EXHIBIT [insert applicable number or letter designation]

LENOVO PRIVACY AND SECURITY REQUIREMENTS ("Requirements")

1. SCOPE

These Requirements apply to suppliers who are providing goods and/or services ("**Company**") to Lenovo PC HK Ltd. and its Affiliates (collectively, "**Lenovo**") and Company's performance of its obligations under all agreements with Lenovo ("**Agreements**") with respect to Lenovo's Proprietary Information (defined below). In the event of an inconsistency or conflict between these Requirements and the terms in the applicable Agreement, these Requirements will control, but only to the extent of such inconsistency or conflict.

2. DEFINITIONS

Access: To view, collect, store, record, adapt, alter, use, process, maintain, transfer, disclose or dispose of Proprietary Information.

***Confidential Information*:** Information that includes, but is not limited to, data or materials of Lenovo business practices and concepts; business and marketing plans; partner, customer or supplier relationships; costs, prices and pricing methods; financial results, forecasts and projections; and technical data, schematics, analyses, ideas, methods, trade secrets, processes, know-how, prototypes, designs, specifications, techniques, and drawings.

Data Breach: The unauthorized Access, loss, disclosure, use or damage of Personal Data.

Information Incident: The unauthorized Access, loss, disclosure, use, damage of Proprietary Information. Includes, but is not limited to, an actual or suspected Data Breach.

Personal Data: Information consisting of personally-identifiable information collected from or about any individuals who may include, but are not limited to, Lenovo employees, their family members, job applicants, customers, consumers, contacts, suppliers, and partners or potential partners. Personal Data includes Regular Personal Data and Sensitive Personal Data.

Personnel: Employees, agents or contractors engaged or appointed by Company or its affiliates that may Access Proprietary Information.

Proprietary Information: Confidential Information or Personal Data provided by Lenovo to Supplier; or Supplier to Lenovo. Lenovo Proprietary Information also includes information collected or created by Supplier on behalf of Lenovo for furtherance of its performance under this agreement. Proprietary Information shall be marked or identified at the time of disclosure as "Confidential", "Restricted", "Proprietary" or with a similar designation.

Regular Personal Data: Basic Personal Data including, without limitation, first, middle or last names; home or business addresses; home or business email addresses; home, mobile or business telephone numbers; employee ID numbers; photographs; and partial dates of birth. Regular Personal Data does not include Sensitive Personal Data.

Sensitive Personal Data: Special categories of Personal Data that includes data defined by law as requiring special care or handling, including the following, without limitation, racial or ethnic origin; religious or philosophical beliefs; political affiliations/opinions; trade union membership; health data; sexual orientation; gender identity; disabilities; background checks; U.S. Social Security Numbers (SSNs) and similar government/national identification numbers (including tax identification numbers); Credit/Debit Card numbers and similar bank/financial account information; passwords and other authentication and authorization credentials; biometric identifiers; geolocation information; web browsing histories, the history of applications installed and used on an individually identifiable device; and complete dates of birth (year+month+day). Sensitive Personal Data does not include Regular Personal Data.

Subcontractor: *A party* to whom Company delegates a function, activity, or service that may involve Access to Proprietary Information.

3. ACCESS TO PROPRIETARY INFORMATION

Company acknowledges that Proprietary Information is and will remain the exclusive property of Lenovo. Company may Access Proprietary Information only to fulfill Company's obligations under an agreement, as otherwise expressly permitted under an agreement, or pursuant to Lenovo's written instructions and for no other purpose. Lenovo will be entitled to take reasonable steps to ensure that Company will only receive Proprietary Information if Company needs to Access Proprietary Information to perform its obligations under an Agreement.

4. PRIVACY

4.1 **Legal Compliance**. Company will comply with all applicable laws regarding privacy, confidentiality, data protection, data security, data breach notification and marketing communications methods.

4.2 **Use, Disclosure and Transfer.** Company will not use, disclose, or transfer across borders Personal Data except to the extent it is necessary to perform under this agreement.

4.3 **Notice and Consent**. If Company will collect Personal Data under this agreement, Company will provide notice to individuals and obtain consent from individuals prior to any Personal Data collection. Sensitive Personal Data requires explicit consent rather than implicit consent. To the extent applicable, Company acknowledges and will comply with the promises and representations made in Lenovo's customer privacy statement, which is located at http://www3.lenovo.com/us/en/privacy/.

5. SECURITY

Company will maintain a comprehensive and documented security program compliant with the latest applicable International Organization for Standardization (ISO) security controls and standards and consisting of appropriate administrative controls, physical controls, and technical Controls (collectively, "**Controls**") that: (i) are designed to address any reasonably foreseeable threats to the confidentiality and security of Proprietary Information; (ii) protect such information from any unauthorized Access, data errors, loss of Access, or service disruption; (iii) limit the Access to such information in accordance with the provisions below; and (iv) are appropriate to Company's role, operations and exposure to Proprietary Information. Upon request, Company will provide Lenovo in writing with confirmation and independent verification that it has implemented and maintains controls and other requirements set forth herein. Company's Controls will include, at minimum, the following specific Controls. Company will ensure that all its Personnel and Subcontractors strictly comply to the controls described herein.

5.1 Company's Controls

(i) **Periodic Risk Assessment.** Company will implement and maintain, throughout the term of the applicable Agreement, a risk assessment program, which will include: (i) periodic assessment of Proprietary Information to identify risks of unauthorized Access; (ii) adoption of reasonable controls, procedures and training to address reasonably foreseeable risks; and (iii) evaluation and possible adjustment of Company's risk assessment program in the event of (A) an Incident, (B) changes in circumstances that reasonably implicate the security or confidentiality of such information, or (C) notification by Lenovo of a reasonably foreseeable risk that Lenovo believes needs to be addressed.

(ii) **Supervision and Training.** Company will provide the required level of training of, and supervision over, relevant Personnel and relevant Subcontractors to ensure appropriate implementation of and compliance with Controls applicable to Proprietary Information.

(iii) **Access Control**. Company will limit Access to Proprietary Information to Company's Personnel and Subcontractors who: (i) have a need to Access such information in order to perform Company's obligations under an applicable agreement; (ii) have been properly

background checked/screened; (iii) have completed Company's training and any other applicable training prepared by Lenovo on the required Controls; and (iv) have agreed in writing to be bound by an Agreement that requires compliance with Company's Controls.

(iv) **Access Control Lists.** Company will maintain a written list of all Personnel and Subcontractors to whom Company has granted Access to Proprietary Information at any time during the term of an applicable agreement. Company will update and maintain the accuracy of such lists at all times during such term, and after expiration or termination of an Agreement if Company has continuing Access to or possession, custody or control of Proprietary Information, and will provide copies of said lists to Lenovo promptly upon request.

(v) **Transmission Across Networks**. Company only will Access Proprietary Information using secured, access controlled business networks. Company will not use personal email addresses, public email systems, public or free file exchanges, or public or free web sites to exchange Proprietary Information.

5.2 **Encryption**

(i) **Portable Devices.** Company will encrypt all Proprietary Information Access on portable devices or media, including but not limited to laptop computers, servers, mobile devices, hard drives, disks, backup tapes or other such electronic storage media using, at a minimum, an industry standard and community-vetted encryption implementation, with certificates. Such portable devices will be password protected and have active and operational antivirus protection where available. If Company will be Accessing Proprietary Information on portable devices where encryption is not technically feasible, Company will obtain Lenovo's express written approval prior to storing said information on unencrypted portable devices.

(ii) **Transport.** Except as otherwise provided above, Company will encrypt all Proprietary Information Accessed on any physical or logical media, before that media is stored or transported outside of Lenovo's or Company's physically secured facilities, using an industry standard and community-vetted encryption implementation. Except as otherwise provided above, Company will encrypt all Proprietary Information stored on any physical or logical media, before that media is stored or transported outside of Lenovo's or Company's physically secured facilities, using only the latest available encryption methods, with certificates.

(iii) **Transmission.** Company will encrypt all transmissions of Proprietary Information across all networks not operated or used exclusively by Company using an industry-standard and community-vetted encryption implementation, with certificates.

(iv) **Exclusions.** Notwithstanding the other provisions in this Section, Company will not be required to encrypt hard copy documents containing Proprietary Information, or to encrypt such information where prohibited by an applicable law, but will take appropriate steps to secure such documents from unauthorized Access as set forth herein.

5.3 **Physical Facilities and Systems.** To the extent that Company Accesses Proprietary Information in physical facilities or using services, systems, computers, devices or media that are owned or managed by Lenovo or Lenovo's designated outsourcing suppliers, Company will require that its Personnel and its Subcontractors conduct themselves in a manner compliant with all internal Lenovo policies provided to Company that are relevant to the use of those facilities, services, systems, computers, devices or media and will require that all relevant Personnel and Subcontractors are aware of and comply with such policies. To the extent that Company Accesses Protected Information in physical facilities or using services, systems, computers, devices or media that are not owned or managed by Lenovo, Company's Controls will include the following:

(i) **Appropriate Physical Security Requirements.** Company will implement and maintain appropriate controls to prevent unauthorized physical Access to Proprietary Information, and the systems, computers, devices or media containing this information. All exterior doors and windows will be protected with industry standard security locks and monitored 24x7 by an industry standard alarm system. All exterior doors will be monitored 24x7 by video cameras. All computer rooms and closets will be protected by industry standard security locks and will be monitored 24x7 by video cameras. All computer rooms or closets will be monitored for unauthorized entry and have restricted Access.

(ii) **Appropriate Systems Security Requirements.** Company will implement and maintain reasonable controls to prevent unauthorized Access to any system, computer, device or media used by Company to Access Proprietary Information. The controls will meet or exceed industry standards, including the following: (i) reasonable account and system access controls, including strong passwords (e.g., following password generation guidelines established by NIST or CERT) to secure any accounts with Access to Proprietary Information; (ii) reasonable malware controls, including the installation, regular update and routine use of both antivirus and antispyware software products on all systems, computers, devices or media with Access to Proprietary Information; and (iii) reasonably up-to-date software, including appropriate maintenance of Company's operating system(s) and other applicable software, and successful installation of reasonably up-to-date security patches on all systems, computers, devices with Access to Proprietary Information.

(iii) **Assessment and Reporting.** Assets that may contain Proprietary Information must have regular inventory reports. In the event that an asset is identified as missing, it will be deemed as an Information Incident and must be reported and documented pursuant to Section 6 herein.

5.4 **Vulnerability Management.**

(i) **Vulnerability Assessments.** Company will perform regular vulnerability assessments (including scans for network access), at least annually, of all infrastructure, applications and other dependencies used in connection with Company's performance of its obligations under an Agreement.

(ii) **Logs.** Company will create and retain for a reasonable period logs and audit records reasonably sufficient to reconstruct all access, authentication and authorization events pertaining to Proprietary Information Accessed by Company and its Subcontractors.

(iii) **Internal Firewall**. If any Company projects exist that are competitive to the Lenovo-specific project that is the subject of this agreement, Company will maintain an internal firewall prohibiting Access to Proprietary Information by any Company Personnel or Subcontractors that work on such competitive projects for at least as long as the competitive projects exist.

(iv) **Disaster Recovery.** If Company will Access Proprietary Information using its own systems, Company will maintain a written disaster recovery program that documents business impact assessments, contingency plans, and recovery procedures. Company will review, update and test its program regularly in accordance with changing technologies, conditions, and operational requirements. Company and Lenovo will determine and agree on prioritized recovery objectives and ensure that Lenovo's and Company's programs are compatible. Any occurrence or omission that causes Company to activate its disaster recovery program will qualify as an Incident as described by Section 6 below.

5.5 **Security Assessment.**

(i) **Cooperation**. Company will cooperate with reasonable efforts by Lenovo to assess the sufficiency, in Lenovo's commercially reasonable judgment, of Company's Safeguards. As part of such an assessment, Company will provide Lenovo with accurate information as Lenovo may reasonably request, respond to reasonable information inquiries, and make Company representatives reasonably available to answer questions.

(ii) **Annual Assessment**. With reasonable prior written notice, Lenovo may initiate annually, a non-intrusive, general assessment conducted pursuant to the terms of this Section.

(iii) **Specific Assessments**. Lenovo may initiate an assessment concerning specific Company Controls and other requirements herein to respond to or otherwise manage an Incident or a change in circumstance that presents reasonably foreseeable risks to the security or confidentiality of Proprietary Information. Company will cooperate with such an assessment on an expedited basis.

(iv) **Assignment.** Lenovo may, in its sole discretion, assign its own employees or independent third parties acting on its behalf to perform assessments described in this section. If Lenovo chooses to employ a third party, Lenovo will ensure that the third party has agreed to terms of confidentiality with respect to any Company-provided information no less restrictive than as apply to Lenovo.

(v) **Confidentiality**. Lenovo agrees to treat information provided by or on behalf of Company or gathered by Lenovo as part of an assessment of Company hereunder as confidential and with appropriate care as obligated under the confidentiality terms of the applicable Agreement.

6. INFORMATION INCIDENTS

Company will maintain a written response program designed to manage any Information Incident in compliance with the requirements set forth herein:

6.1 **Notice to Lenovo**. Company will notify Lenovo when Company has reason to believe that there has been or is reasonably likely to be an Information Incident. Company will notify Lenovo without unreasonable delay, but in no event longer than 24 hours after discovery of an Information Incident.

6.2 **Method of Notice**. Notification to Lenovo under this Section will be made by sending an email to secresponse@lenovo.com that (i) provides a description of the Information Incident, identifies Proprietary Information at issue, identifies the known or suspected unauthorized recipients of the information, and summarizes all efforts undertaken and planned to investigate and resolve the Incident and secure the information, systems and services at issue; and (ii) identifies a point of contact at Company who will be available to Lenovo as a contact regarding the Incident.

6.3 **Remediation**. In the event of an Information Incident, Company will promptly provide assistance to Lenovo in investigating the Incident, remedying the cause of such Incident, and taking any other actions reasonably necessary to halt the Information Incident (if it is ongoing).

6.4 **Review of Public Statements**. The content of any statements, communications, notices, filings or reports by Company or its Subcontractors related to any Incident, including those required by law, will be provided to Lenovo within a reasonable time prior to any publication or communication. Except for any notices and content thereof that Company or its Subcontractors are required by law to provide, all public statements, press releases or customer notifications by Company or its Subcontractors relating to the Incident will be approved by Lenovo prior to any publication or communication.

6.5 **Company Point of Contact**. Company will provide Lenovo with the name, address, phone number, and email of a point of contact that will be available 24 hours a day, seven days a week so Lenovo can report Incidents or obtain information about Incidents that Company has reported.

7. CORRECTIVE ACTION

If Lenovo determines that Company's Controls contain a material vulnerability, it will promptly notify the Company in writing. Company will promptly correct or mitigate any material vulnerabilities (either discovered by Company or Lenovo) in its Controls, systems, processes, policies, procedures involving its Access to Proprietary Information, within a reasonable period of time, but in no event longer than 60 days after Company's discovery unless no commercially reasonable solution is available within such period of time. Upon discovery or notification of a material vulnerability that is not corrected or mitigated within five business days of Company's discovery or receipt of notification of the same, Company agrees promptly to provide Lenovo with a corrective action plan documenting the risks identified, Company's response to the risks, and specific dates by which the risks will be eliminated, or reduced to a level acceptable to Lenovo, by Company.

8. SUBCONTRACTORS

If Lenovo has agreed in writing to permit Company's use of Subcontractors to provide services and/or products to Company on Lenovo's behalf, then Company agrees to: (i) provide its Subcontractors with Access to Proprietary Information only where there is a legitimate need to do so in connection with Company's obligations under a Agreement; (ii) ensure that members of Company's Subcontractors who have Access to Proprietary Information agree in writing to take appropriate steps to implement their own controls consistent with the requirements herein and the confidentiality provisions in the applicable Agreement; (iii) take reasonable steps to ensure that Company's Subcontractors have implemented appropriate controls consistent with the requirements herein and the confidentiality provisions of the applicable Agreement; (iv) assume responsibility for the sufficiency of the controls that its Subcontractors have implemented; and (v) and assume liability for any failure of controls implemented by its Subcontractors to meet the terms and conditions herein and the confidentiality provisions of the applicable Agreement.

9. TERMINATION AND RETENTION

9.1 **Termination**. Company will ensure that all Personnel or Subcontractors: (i) immediately cease Accessing Proprietary Information; (ii) return or destroy all Proprietary Information and materials related thereto at Lenovo's election, within 90 days or sooner if reasonably requested by Lenovo, except to the extent that Company's retention of such information is required by law; and (iii) upon written request of Lenovo, confirm to Lenovo in writing that it has done so.

9.2. **Retention**. Company may retain only the portions of Proprietary Information as required by law, rule, or regulation following expiration or termination of an Agreement. The Proprietary Information Accessed in this manner will be kept solely as an archival copy, and will be securely destroyed as soon as Company is not required by law to retain it. Covered Information destruction should follow an industry standard procedure for complete destruction such as NIST Special Publication 800-88. Prior to such destruction, Company will maintain all Controls to protect the retained Proprietary Information. Upon request, Company will provide verification of such destruction.

10. INDEMNIFICATION

In the event that an Information Incident found to have been caused by an action or inaction of Company, its Personnel or its agents leads to a loss, disclosure or misuse of Personal Data, Company will remain liable and will indemnify Lenovo for any direct costs related to investigation and remediation of said incident

11. NOTICE AND LEGAL PROCESS

Other than as necessary to perform its obligations under an Agreement, Company will not release Proprietary Information unless compelled to do so by a court or other government authority of competent jurisdiction, subject

to the conditions that Company: (i) takes reasonable steps to preserve the confidentiality of Proprietary Information, including without limitation (A) releasing or providing Access to only the minimum amount of information requested, and (B) taking reasonable steps to ensure that the release or Access does not result in further disclosure of the requested information to improper or unauthorized third parties or the public; (ii) provide, except as prohibited by law, Lenovo with prompt notice of the legal process and give Lenovo the opportunity to seek an appropriate protective order or to pursue such other legal action necessary to preserve the confidentiality of Proprietary Information; and (iii) cooperate with Lenovo in its efforts to preserve the confidentiality of Proprietary Information.

12. California Consumer Privacy Act ("CCPA") Provisions

A. Lenovo is a Business. Company is Lenovo's Service Provider and will process Personal Data on behalf of Lenovo.

B. Company shall not sell the Personal Data or Proprietary Information. "Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating the information for monetary or other valuable consideration.

C. Company shall not retain, use, or disclose the Personal Data: (a) for any purpose other than for the specific purpose of performing the services set forth in the Agreement for Lenovo or as otherwise permitted by the CCPA and its implementing regulations, (b) for a commercial purpose other than providing the services specified in the contract with the business, or (c) outside the direct business relationship between the person and Lenovo.

D. Company will cooperate with Lenovo in order to efficiently, effectively, and timely respond to requests from individuals related to the Personal Data. These requests include, but are not limited to, requests to review, correct, amend or delete Personal Information.

E. Company will not collect, process, use, retain or disclose any Personal Data of individuals 15 years of age or younger under the terms of this Agreement unless specifically authorized in writing by Lenovo.

F. This Exhibit shall serve as Company's certification that Company understands the CCPA requirements applicable to businesses and service providers, including the restrictions in Cal. Civ. Code § 1798.140(w)(2)(A), and will comply with them.