Exhibit 4

SECURITY MEASURES

This forms part of the Standard Contractual Clauses and must be completed and agreed by the parties.

The importer uses the cloud service that Cisco Systems G.K. (“Cisco”) provides. The technical and organisational security measures implemented by Cisco are as follows:

1. General Compliance

1.1. Compliance. Cisco shall document and implement processes to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes shall be designed to provide appropriate security to protect Data given the risk posed by the nature of the Data processed by Cisco. Cisco shall implement and operate information security in accordance with Cisco’s own policies, which shall be no less strict than the information security requirements set forth in this document.

1.2. Protection of logs and records. Cisco shall implement appropriate procedures designed to protect logs and records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

1.3. Review of information security. Cisco’s approach to managing information security and its implementation shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

1.4. Compliance with security policies and standards. Cisco’s management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

1.5. Technical compliance review. Cisco shall regularly review information systems for compliance with Cisco’s information security policies and standards.

1.6. Information Risk Management (“IRM”). Cisco shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Threat and vulnerability assessments must be reviewed periodically and prompt remediation actions taken where material weaknesses are found.

1.7. Processing of Sensitive Personal Data. To the extent that Cisco processes Sensitive Personal Data and the security measures referred to in this document are deemed to provide insufficient protection, Customer may request that Cisco implement additional security measures.

2. Technical and Organizational Measures for Security

2.1. Organization of Information Security

a. Security Ownership. Cisco shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

b. Security Roles and Responsibilities. Cisco shall define and allocate information security responsibilities in accordance with Cisco's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.

c. Project Management. Cisco shall address information security in project management to identify and appropriately address information security risks.

2.2. Human Resources Security

a. General. Cisco shall ensure that its personnel are subject to confidentiality obligations and shall provide adequate training about relevant privacy and security policies and procedures. Cisco shall further inform its personnel of possible consequences of breaching Cisco's security policies and procedures, which must include disciplinary action, including possible termination of employment for Cisco's employees and termination of contract or assignment for relevant external Representatives (e.g., contractors, agents, consultants etc.).

b. Training. Representatives with access to Data shall receive appropriate, periodic (i.e., at least annual) education and training regarding privacy and security procedures to aid in the prevention of unauthorized use (or inadvertent disclosure) of Data and training regarding how to effectively respond to security incidents. Training shall be provided before Representatives are granted access to Data or begin providing Services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

c. Background Checks. Cisco shall require criminal and other relevant background checks for Representatives in compliance with mandatory applicable law and Cisco's policies.

2.3. Access Controls

a. Access.

i. Limited Use. Cisco will not (i) access the Customer's computer systems for any purpose other than as necessary to perform its obligations under the Agreement or as otherwise agreed to by the parties; or (ii) use any system access information or log-in credentials to gain unauthorized access to Data or Customer's systems, or to exceed the scope of any authorized access.

ii. Authorization. Cisco shall restrict access to Data and systems at all times solely to those Representatives whose access is necessary.

iii. Suspension or Termination of Access Rights. At Customer's reasonable request, Cisco shall promptly and without undue delay suspend or terminate the access rights to Data and systems for any Representatives reasonably suspected of breaching any of the provisions of this document; and Cisco shall remove access rights of all Cisco employees and relevant external parties upon suspension or termination of their employment or engagement.

iv. Information Classification. Cisco shall classify, categorize, and/or tag Data to help identify it and to allow for access and use to be appropriately restricted.

b. Access Policy. Cisco shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Cisco shall maintain a record of security privileges of Representatives that have access to Data, networks, and network services. Cisco shall restrict the use of utility programs that might be capable of overriding system and application controls.

c. Access Authorization

i. Cisco shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to its systems and networks. Cisco shall use an enterprise access control system that requires revalidation of Representatives by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

ii. Cisco shall maintain and update a record of its users authorized to access systems that contain Data and Cisco shall review such users' access rights at regular intervals.

iii. For systems that process Data, Cisco shall revalidate (or where appropriate, deactivate) access of Representatives who change Cisco reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.

iv. Cisco shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

d. Network Design. For systems that process Data, Cisco shall have controls to avoid Representatives assuming access rights that could be used to gain unauthorized access to Data.

e. Least Privilege. Cisco shall limit Representatives' access to Data to those Representatives who have an actual need to access such Data to perform their assigned duties.

f. Authentication

i. Cisco shall use industry standard practices including ISO/IEC 27002:2013 and NIST SP 800-63B (Digital Identity Guidelines) to identify and authenticate users who attempt to access information systems.

ii. Where authentication mechanisms are based on passwords, Cisco shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability) with at least 8 characters and containing the following four classes: upper case, lower case, numeral, special character.

iii. Cisco shall maintain industry standard procedures to prevent de-activated or expired identifiers and log-in credentials from being granted to other individuals.

iv. Cisco shall monitor repeated failed attempts to gain access to its information systems.

v. Cisco shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

vi. Cisco shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

vii. Cisco shall implement a multi-factor authentication solution to authenticate Representatives accessing its information systems.

2.4. Physical and Environmental Security

a. Physical Access to Facilities

i. Cisco shall limit access to facilities where systems that process Data are located to authorized individuals.

ii. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

iii. Facilities shall be monitored and access-controlled at all times (24x7).

iv. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Data. Cisco must register authorized individuals and require them to carry appropriate identification badges.

b. Physical Access to Equipment. Cisco equipment used to process Data shall be protected using industry standard processes to limit access to authorized Representatives.

c. Protection from Disruptions. Cisco shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

d. Clear Desk. Cisco shall have policies requiring a “clean desk/clear screen” designed to prevent inadvertent disclosure of Data.

2.5. Operations Security

a. Operational Policy. Cisco shall maintain written policies describing its security measures and the relevant procedures and responsibilities of Representatives who have access to Data and to its systems and networks. Cisco shall communicate its policies and requirements to all Representatives involved in the processing of Data. Cisco shall implement the appropriate management structure and control designed to maintain compliance with such policies and with mandatory applicable law concerning the protection and processing of Data.

b. Security and Processing Controls.

i. **Areas.** Cisco shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks that process Data.

ii. **Standards and Procedures.** Such standards and procedures shall include security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

c. Logging and Monitoring. Cisco shall maintain logs of administrator and operator activity and data recovery events related to Data.

2.6. Communications Security and Data Transfer

a. Networks. Cisco shall, at a minimum, use the following controls to secure its corporate networks that process Data:

i. Network traffic shall pass through firewalls, which are monitored at all times. Cisco mustimplement intrusion detection systems and/or intrusion prevention systems.

ii. Anti-spoofing filters and controls must be enabled on routers.

iii. Network, application, and server authentication passwords are required to meet the same industry standard practices used for the authentication of users set forth in Section 2.3.f above (Authentication). System-level passwords (privileged administration accounts or userlevel accounts with privileged administration access) must be changed at minimum every 90 days.

iv. Initial user passwords are required to be changed at first log-on. Cisco shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

v. Firewalls must be deployed to protect the perimeter of Cisco’s networks.

b. Virtual Private Networks (“VPN”). When using VPN to remotely connect to the Customer’s or Cisco’s network for processing of Data:

i. Connections must be encrypted using industry standard cryptography.

ii. Connections shall only be established using VPN servers.

iii. The use of multi-factor authentication is required.

c. Data Transfer. Cisco shall have formal transfer policies in place to protect the transfer of Data through the use of all types of communication facilities that adhere to the requirements of this document. Such policies shall be designed to protect transferred Data from unauthorized interception, copying, modification, corruption, routing and destruction.

2.7. System Acquisition, Development, and Maintenance

a. Security Requirements. Cisco shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

b. Development Requirements. Cisco shall have policies for secure development, system engineering, and support. Cisco shall conduct appropriate tests for system security as part of acceptance testing processes. Cisco shall supervise and monitor the activity of outsourced system development.

2.8. Penetration Testing and Vulnerability Scanning & Audit Reports

a. Testing. Cisco will perform periodic vulnerability scans and penetration tests on its internetperimeter network. These scans and tests will be conducted by qualified professionals, including among other entities, Cisco's independent internal compliance team, using industry standard tools and methodologies.

b. Audits and Certifications. Cisco shall cooperate with reasonable requests by Customer for legally required security audits (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for testing reports. Cisco shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains (such as SSAE 16 – SOC1, SOC2, SOC3 attestations or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the Service, to the extent that Cisco maintains such certifications in its normal course of business. Customer shall treat the contents of reports related to Cisco's security and certifications as confidential information.

c. Remedial Action. If any penetration test or vulnerability scan referred to in Section 2.8.a above reveals any deficiencies, weaknesses, or areas of non-compliance, Cisco shall promptly take such steps as may be required, in Cisco's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable considering Cisco's prioritization of such, based upon their criticality (e.g. nature, severity, likelihood).

d. Status of Remedial Action. Upon request, Cisco shall keep Customer reasonably informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same.

2.9. Contractor Relationships

a. Policies. Cisco shall have information security policies or procedures for its use of external Representatives that impose requirements consistent with this document.

b. Monitoring. Cisco shall monitor and audit service delivery by its external Representatives and review its external Representatives' security practices against the security requirements set forth in Cisco's agreements with such Representatives.

2.10. Management of Data Breaches and Improvements

a. Responsibilities and Procedures. Cisco shall establish procedures to ensure a quick, effective, and orderly response to Data Breaches.

b. Reporting Data Breaches. Cisco shall implement procedures for Data Breaches to be reported as appropriate. Representatives should be made aware of their responsibility to report Data Breaches as quickly as reasonably possible.

c. Reporting Information Security Weaknesses. Cisco's Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

d. Assessment of Information Security Events. Cisco shall have classification scale in place in order to decide whether an information security event should be classified as a Data Breach.

e. Response Process. Cisco shall maintain a record of Data Breaches with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

2.11. Information Security Aspects of Business Continuity Management

a. Planning. Cisco shall maintain emergency and contingency plans for the facilities where Cisco information systems that process Data are located. Cisco shall verify the established and implemented information security continuity controls at regular intervals.

b. Data Recovery. Where and as applicable, Cisco shall design redundant storage and procedures for recovering Data in its possession or control in a manner sufficient to reconstruct Data in its original state as found on the last recorded backup provided by the Customer or in a manner sufficient to resume the Service.

3. Definitions

3.1. "Affiliates" means companies within the Cisco group that may process Data in order to provide the Products and/or Services. Such Affiliates include Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia Pty Limited, Cisco Systems Canada Co., Cisco International Limited, Cisco Systems (Italy) S.R.L., Cisco Systems International B.V., ThousandEyes LLC, Broadsoft, Inc., AppDynamics LLC, AppDynamics International Ltd. And Meraki LLC. Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger are not considered Affiliates for the purposes of this document.

3.2. "Agreement" means the written or electronic agreement between Customer and Cisco or the relevant Cisco Affiliate for the provision of the Services and/or Products to Customer.

3.3. "Customer Content" means data such as text, audio, video or image files, provided by you to Cisco in connection with your use of Cisco solutions, and data developed at your specific request related to a statement of work or contract.

3.4. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data relating to you.

3.5. "Personal Data" means any information about, or relating to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.

3.6. "Product" means Cisco or its Affiliates' branded hardware and software that is purchased under the Agreement.

3.7. "Representatives" means Cisco's or its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

3.8. "Service" means Cisco or its Affiliates' branded service offering that is purchased by Customer under the Agreement.

3.9. "Sensitive Personal Data" refers to sensitive personal information (as defined under the California Consumer Protection Act), special categories of personal data (as described in Article 9 of the General Data Protection Regulation), and other similar categories of Personal Data that are afforded a higher level of protection under applicable law.

3.10. "Systems Information" means data generated or collected in connection with your use and operation of Cisco solutions, and data provided by you in connection with our delivery of products and services to you (including, for example, when you submit a request related to support services).