SUMMARY OF HP SECURITY MEASURES

_____

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures and organizational structures to protect the confidentiality, integrity and availability of its own and its Customers' information (including Personal Data as defined in HP's Customer and Data Processing Addenda). The following sets forth an overview of the technical/organizational security measures deployed by HP throughout the company.

1. Security Policy

HP maintains globally applicable policies, standards, and procedures intended to protect HP and Customer data. The detail of HP's security policies are confidential to protect the integrity of HP's data and systems. However, summaries of our key policies are included below.

2. Information Security Organization

HP has an Information Security Organization that is responsible for directing and managing the information security strategy and controls adopted by the organization.   An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls as well as to confirm that the security requirements of its Customers are complied with. This Framework is structured in alignment with the NIST Cybersecurity Framework and is reviewed annually.

3. Asset Management

HP has a process in place for identifying technical information assets and through this process HP identifies all assets under its responsibility and categorizes the critical assets.   HP further maintains a set of documented handling procedures for each information classification type including those assets that contain Personal Data. Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

4. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HP's password policy has defined complexity, strength, validity and password-history related controls.   Access rights are reviewed on a periodic basis and revoked upon personnel departure.

User account creation and deletion procedures as have been mutually agreed upon are implemented, for granting and revoking access to client systems that are used during the course of the engagement.

5. Personnel Training

HP employees are required to complete the Integrity at HP training which is designed to ensure that new employees are familiar with the program, policies, and resources that govern HP expectations for ethical behavior, excellence, and compliance. Integrity at HP features modules on security and data privacy and employees also are required to take an annual "refresher" course. HP employees also undergo a periodic

security awareness training focused on essential security policies and emphasizing the user responsibilities related to incident management, data privacy and information security.

6.   Third Parties and Subcontractors

HP has processes in place to select sub-contractors that are able to comply with comprehensive contractual security requirements.

7.   Systems Security

By policy, development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, which include modules, libraries, services, and discrete components, are evaluated to determine their impact on the overall system security state.

HP has defined controls for the protection of application service transactions. These controls include: validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed both on a quarterly basis and after any significant change.

8.   Physical and Environmental Security

HP facilities are secured using various combinations of physical and electronic access controls and surveillance capabilities. Depending on the facility, this could include security guards, electronic access control and closed-circuit television (CCTV).

All HP personnel are registered and are required to carry appropriate identification badges.

Facilities have required infrastructure support with temperature control and power backups where required, using UPS and / or diesel generators to support critical services.

9.   Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure which includes workstations, servers and network equipment. Workstation / servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented.

HP has deployed Network Intrusion Detection / Prevention Systems (NIDS/ NIPS) within the network and are monitored and managed 24*7.

HP security policies and standards mandate secure disposal of media.

10. Cryptography

HP has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets including those that contain personal data.

May 2018

12. Information Security Incident Management

HP follows a developed Cyber Incident Management Process that addresses purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. HP reviews and updates this process on an annual basis.

A Cyber Incident Response Team, which includes HP Cybersecurity personnel trained in incident response and crisis management, is assembled for regular table-top reviews of process and any incident or event.

13. Business Continuity Management

HP maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach for end-to-end continuity through a set of collaborative, standardized, and internally documented planning processes.

HP periodically exercises its business continuity plans to ensure effectiveness of the plans. HP currently tests and updates all plans at least yearly, as well as ensures that people with a role in the business continuity plan are trained.