Palo Alto Networks Information Security Measures

1. Scope

Taking into account the nature, scope, context, and purposes of processing, the state of the art, the costs of implementation, as well as the risk of varying likelihood and severity of the rights and freedoms of natural persons, this document describes the Information Security Measures ("Measures") that Palo Alto Networks has in place when processing Personal Information and End User Data by any Palo Alto Networks Product. Customer agrees that the terms set forth in these Measures are appropriate technical and organizational measures to protect Customer's Personal Information and End User Data.

2. Definitions

a. "Customer" means the entity that entered into the Agreement with Palo Alto Networks.

b. "End User Data" means data that may be collected by Products during the relationship governed by the Agreement, in the form of logs, session data, telemetry, user data, usage data, threat intelligence data, and copies of potentially malicious files detected by the Product. End User Data may include confidential data and Personal Information, such as source and destination IP addresses, active directory information, file applications, URLs, file names, and file content.

3. Security Management

a. Security Program. Palo Alto Networks maintains a written information security program that:

i. is managed by a senior employee responsible for overseeing and implementing the program;

ii. includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Personal Information and End User Data; and

iii. is appropriate to the nature, size, and complexity of Palo Alto Networks' business operations.

b. Personnel Security. Palo Alto Networks will engage a reputable, commercially recognized background check or investigative entity to conduct background checks in compliance with applicable laws.

i. For US employees only, the background check will include a federal and county criminal conviction check in the counties of residence in the previous seven (7) years for felony and misdemeanor convictions, pending charges, and outstanding warrants, employment in the last seven (7) years, the highest degree of education, and global blacklists.

ii. For non-US employees only, the background check will include a check against global blacklist for all countries, and criminal background checks in certain countries, according to Palo Alto Networks' risk assessment standards and applicable law. Palo Alto Networks will ensure that all employees have the reasonable skill and experience suitable for employment and placement in a position of trust and trained with respect to Palo Alto Networks security policy and procedures.

c. Due Diligence on Sub-Contractors. Palo Alto Networks will:

i. maintain a security process to conduct appropriate due diligence prior to engaging subcontractors;

ii. assess the security capabilities of any such subcontractors on a periodic basis to ensure subcontractors' ability to comply with the Measures described in this document;

iii. apply written information security requirements that oblige subcontractors to adhere to Palo Alto Networks' key information security policies and standards consistent with and no less protective than these Measures.

4. Physical Security

a. General. Palo Alto Networks restricts access to, controls, and monitors all physical areas where Palo Alto Networks Products process Personal Information and End User Data ("Secure Areas") and maintains appropriate physical security controls on a 24-hours-per-day, 7-days-per-week basis ("24/7"). Palo Alto Networks revokes any physical access to Secure Areas promptly after the cessation of the need to access buildings and system(s).

b. Access and Authorization Processes. Palo Alto Networks maintains a documented access authorization and logging process. The authorization and logging process will include at minimum:

i. reports detailing all access to Secure Areas, including the identities and dates and times of access;

ii. video surveillance equipment to monitor and record activity at all Secure Areas entry and exit points on a 24/7 basis to the extent permitted by applicable laws and regulations.

c. Data Centers. To the extent Palo Alto Networks is operating a data center, Palo Alto Networks complies with physical security controls in alignment with industry standards such as ISO 27001 and SSAE 16 or ISAE 3402 or similar standard.

5. Logical Security

a. Systems Access Control and Network Access Control.

i. Palo Alto Networks employs access control mechanisms that are intended to: (a) prevent unauthorized access to Personal Information and End User Data; (b) limit access to users who have a need to know; (c) follow the principle of least privilege, allowing access to only the information and resources that are necessary; and (d) have the capability of detecting, logging, and reporting access to the system and network or attempts to breach security of the system or network.

ii. Palo Alto Networks users have an individual account that authenticates that individual's access to Personal Information and End User Data. Palo Alto Networks does not allow sharing of accounts. Access controls including passwords are configured in accordance with industry standards and best practices.

iii. Palo Alto Networks maintains a process to review/audit controls (including access controls) on a minimum annual basis for all Palo Alto Networks systems that transmit, process, or store Personal Information and End User Data.

iv. Palo Alto Networks configures remote access to all networks storing or transmitting Personal Information and End User Data to require multi-factor authentication for such access.

v. Palo Alto Networks revokes access to systems and applications that contain or process Personal Information and End User Data promptly after the cessation of the need to access the system(s) or application(s).

b. Telecommunication and Network Security.

i. Palo Alto Networks deploys firewall technology in the operation of the Palo Alto Networks' sites. Traffic between Customer and Palo Alto Networks will be protected and authenticated by industry standard cryptographic technologies.

ii. Palo Alto Networks deploys an intrusion detection system to generate, monitor, and respond to alerts which could indicate potential compromise of the network and/or host.

iii. Palo Alto Networks implements network segmentation between the corporate enterprise network and hosting facilities for Personal Information and End User Data. Within hosting facilities, we apply separation between environments dedicated to development, staging, and production, with multiple layers of access.

c. Malicious Code Protection.

i. Excepting specific servers dedicated to analysis of compromised End User Data, Palo Alto Networks workstations and servers run the current version of industry standard antivirus/anti-malware software with the most recent updates available on each workstation or server. Virus definitions are updated within twenty-four (24) hours of release by the software vendor. Palo Alto Networks configures such equipment and has supporting policies to prohibit

users from disabling anti-virus/anti-malware software, altering security configurations, or disabling other protective measures put in place to ensure the safety of Personal Information and End User Data. Palo Alto Networks has anti-virus/anti-malware software configured to run real-time scanning of machines and a full system scan on regularly scheduled intervals.

ii. Palo Alto Networks scans incoming and outgoing content for malicious code on all gateways to public networks, including, but not limited to, email and proxy servers.

d. Data Loss Prevention. Palo Alto Networks employs a comprehensive system to prevent the inadvertent or intentional compromise of Personal Information and End User Data.

6. Software Development and Maintenance

a. Security by Design. Palo Alto Networks applies security by design principles throughout the software development lifecycle, at the design and architecture level, by conducting security design review and threat modeling, using the STRIDE methodology.

b. Open Source. Palo Alto Networks evaluates and tracks vulnerabilities of open source software (OSS) and other 3rd party libraries that are incorporated into the Products; Palo Alto Networks performs static code analysis and manual code review, as required by risk. Security verifications, including penetration testing and multiple dynamic analysis tools, are conducted by third-party firms, red teams, and threat researchers.

c. Change Management. Palo Alto Networks employs a documented change management program with respect to the Products as an integral part of its security profile. This includes logically or physically separate environments from production for all development and testing.

d. Vulnerability Management and Application Security Assessments. Palo Alto Networks runs internal and external network vulnerability scans at least quarterly and after any material change in the network configuration. Vulnerabilities identified and rated as critical risk are remediated or mitigated promptly after discovery.

In addition:

i. For all Internet-facing applications that collect, transmit or display Personal Information or End User Data, Palo Alto Networks conducts an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security, including, but not limited to, a penetration test of the application, as well as a code review.

ii. For all mobile applications (i.e. running on Android, Blackberry, iOS, Windows Phone) that collect, transmit or display Personal Information or End User Data, Palo Alto Networks

conducts an application security assessment review to identify and remediate industry-recognized vulnerabilities specific to mobile applications.

iii. Palo Alto Networks utilizes a qualified third party to conduct the application security assessments. Palo Alto Networks may conduct the security assessment review directly, following industry standard best practices.

7. Storage, Handling and Disposal

a. Data Segregation. Palo Alto Networks physically or logically separates and segregates Personal Information and End User Data from its other customers' data.

b. Encryption of Electronic Form Data. Palo Alto Networks utilizes strong industry standard encryption algorithms and key strengths (i.e., AES 256-bit at rest, TLS v1.2 in transit) to encrypt all Personal Information and End User Data in electronic form while in transit over all public wired networks (e.g., Internet) and all wireless networks.

c. Destruction of Data. Personal Information and End User Data is disposed of in a method that renders the data unrecoverable, to the extent reasonably possible, in accordance with industry best practices for wiping of electronic media (e.g. NIST SP 800-88). Palo Alto Networks destroys any equipment containing Personal Information and End User Data that is damaged or non-functional.

8. Business Continuity and Disaster Recovery

a. Palo Alto Networks develops, implements, and maintains a business continuity management program to address the needs of the business and Products provided to the Customer. To that end, Palo Alto Networks completes a minimum level of business impact analysis, crisis management, business continuity, and disaster recovery planning.

i. Palo Alto Networks' Business Impact Analysis Plan includes, but is not limited to, a systematic review of business functions and their associated processes that identifies dependencies, evaluates potential impact from disruptions; defines recovery time objectives, and improves process understanding improvement, performed annually.

ii. Palo Alto Networks' Crisis Management Plan includes, but is not limited to, elements such as event management, plan and team activation, event and communication process documentation, exercised at least annually.

iii. Palo Alto Networks' Business Continuity Plan includes, but is not limited to, elements such location work-arounds, application work-arounds, vendor work-arounds, and staffing workarounds, exercised at minimum annually.

iv. Palo Alto Networks' Disaster Recovery Plan includes, but is not limited to, infrastructure, technology, and system(s) details, recovery activities, and identifies the people/teams required for such recovery, exercised at least annually.

b. Plan Content. Palo Alto Networks' plan documentation under 8.a. addresses actions that Palo Alto Networks will take in the event of an extended outage of service. Palo Alto Networks ensures that its plans address the actions and resources required to provide for (i) the continuous operation of Palo Alto Networks, and (ii) in the event of an interruption, the recovery of the functions required to enable Palo Alto Networks to provide the Products, including required systems, hardware, software, resources, personnel, and data supporting these functions.