TECHNICAL AND ORGINIZATIONAL MEASURES

(FOR SUPPLIERS)

These Technical and Organizational Measures (the "**TOMs**") are an integral part of respective Personal Data Processing Agreement / Addendum / Attachment / Schedule / Section (or any other equivalent document, as applicable) between Avaya (including its Global Affiliates) and Supplier (including its Global Affiliates, if any), which incorporates them by reference.

1. Access control to premises

Supplier shall take reasonable steps to prevent physical access to Personal Data processing equipment by unauthorized persons as follows:

1.1. Implement electronic access control to enter buildings hosting Personal Data.

1.2. Implement electronic access control for sensitive areas within the building such as data centers, phone rooms, LAN closets and labs.

1.3. Ensure that policies are in place to ensure only authorized individuals gain access to sensitive areas such as data centers, LAN rooms, phone closets and any other location where Personal Data is processed or stored. Ensure all access rights to such areas are revalidated semi-annually.

1.4. Create and retain access logs for a minimum of 90 days.

1.5. Ensure that perimeter doors and sensitive areas are monitored and recorded via CCTV 24/7.Ensure all CCTV recordings are retained for at least 30 days.

1.6. Maintain an actively monitored alarm system that physically secures sensitive areas (includes, LAN rooms, labs, and any other area where processing of Personal Data will take place).

1.7. Ensure that there are security guards present at any corporate site that processes Personal Data.

1.8. Ensure that a process is in place to validate the identity of an individual before assigning an ID badge.

1.9. Visitors must sign in and wear a badge which easily identifies them as visitor. Visitors shall be escorted by staff during their presence at the site. All visitor logs must be retained for a minimum of one year.

1.10. Limit and control access to data center and media storage facilities containing Personal Data for outside contractors such as security guards, janitorial services.

1.11. Maintain a documented key control program for the facility with a master key log. Keys to cabinets, equipment rooms, and wiring closets must be held under proper custody, only given out to authorized persons, and tracked to return.

1.12. Ensure that access control records are reviewed by the administrator for alarm activity, including door held or door forced alarms.

2. Access control to use of system

In order to prevent logical access to its equipment or applications processing Personal Data by unauthorized persons, the Supplier shall take reasonable steps to implement and maintain the following measures:

2.1. Ensure that a unique identifier must be associated with each user of a system (network, server, database, application).

2.2. Ensure that the issuance of access accounts and privileges requires management approval and are reviewed every 6 months.

2.3. Maintain an access control list (ACL) for all systems containing Personal Data and review regularly.

2.4. Practice least privilege rule and the right to know principle when granting user access.

2.5. Practice separation of duties.

2.6. Ensure that processes are in place to suspend the access authorizations within 24 hours of users whose employment at Supplier ends (termination, transfer, etc.).

2.7. Disable user accounts after 90 days of inactivity and delete after 120 days of inactivity.

2.8. Ensure that each user's identity is verified when the user attempts to logon through the use of passwords, multi factor authentication or biometric data. Successful and unsuccessful logon attempts shall be logged and kept for 1 year.

2.9. Set automated password protected screen-lock after more than 20 minutes of inactivity.

2.10. User passwords must have the minimum length of 8 characters, containing at least one character from 3 out of 4 categories (upper case letter, lower case letter, number and special character).

2.11. Administrator, system level and service account passwords must have a minimum length of 15 characters, containing at least one character from 4 out of 4 categories (upper case letter, lower case letter, number and special character).

2.12. Passwords must expire every 90 days.

2.13. New passwords shall differ from the last 10 passwords.

2.14. An account shall auto-lock after 5 unsuccessful login attempts.

2.15. All installation and vendor-default passwords provided with new hardware, system software and applications must be reset upon installation.

2.16. Passwords must be stored and transmitted in encrypted format.

2.17. Initial temporary password and ID must be communicated securely. Clear-text passwords and ID's must never be sent in the same email.

2.18. Ensure user identity is validated before allowing password reset or providing password to users.

2.19. Standardize servers and operating system builds and configuration in accordance with industry standards so as to be resistant to attacks.

2.20. Ensure that systems storing or processing Personal Data are on a separated network segment(s) based on the label or classification level of the information stored on the servers to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

2.21. Maintain a documented patch management process and perform updates on systems with Critical and High Risk vulnerabilities within 2 weeks from the patch release and all others within one month. Additionally, shall remediate any patch immediately as requested by Avaya.

2.22. Antivirus software must be loaded and operational on all servers and PCs Processing Personal Data. Suppliers shall use other malware detection techniques where possible (e.g., email scanning, file system scanning, Internet traffic scanning, etc.).

2.23. Antivirus scanning software shall be updated on, at minimum, a daily basis and shall be able to support urgent, out-of-cycle signature updates.

2.24. Antivirus software must be configured such that non-privileged users are not able to disable the software. Subject to appropriate change controls, privileged users may disable the software, where appropriate.

3. Access control to Personal Data

The Supplier shall take reasonable steps to prevent logical access to Personal Data by unauthorized persons by implementing and maintaining suitable measures to prevent unauthorized reading, copying, alteration or removal of the media containing Personal Data, unauthorized input into memory, reading, alteration or deletion of the stored Personal Data. This will be accomplished by the following measures:

3.1. Maintain a written data classification and handling policy and an inventory of records with classification with physical and electronic location provided.

3.2. Supplier shall ensure that Personal Data is encrypted in transit using non deprecated industry standard protocols (e.g. SSH/SCP/SFTPV2, TLSv1.2 or greater).

3.3. Supplier shall ensure an industry standard level of encryption of Personal Data appropriate to the risks that are presented by the processing of Personal Data at rest. Notwithstanding, all backups of Personal Data shall be encrypted on backup media.

3.4. Personal Data may only be downloaded to a Supplier's PC, laptop, mobile device, or removable storage if hard disk encryption is enabled on that device.

3.5. Ensure periodic encryption key rotation and management.

3.6. Personal Data may never be used in development, testing, and / or staging environments unless the Personal Data are pseudonymised and such use is authorized in writing by Avaya.

3.7. If credit cardholder information is handled, stored, or otherwise processed, the Supplier's systems must be PCI DSS certified.

4. Transmission control

The Supplier shall take reasonable steps to prevent any unauthorized access, modification to Personal Data during transmission via implementation of secure communication channels and shall implement logging of transmissions as follows:

4.1. Ensure perimeter networks are physically or logically separated from internal networks containing Personal Data.

4.2. Setup firewalls between: Internet and web facing systems; web facing systems and application systems; application systems and internal networks. These firewalls shall be physically unique devices.

4.3. Utilize Network Intrusion Detection Systems (IDS) as part of network security strategy in addition to firewalls. All NIDS logs shall be monitored on a regular basis to detect likely unauthorized access attempts to Personal Data.

4.4. Firewalls shall be used with stateful inspection and firewall rules shall be reviewed annually.

4.5. Restrict and control wireless network access using industry standard wireless security protocols, but nothing less secure than WPA2.

4.6. Restrict and control remote network access and require the use of VPN with two-factor authentication.

5. Input control

The Supplier shall take reasonable steps to ensure the ability to check and establish whether, and by whom, Personal Data was inputted, modified or removed from the data processing equipment as follows:

5.1. Every change to configuration of servers, networks, databases, or business applications containing Personal Data, or changes to the Personal Data itself, shall be logged. Audit logs shall ensure actions can be traced to an individual and shall include, at minimum, the time, date, and type of action. Audit logs shall be kept for 1 year.

5.2. Audit, change, event and access control logs shall be actively monitored, reviewed and centrally aggregated for all systems that process or control Personal Data at rest and in transit using an industry proven collection mechanism e.g. SIEM. Unauthorized access and anomaly alerts shall be created. Log audit and anomaly reports shall be provided on request.

5.3. Maintain configuration management including secure baseline configurations.

5.4. Monitor to detect and generate alerts for unauthorized changes.

5.5. Ensure that emergency changes require appropriate level management approval before implementation.

5.6. Ensure that consequences for policy violations are established, communicated, and acted upon.

6. Organization control

The Supplier shall take reasonable steps to arrange the internal organization in such a way that it meets the specific requirements of data protection and implement and maintain the following measures:

6.1. Maintain a written information security policy that is approved annually by Supplier management team and published and communicated to all Supplier employees and relevant third parties.

6.2. Maintain a dedicated security and compliance function to design, maintain and operate security in support of its "trust platform" in line with industry standards. This function shall focus on system integrity, risk acceptance, risk analysis and assessment, risk evaluation, risk management and treatment statements of applicability and vendor management.

6.3. Undergo regular independent 3rd party security reviews and provide audit reports such as SSAE16 or ISAE3402.

6.4. Use industry-recognized independent third party services to conduct vulnerability assessments and penetration tests of networks, systems, applications and databases where Personal Data is located at rest, in transit and in use. The Supplier shall triage identified vulnerabilities and remediate Critical vulnerabilities within 4 weeks of patch release and High vulnerabilities in accordance with generally accepted industry standards.

6.5. Maintain data protection, security awareness and compliance program, procedures and tools which address information security threats and best practices; as well as information security policies, procedures, and controls in place to protect Personal Data.

6.6. Maintain, and provide Avaya access to, upon request, reporting policies, procedures, and tools which provide relevant documentation and reporting on the implementation, effectiveness, and, if necessary, remediation, of the appropriate safeguards related to the processing of Personal Data.

7. Availability control

The Supplier shall take reasonable steps to prevent any accidental destruction or the loss of Personal Data by appropriate measures as follows:

7.1. Monitor security events and set up notification and alert process(es) on all the servers, networks, databases containing Personal Data.

7.2. Manage a security incident response process.

7.3. Maintain contingency planning policies, procedures, and tools which define roles and responsibilities and provide clear guidance and training on the proper handling of contingency events including: natural threat events such as floods, tornadoes, earthquakes, hurricanes, and ice storms; accidental threat events such as chemical spills, and mechanical or electrical failures; and intentional acts such as privacy and security breaches, bomb threats, assaults, and theft.

7.4. Have a business continuity/disaster recovery plan in place for the restoration of critical processes and operations of the Supplier's services at the location(s) from which the Supplier's services is provided. Supplier shall also have an annually tested plan in place to assist in reacting to a disaster in a planned and tested manner.

7.5. Implement and maintain, following industry standards, redundant power supply, fire and smoke alarms, fire suppression systems, generators, cooling systems and raised flooring at data centers processing Personal Data.

7.6. Perform full backups of the database(s) containing Personal Data in a secure manner to ensure availability in line with the criticality of the data.

8. Asset control

In order to ensure the protection of equipment or applications processing Personal Data, the Supplier shall take reasonable steps to implement and maintain the following measures:

8.1. Ensure that procedures and tools are in place to identify and track all equipment and media used in the processing Personal Data.

8.2. Assign responsibility for all equipment and media to one or more custodians.

8.3. Perform annual full review of the asset inventory and signoff of the asset inventory for accuracy and to identify missing equipment and media.

9. Application control

In order to ensure the protection of applications processing Personal Data, the Supplier shall take reasonable steps to implement and maintain the following measures:

9.1. If applicable, prior to application release, conduct penetration tests, web application vulnerability tests and high severity vulnerabilities mitigation.

9.2. Conduct penetration tests at least once per year on its computing environment and provide Avaya with written copies of the results of such penetration tests performed by Supplier or its sub–processors no more than 30 days after Supplier obtains the results or reports.

9.3. Where applications that will process Personal Data are being developed for the provision of Supplier's services to Avaya, ensure that developers are trained on industry-standard secure developing best practices.

9.4. Ensure that applications that will process Personal Data are developed in a secure manner using Supplier's formal, documented, process that provides evidence that application security vulnerabilities are not present prior to moving into production. Retests will be conducted at least quarterly thereafter, and after each significant change. At a minimum, application security vulnerabilities would include the SANS Top 20 and OWASP Top 10.

9.5. Application security vulnerabilities that affect Personal Data shall be corrected within a reasonable time after identification.

9.6. These requirements should be validated by tools such as dynamic application scanning and/or static code analysis.

10. **Change and separation of data control**

The Supplier shall take reasonable steps to implement and maintain the following change control measures for processing of Personal Data:

10.1. Maintain change management processes that include documentation of the purpose, security impact analysis, testing plan and results, and appropriate management authorization for all changes on systems processing Personal Data.

10.2. The configuration of systems processing Personal Data must be validated prior to release in the production network.

10.3. Changes to production environments containing Personal Data shall be reviewed and approved by Supplier's management with documentation of review / approvals availability in the event of an audit.

10.4. Maintain physically and / or logically separate development/ testing/ staging environments from production environments where Personal Data is processed.

10.5. The Supplier shall keep physically or logically separated databases for processing Personal Data for Avaya.

- END OF THE TOMs -