, "entities") that provides a product or service to Dynatrace.

3. Authorized Users: Personnel who are authorized to access Supplier's information systems (including, but not limited to, systems that contain Dynatrace Information). Authorized Users may be employed by Suppliers or entities working on their behalf.

C. Physical Requirements

1. Personnel Security: Supplier shall perform appropriate due diligence on its personnel, including background and criminal history checks.

2. Physical Security: Supplier shall, for all locations at which Dynatrace Information is accessed, stored, or processed:

    i. Establish a defined security perimeter, including appropriate security barriers, security cameras, and entry controls.

    ii. Implement CCTV at key points (*e.g.*, entry/exit points and computer rooms), with recordings retained for at least 90 days.

    iii. Ensure that only authorized personnel have physical access to premises where Dynatrace Information is stored.

    iv. Require that visitors be escorted by authorized personnel at all times.

v. Retain physical security access logs.

vi. Implement a “clear desk”/ “clear screen” policy.

3. Environmental Security: Supplier shall, for all locations at which Dynatrace Information is accessed, stored, or processed:

   i. Implement fire detection and suppression systems.

   ii. Protect equipment from power failures and other disruptions caused by failures in supporting utilities.

   iii. Protect equipment against all reasonably foreseeable natural weather phenomena (*e.g.*, hurricanes, floods, etc.).

   iv. Protect all backup and archival media containing Dynatrace Information in secure, environmentally controlled storage areas.

4. Asset Inventory: Supplier shall maintain a register of all hardware, software, and third-party licensing requirements.

5. Asset Removal: Supplier shall have controls for the removal of media containing Dynatrace Information, including:

   i. Media may be removed from designated premises only if specifically authorized by Supplier.

   ii. Supplier shall maintain logs of all media removal.

   iii. Supplier shall take necessary measures to prevent unauthorized access to the media and the Dynatrace Information therein.

6. Asset Re-Use and Disposal:

   i. Supplier shall have a policy and controls for asset re-use and disposal. These controls shall, at a minimum, meet the specifications of NIST Standard 800-88, Revision 1, Appendix A (Minimum Sanitization Recommendations).

   ii. Supplier shall ensure the secure and irretrievable deletion of data, with certificates of destruction.

iii. Supplier shall ensure the secure and irretrievable destruction of paper documents.

D. Technical Requirements

1. Authorization: Supplier shall have an authorization system where different authorization profiles are used for different purposes.

2. Identification:

   i. Supplier shall establish identification and authentication procedures for all access to information systems.

   ii. Every Authorized User shall receive a personal and unique identification code for that purpose ("User ID"). A User ID may not be assigned to another person, even at a subsequent time.

3. Authentication:

   i. Authorized Users shall be allowed to access Supplier's information systems only if they have been provided with authentication credentials.

   ii. Supplier shall ensure that authentication is based on:

      a. a secret password, which is associated with the User ID and is known only by the Authorized User; and

      b. a Multi-Factor Authentication ("MFA") solution, as described below.

   iii. Supplier shall have a procedure to assign, distribute, and store passwords in a manner that ensures password confidentiality and integrity—including storing passwords in a way that makes them unintelligible while they remain valid.

   iv. Supplier shall ensure that passwords shall:

      a. consist of at least 12 characters—or, if this is not technically permitted by the relevant information systems, the maximum number of permitted characters;

      b. not contain any item that can be easily related to the Authorized User;

      c. be modified by the Authorized User to a secret value known only to the Authorized User when it is first used; and

d. be changed by the Authorized User at regular intervals, consistent with NIST Special Publication 800-63.

v. In addition to a valid User ID and password combination, Supplier shall secure all access to information systems by an MFA solution. The MFA solution may be software or hardware in nature.

vi. Supplier shall promptly de-activate an Authorized User's authentication credentials if the Authorized User is terminated, transferred, or de-authorized.

4. Access:

i. Supplier shall enact operating system and database access controls to ensure access only by Authorized Users.

ii. Supplier shall have a logical access control policy that categorizes and restricts access based on job function. Supplier shall review categorizations on at least a semi-annual basis.

iii. Supplier shall maintain an up-to-date record of Authorized Users and the access available to each.

iv. Supplier shall grant Authorized Users access to only Dynatrace Information necessary to provide products or services to Dynatrace.

v. Supplier shall record all Authorized User access to Dynatrace Information, with a secure audit trail retained for at least 180 days.

vi. Supplier shall ensure that only authorized administrators are able to grant, alter, or cancel access by Authorized Users to Dynatrace Information.

vii. Supplier shall periodically review all privileged access authorizations.

5. Segregation Control:

i. Supplier shall ensure logical separation of Dynatrace Information from that of other clients.

ii. Supplier shall provide for separate processing (*e.g.*, storage, modification, access, deletion, and transmission) of Dynatrace Information for different purposes, as follows:

a. Development, testing, and production environments shall be physically or logically separated.

b. Production data shall not be used in non-production environments unless it is necessary, and there is no reasonable alternative. If used, production data shall be anonymized, limited to the extent necessary, and protected by security measures that are proportionate to the sensitivity of the data.

6. Encryption: Supplier shall encrypt Dynatrace Information (including data at rest, data in transit, and backups) as follows:

   i. Supplier shall implement current industry standards for encryption algorithms, minimum key lengths, and secure hashes.

   ii. Minimum key lengths shall be 256 bits (symmetric encryption) and 2048 bits (asymmetric encryption), unless otherwise approved by Dynatrace.

   iii. Supplier shall encrypt all Dynatrace Information transmitted over a public network.

   iv. Supplier shall encrypt all Dynatrace Information on portable media and storage devices (including servers, laptop computers, smartphones, tablet computers, solid state devices, and magnetic tapes).

   v. Supplier shall store encryption keys in a non-tamperable location (hardware security module preferred).

   vi. Supplier shall ensure that access to encryption keys is strictly restricted to named administrators.

7. Data Transmission: For any Dynatrace Information that is transmitted over an electronic communications network:

   i. Supplier shall have measures to control the flow of Dynatrace Information.

   ii. Supplier shall record the timing of the transmission, the Dynatrace Information transmitted, the destination of the transmission, and the Authorized User conducting the transmission.

8. Email:

    i. Supplier shall secure email communications by using either the most current release of Transport Layer Security or one prior version.

    ii. Supplier shall implement anti-spoofing configurations, including SPF, DKIM, and DMARC.

    iii. Supplier shall prohibit auto-forwarding.

9. Virtual Computing: If Supplier will have remote access to Dynatrace systems, networks, or applications, Supplier shall:

    i. Implement and maintain a virtualization solution—with proper configuration and system resources—as selected by Dynatrace.

    ii. Implement full-desk encryption on all systems running the virtualization solution.

10. Data Recovery:

    i. Supplier shall make backups of Dynatrace Information at least daily, and on a more frequent basis if required by the Dynatrace contract with Supplier.

    ii. Supplier shall store backups and data recovery procedures in a different location than (but the same region as) the information systems that process Dynatrace Information.

    iii. Supplier shall encrypt backups if they are transferred or stored off-site.

    iv. Supplier shall have procedures to ensure that, in the event of data loss or destruction, Dynatrace Information is restored promptly without material data loss.

11. Vulnerability Identification and Remediation:

    i. Supplier shall periodically review the hardware, firmware, and software used in information systems to identify security vulnerabilities.

    ii. Supplier shall conduct annual penetration tests.

    iii. Supplier shall remediate identified security vulnerabilities promptly, in accordance with the severity and criticality of each vulnerability.

12. Information System Security: Supplier shall employ:

    i. Threat intelligence monitoring: continuous monitoring and analysis of emerging threats, attacks, and vulnerabilities.

    ii. System monitoring: logging of all events that may assist in the identification or investigation of security incidents.

    iii. Intrusion Detection Systems ("IDS"): tools to identify unauthorized access to Dynatrace Information, as well as actual and potential attacks on the network and anywhere Dynatrace Information is stored, processed, or accessed. IDS shall reflect industry best practice.

    iv. Firewalls: Routing of all traffic networks owned or managed by a third party through a firewall and ensuring secure connections between internal and external systems. Firewall configuration shall include anti-spoofing, prevention of source routing, an inactivity timeout, and the disablement of packet forwarding and the ANY-ANY rule.

    v. Malware protection: tools and processes to detect, protect against, and remove malware.

    vi. Security patches: Timely implementation of security patches and other vulnerability updates.

    vii. Change control: procedures to ensure that modifications to the production environment (*e.g.*, application, operating system, and hardware level changes) protect the confidentiality, integrity, and availability of information systems

    viii. Emergency change control: procedures to ensure that emergency access to the production environment and the introduction of unscheduled changes occur only with appropriate authorization.

E. Organizational Requirements

1. Overview: Supplier shall have an organizational framework, adopted by executive leadership, and written policies and procedures that establish an appropriate and accountable information security organization and ensure the proper training and competent performance of its personnel.

2. Chief Information Security Officer:

    i. Supplier shall have a Chief Information Security Officer ("CISO"), or someone in a comparable position, who is suitably trained and experienced

in managing information security and provided with appropriate resources.

ii. The CISO or comparable person shall be responsible for the overall compliance with the requirements set forth in this document.

iii. The contact details of the CISO or comparable person shall be provided to Dynatrace upon request.

3. Information Security Policies and Procedures:

   i. Supplier shall maintain information security policies and procedures that address:

      a. Physical security, including:

         1. The security of premises.

         2. The security of equipment and telecommunications systems.

         3. Environmental security.

         4. The physical security requirements described herein.

      b. Technical security, including:

         1. The security and maintenance of telecommunications systems, computers, software, databases, and removable media.

         2. Secure software development (including design, implementation, and maintenance).

         3. The security of connecting systems to the Internet.

         4. The security of encryption keys, passwords, and other signals and codes.

         5. Malware identification, containment, and removal.

         6. Vulnerability identification and remediation.

7. The identification and prevention of unauthorized attempts to access systems and applications.

8. Backups and data recovery.

9. The technical security requirements described herein.

c. Organizational security, including:

1. Defined responsibilities for personnel regarding data protection and information security.

2. Data retention and disposal.

3. The organizational security requirements described herein.

ii. Supplier shall maintain the policies and procedures in a manner that is accessible to appropriate personnel.

iii. Supplier shall review the policies and procedures at least annually, and whenever material changes are made to information systems or to physical, technical, or organizational measures.

4. Incident Response Plan:

i. Supplier shall maintain a plan for reporting, responding to, and managing security incidents. The plan shall include, at a minimum:

a. A detailed specification of protected resources (including, but not limited to, “crown jewels” analysis).

b. Procedures for reporting and escalating incidents to appropriate management.

c. A designated team, led by the CISO or comparable person, which manages and coordinates incident response.

d. Recordkeeping requirements, including the time the incident occurred, the person reporting the incident, the impact of the incident, mitigation measures and the effects thereof, and other material facts.

e. Remediation standards for different types of foreseeable security incidents (*e.g.*, malware, DDoS, etc.).

f. The requirement to notify Dynatrace, as specified in the Dynatrace contract with Supplier, if an incident results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Dynatrace Information.

g. The requirement to work with Dynatrace where appropriate until such security incident has been satisfactorily resolved.

h. Procedures for recovering Dynatrace Information, including recording the personnel who undertook recovery activities, the data restored, and if data needed to be input manually during the recovery process.

ii. Supplier shall maintain the incident response plan in a manner that is accessible to appropriate personnel, including during a security incident.

iii. Supplier shall review the incident response plan at least annually, and whenever material changes are made to information systems or to physical, technical, or organizational measures.

iv. Supplier shall test the incident response plan at least once a year.

5. Business Continuity and Disaster Recovery: Supplier shall maintain business continuity and disaster recovery plans. Each plan shall be exercised on at least an annual basis and shall contain a recovery time objective (RTO) and a recovery point objective (RPO).

6. Artificial Intelligence: If Supplier is authorized by Dynatrace to provide products or services that use or rely on machine learning, deep learning, large language models, neural networks, or other similar models or artificial intelligence capabilities (collectively, "AI"), then Supplier shall employ a risk management program that implements the NIST AI Risk Management Framework and is sufficient to identify, reduce, mitigate, and remedy any risks associated with reasonably foreseeable misuse of AI.

7. Training: Supplier shall train personnel regularly on:

i. Applicable law (*e.g.*, cybersecurity, data privacy, and data protection).

ii. Relevant security policies and procedures.

iii. How to report and escalate security incidents.

iv. For personnel who have access to Dynatrace Information, the requirements in this document.

v. The consequences of violating the foregoing, with disciplinary measures clearly documented and communicated.

8. Contractors and Processors: Supplier shall perform adequate due diligence and implement appropriate controls on all entities working on its behalf (*e.g.*, contractors, processors, and sub-processors). These measures shall include, for each entity:

   i. A pre-onboarding review of the entity's information security and data protection program for fitness and suitability.

   ii. A written agreement that sets forth the requirements in this document and other appropriate obligations.

   iii. A requirement that entities receiving Dynatrace Information shall: (a) use and grant access to such information only as necessary to provide products or services to Dynatrace; and (b) anonymize or mask such information to the greatest extent possible.

   iv. Reviews—on at least an annual basis—to ensure compliance with the requirements in this document.

9. Supplier Security Policy Review:

   i. Supplier shall review its compliance with the requirements in this document at least annually, and whenever material changes are made to this document or to Supplier's information systems or physical, technical, or organizational measures.

   ii. As part of the review, Supplier shall assess the extent to which its security measures and controls comply with these requirements, identify any gaps, and propose corrective or supplementary measures as necessary.

10. Audit:

    i. Supplier shall have an annual program to audit its information security and data protection program against suitable industry standards, such as NIST CSF, SOC1 Type II, SOC2 Type II, and similar programs.

ii. Supplier shall provide copies of certifications to Dynatrace upon request.