TECHNICAL AND ORGANIZATIONAL MEASURES

Unless otherwise defined below, each term defined herein shall have the meaning assigned thereto in the SDPA.

Supplier's technical and organizational measures should include, without limitation, the following:

(i) **Organization of Information Security** – Establishment, implementation, and maintenance of information security policies and a program of Technical and Organization Security Measures appropriate to protect Customer Information, meeting Good Industry Practice.

(ii) **Secure Baseline Standards** – Measures to ensure that secure configurations are developed, documented, and maintained for information systems.

(iii) **Access Controls** – System access, user access and authentication measures to prevent access to Customer Information in any manner or for any purpose not authorized by Customer; measures should include, without limitation, prevention of unauthorized input, reading, copying, removal, modification or disclosure of Customer Information.

(iv) **System Security** – Measures to harden information systems and other resources in accordance with Good Industry Practice.

(v) **Auditing and Monitoring –** Measures to maintain an automated audit trail that documents system security events and any change management event that results in the access, modification, and/or deletion of Customer Information.

(vi) **Network Security** – Measures to maintain a formal process for approving, testing, and documenting all network connections, and changes to network device configurations.

(vii) **Data Protection** – Measures to prevent the unauthorized access, alteration or removal of Customer Information being stored or in transmission.

(viii) **Security Awareness and Training** – Measures to regularly provide employees annual security awareness training that is reflective and appropriate for security trends, threats, and best practices.

(ix) **Security Testing –** Measures to regularly identify and remediate vulnerabilities per Supplier policy and perform periodic security testing on systems and applications or upon significant changes. These measures should include, without limitation, (1) engaging an independent third party to perform a security audit annually on all Supplier Systems, (2) conducting regular penetration testing and weekly vulnerability scanning on all Supplier Systems, (3) establishing and maintaining a patch management program which meets or exceeds Good Industry Practice, pursuant to which Supplier will regularly update and patch software which may directly or indirectly affect Customer Information and/or Supplier Systems and (4) designating a security liaison for Customer who will be available to discuss Information Security Incidents, security tests, security findings, and other security concerns at regular intervals. If any material deficiency is identified as a result of any of the above or Customer's security assessment, Supplier will remediate the material deficiency within

30 days (any critical finding not remediated within 30 days must be immediately escalated to Customer and at Customer's request, and Supplier will provide written attestation that the foregoing security tests have been conducted and a detailed list of open vulnerabilities and remediation plans).

(x) **Availability Controls –** Measures to develop, operate, manage, and revise business continuity and disaster recovery plans, including technology recovery.

(xi) **Remediation of Software Security Issues –** If, as part of the Services, Supplier provides SaaS or PaaS or any hosted software service, and if vulnerabilities or other security issues in the software are discovered or suspected by Supplier or Customer, measures to provide error corrections, updates, patches, revisions, fixes, upgrades and new releases of software (with documentation of each) included in the application to Customer in accordance with the timeline below. Supplier will provide evidence to Customer demonstrating that all identified security issues have been fully remediated in accordance with the established corrective action plan.

Severity	Description	Acknowledgement	Updates	Resolution	Closure
Emergency	Catastrophic issues without a viable work around	1 business hour of discovery of vulnerability or security issue	Every 3 business hours	1 day	7 days
Critical	Issues that pose a serious threat to the end user and/or Customer	4 business hours of discovery of vulnerability or security issue	Daily	5 days	14 days
Important	Issues with a viable workaround and can be mitigated with other security controls in place	2 business days of discovery of vulnerability or security issue	5 days	10 days	45 days
Non-critical	All other issues or work around	5 business days of discovery of vulnerability or security issue	5 days	15 days	Next release