SCHEDULE B -
TECHNICAL AND ORGANISATIONAL SECURITY MEASURES
Also serves as Annex II to the EU SCC

Processor shall implement appropriate technical and organizational security measures intended to protect the Customer Personal Data it Processes against accidental or unauthorized loss, destruction, alteration, disclosure or access:

IS Program - Radware maintains an information security program with the aim to identify reasonably foreseeable external and internal risks to the security of Radware Network and minimize security risks through risk assessments and regular testing.

CISO - Radware has designated a Chief Information Security Officer (CISO) to coordinate and be accountable for the information security management system.

Baseline for the Security and Privacy Management System - Radware follows industry best practices for its Information Security Management system (ISMS) and Privacy Management System(PIMS). Radware's compliance with these standards is certified annually for ISO 27001, ISO 27017, ISO 27018, ISO 27032 and ISO 27701.

PCI Service Provider (where appropriate) and HIPAA compliance is confirmed by an annual self-assessment process.

Security Reviews - Radware conducts periodic reviews of the security of its infrastructure and the adequacy of its information security program. Evidence of these reviews include annual SOC2 Type II reports prepared by a qualified 3rd party.

Human Resources - Radware provides that employees, contractors, partners, and vendors understand their data protection and security responsibilities. These responsibilities include maintaining the confidentiality, integrity and availability of the Customer information processed by Radware. All employees of the organization and where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Access Control

Radware provides that only authorized users will have access to its information assets and to private data. Users are only be provided with access to assets that they have been specifically authorized to use.

Radware provides the customers with an access control management system for the relevant cloud management portals as part of the service.

Encryption - Radware provides proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, Radware will provide that confidential data will be encrypted whenever extracted from their primary repository.

Physical and Environmental Security - Radware will use physical and environmental measures to prevent unauthorized physical access, damage to or disruption of the organization's information and information processing facilities.

Operational & Communication Security - Radware will maintain appropriate controls related to management of IT production including change management, capacity management, malware, backup, logging, monitoring and vulnerabilities management.

System acquisition, development, and maintenance - Radware maintains security throughout the lifecycle of the information systems.

Supplier Relationship - Radware provides that its partners, suppliers, and contractors maintain adequate security measurements to secure Radware and its customers' information, through contracts and periodic audits.

Data Retention and disposal

Information stored withing the service, such as logs and alerts will be retained according to customer requirements. When no longer required, the information will be securely deleted or destroyed.