DYNATRACE SUPPLIER SECURITY MEASURES

The technical and organizational security measures implemented by Vendor and each Vendor Affiliate shall, as a minimum, include the following:

1. **Data protection and information security governance:** a documented framework, approved bysenior management, which includes:
    a) Assigning clear accountability for data protection and information security governance.
    b) A clear data protection and information security policy.
    c) Defined responsibilities for data protection and information security (which are also communicated to all relevant staff).
    d) Data protection training for all staff that will have access to Personal Data.
    e) Staff awareness of the need to escalate any security incidents.
    f) A data incident management process.
    g) Defined and audited access controls for Personal Data.
2. **Staff security:** reasonable steps to ensure the reliability of all staff who will have access to Personal Data, including background checks.
3. **Subcontractors:** performance of adequate Vendor due diligence (both pre- and post-contract), including entering into a written agreement with each Subcontractor that imposes appropriate obligations on that Subcontractor in respect of Personal Data.
4. **Asset Management:** maintaining an asset register of hardware and software and ensuring third party software licensing requirements are met.
5. **Disposal of Redundant Equipment, Media, and Data:** processes to ensure the secure and irretrievable deletion of data and/or destruction of redundant IT assets with certificates of destruction, and secure and irretrievable destruction of paper documents.
6. **Physical Security:** for locations at which Personal Data is stored and processed:
    a) Use of a defined security perimeter, appropriate security barriers, security cameras andentry controls.
    b) CCTV at key points e.g., entry/exit points and computer rooms. Retention of recordings ofimages for 90 days.
    c) Maintenance physical security access logs.
    d) Requirement for visitors to be escorted.
    e) Clear desk/clear screen policy.
7. **Environmental Security:**
    a) Protection of equipment from power failures and other disruptions caused by failures in supporting utilities, and fire detection and suppression systems in data centers that store Personal Data.
    b) Protection of all backup and archival media containing Personal Data in secure environmentally controlled storage areas.
8. **Access Controls:**
    a) Granting of access to Personal Data only to those staff who reasonably need it for thepurposes of delivering the Services and in accordance with their role or function.
    b) Timely removal of access to Personal Data when no longer required.

c) Access to Personal Data to be authenticated.

d) Effective password management including complexity requirements.

9. **Information Systems Security:**

a) System Monitoring: logging key events that may assist in the identification or investigation of data incidents.

b) Intrusion Detection: deployment of intrusion detection tools to identify potential attacks on the network.

c) Backups: daily backups of the system to enable data restoration. Backups must be encrypted if they are transferred or stored offsite.

d) Firewalls: Routing all traffic networks owned or managed by a third party through a firewall, that also ensures secure connections between interna! and externa! systems.

e) Wireless Access: authentication and encryption protocols for permitting access to information systems.

f) Malware Protection: processes to detect and protect against malware.

g) Separation of data: logical separation of clients' data.

h) Security patches: Timely implementation of security patches and other relevant security vulnerability updates unless this introduces higher business risks.

i) Vulnerability management: process to regularly identify and remediate security vulnerabilities.

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

k) Emergency changes: procedures for authorizing emergency access or introducing unscheduled changes to the production environment.

10. **Encryption:**

a) Adoption of standards for encryption and secure hashes that mandate currently accepted encryption algorithms and key lengths. For symmetric encryption, the minimum key length shall be 128 bits.

b) Encryption of Personal Data transmitted over a public network.

c) Encryption of Personal Data on portable media and all storage devices (including servers, laptop computers, smartphones, tablet computers, solid state devices and magnetic tapes).

11. **Segregation control:** Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

a) The environments used for development, testing and production purposes are physically separated.

b) Usage of un-anonymized production data on development environment is not allowed.

12. **Business continuity and disaster recovery:** implementation of business continuity and disaster recovery plans, which are exercised annually.

13. **Annual Information Security Audits:** adherence to an annual program to audit its information security and compliance against industry-standards such as ISO 27011, SOC2 Type II, or similar programs.