TECHNICAL AND ORGINIZATIONAL MEASURES

(FOR CUSTOMERS)

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

1. Access control to premises

Avaya will prevent physical access to Personal Data processing equipment by unauthorized persons as follows:

1.1. Avaya will implement and maintain physical security measures in order to prevent unauthorized access. This is accomplished by the following measures:

1.1.1. an electronic access control system with a 90-day log retention;

1.1.2. a 24/7 video recording of physical facility with 30-day log retention; and

1.1.3. intrusion detection / burglar alarms, or engaging on premise security officers.

1.2. Avaya will restrict the access to various zones at its premises based on roles, and periodically revalidate the access by owners.

1.3. Avaya will have personnel and visitor security measures in place to prevent unauthorized access, which is accomplished by the following measures:

1.3.1. Personnel must display IDs;

1.3.2. Visitors must sign in;

1.3.3. Visitors will be reasonably escorted by staff; and

1.3.4. Visitors must wear a badge which easily identifies them as visitor.

2. Access control to use of system

In order to prevent logical access to its Personal Data processing equipment by unauthorized persons, Avaya will implement and maintain the following measures:

2.1. Avaya will only grant individuals access to the Personal Data processing equipment with

2.1.1. a unique user ID for access with formal authorization process, and

2.1.2. a unique password with the following features:

2.1.2.1. a complex password, consisting of eight characters and three of four character sets;

2.1.2.2. a maximum password lifetime of ninety days; and

2.1.2.3. an account lockout on failed logins.

2.2. Avaya will grant the individuals access based on their job function with the following criteria:

2.2.1. role-based access;

2.2.2. least-privileged access; and

2.2.3. access only on a need-to-know basis.

2.3. The screen of endpoints will be automatically locked after 20 minutes idle time.

2.4. Avaya will log access to the data processing equipment.

2.5. Avaya will use a multi-factor authentication of Avaya's virtual private network (VPN) for remote access.

2.6. Avaya will implement and maintain a central user administration.

2.7. Avaya will encrypt endpoints provided by itself.

3. Access control to Personal Data

Avaya will 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. Avaya will only grant individuals access to the Personal Data with:

3.1.1. a unique user ID for access with formal authorization process, and

3.1.2. a unique password with the following features:

3.1.2.1. a complex password, consisting of eight characters and three of four character sets;

3.1.2.2. a maximum password lifetime of ninety days; and

3.1.2.3. an account lockout on failed logins.

3.2. Avaya will grant individuals access to the Personal Data based on their job function with the following criteria:

3.2.1. role-based access;

3.2.2. least-privileged access; and

3.2.3. access only on a need-to-know basis.

3.3. The screen of endpoints will be automatically locked after 20 minutes idle time.

3.4. Avaya will log access to the data processing equipment.

3.5. Avaya will maintain access control lists (ACL).

3.6. Avaya will conduct data backups and retrievals, using a secure storage of backup media and testing backups.

3.7. Avaya will implement and maintain a formal access control change management program.

3.8. Avaya will implement and maintain internal policies and standards comprising security policies and standards, both at a corporate and business unit level.

3.9. Avaya will conduct periodic mandatory trainings with respect to protection of personal data, and will monitor and enforce the training participation.

3.10. Avaya will implement and maintain anti-virus programs, which are centrally monitored and updated, and conduct regular anti-virus scans.

3.11. Avaya will conduct a secure deletion and /or disposal of data.

4. Transmission control

Avaya will prevent any unauthorized access to Personal Data via implementation of secure communication channels and logging as follows:

4.1. Avaya will use a VPN with a multi-factor authentication for remote access.

4.2. Avaya will use firewalls with the following features and processes:

4.2.1. stateful inspection;

4.2.2. default denial access rules are implemented unless access rules are explicitly approved;

4.2.3. role-based and least-privileged access on a “need to know” basis;

4.2.4. logging and alerting of access; and

4.2.5. annual review of firewall rules.

4.3. Avaya will use encrypted email if the same has been enabled by Customer, using transport layer security (TLS) as the methodology.

4.4. Avaya will implement and maintain security policies and standards both at a corporate and business unit level.

5. Input Control

Avaya will ensure the possibility to check and establish whether and by whom Personal Data have been put into, modified or removed from the Personal Data processing equipment as follows:

5.1. Individuals accessing personal data will require a unique user ID and authorization for access.

5.2. Avaya will implement and maintain security policies and standards both at a corporate and business unit level.

5.3. The Personal Data processing equipment will have logging functionalities.

5.4. Avaya will only grant individuals access to Personal Data based on their job function, with the following categories:

5.4.1. role-based access;

5.4.2. least-privileged access; and

5.4.3. access on a "need-to-know" basis.

6. Organization control

6.1. Avaya will ensure that in case of commissioned data processing, the Personal Data are processed strictly in accordance with the instructions of Customer.

6.2. Customer will provide clear instructions to Avaya regarding the scope of the processing of personal data, and Avaya will adhere to these instructions.

7. Availability control

Avaya will prevent any accidental destruction or the loss of Personal Data by appropriate measures as follows:

7.1. Avaya will implement and maintain uninterruptable power supply, fire and smoke alarms, fire suppression systems, generators, cooling systems and raised flooring.

7.2. Avaya will implement and maintain a disaster recovery plan, and annually review and test it.

7.3. Avaya will implement and maintain a backup strategy and backup procedures.

7.4. Avaya will implement and maintain anti-virus programs and firewall systems.

8. Control of separation of data

Avaya will implement and maintain appropriate measures to allow the separate processing of data which have been collected for different purposes as follows:

8.1. Avaya will separate different customers' Personal Data by storing Personal Data in logically separated databases.

8.2. Avaya will separate between productive and test data.

- END OF THE TOMs -