Information Security Addendum

This Information Security Addendum ("ISA") supplements any Agreement between Avaya and Company for provision of Services (as defined below) and sets out Avaya's approach to managing Information Security (as defined below) associated with the provision of the Services.

This ISA does not apply to Avaya Cloud Office by RingCentral (ACO). Please visit the RingCentral web page at https://assets.ringcentral.com/legal/privacy/customer-security-addendum/rc-trust-center-security-addendum.pdf (or a successor website) to access the Security Addendum for ACO.

This ISA does not apply to processing of personal data on behalf of the Company. Please visit https://www.avaya.com/en/trust-center/privacy/data-processing-addendum/ (or a successor website) for further information.

1 Definitions

Agreement means terms and conditions agreed between the Company and Avaya governing the purchase and the provision of the Services.

Cloud Services means on demand computing services which are delivered across networks, typically using the internet, such as Software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS)) and other variants.

Company means the entity purchasing the Services from Avaya for itself or an end-customer under the Agreement of which this ISA is a part.

Company Content means the content of all data, information and communications, whether visual, written, audible, or of another nature, sent, displayed, uploaded, posted, published, or submitted by Company or Company personnel, including Other Users Content, while utilizing the Services.

Cryptographic Protocols refers to mechanisms to safeguard the confidentiality and integrity of information as well as support authentication and non-repudiation objectives; for example, symmetric (secret) and public key encryption, hashing, digital certificates, digital signatures, key exchange.

Denial of Service Attack (DoS/DDoS) means an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet.

Good Industry Practices means the standards, practices, methods and the degree of skill and diligence which would reasonably be expected from a skilled and experienced company engaged in the same type of undertaking under the same or similar circumstances.

Hardware means equipment, plant, machinery, hardware, computer and communications devices and network equipment (including computer and communications hardware and servers), any associated peripherals, connecting equipment and cabling.

Information Security means the confidentiality, integrity and availability of information, including the establishment and maintenance of security controls to protect privacy, deal with adverse contingencies and promote resilience.

Least Privilege means granting the minimum possible access privileges to Software and users or making only necessary services and features available.

Logical Access Controls means controls that enable a business decision to allow or deny access to IT systems, resources and information which shall be:

(a) based on a set of guiding principles (e.g. need to know, Least Privilege etc.);

(b) used to define the level of access to an IT system or resource (e.g. read, write, delete etc.);

(c) applied explicitly to specific entities (e.g. individual or group users, systems or processes etc.); and

(d) implemented internally or externally using a range of protection mechanisms (e.g. applications, Technical Infrastructure etc.)

Malware means malicious Software programs such as viruses, worms, trojans, spyware etc.

Network Devices means devices such as hubs, switches and routers used to aggregate IT components, switch or route traffic.

On-Prem Services means maintenance or managed services for systems that are located on the customer's premises or within the customer's IT environment.

Other Users Content means the content of any information and communications, whether visual, written, audible, or of another nature, sent, displayed, uploaded, posted, published, or submitted by other users while interacting with the Services, including, without limitation, likenesses or photo images, advertisements or sponsored content.

.

Privacy by Design refers to a principle and approach that ensures privacy and data protection compliance is not an add-on, but an integral part of the system, product, or service design from the beginning. Privacy by Design involves considering privacy at every stage of the development process and embedding privacy controls and measures into the technology, business practices, and physical design. It encompasses seven foundational principles: proactive not reactive; privacy as the default setting; privacy embedded into design; full functionality; end-to-end security; visibility and transparency; and respect for user privacy.

Privileged Access means an account that has elevated privileges (aka 'god' or 'superuser' account) that provide the user greater abilities than a standard user account.

Processing means any operation or set of operations which is performed on any data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Security Architecture means a set of representations that describe the function, structure and interrelationship of the security components within an environment.

Security by Design refers to a proactive approach and practice of embedding security measures and considerations into the design and architecture of Software, Hardware, systems, and business processes from the outset, rather than as an afterthought. This approach ensures that security is an integral component of the product lifecycle, including planning, design, development, deployment, and maintenance phases. Security by Design aims to minimize Vulnerabilities, prevent security breaches, and protect against unauthorized access or misuse of information and systems.

Security Event means the occurrence of any incident which has resulted, or is reasonably likely to result, in:

(a) a breach by Avaya of any of the protections relating to Company Content set out in this ISA;

(b) any loss, theft, corruption, or unauthorised deletion or disclosure of Company Content; or

(c) any unauthorised use of or access to Company Content.

Sensitive Data means confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it.

Services means On-prem Services or Cloud Services provided by Avaya.

Software means any application, program, operating system software, database, firmware, computer software language, utilities, and other computer programs in machine-executable object code and/or source code form, and related documentation, in whatever media or form of storage, including the tangible media upon which they are recorded or printed, together with any corrections, updates, versions, upgrades and releases.

Technical Infrastructure means infrastructure components such as computer systems, network and telecommunication installations that support business applications.

Threat means any circumstance or event with the reasonable potential to adversely impact the Company's value, brand or operations by targeting its Company Content via unauthorised access, disclosure, modification, destruction of information and/or Denial of Service Attacks.

Vulnerabilit(y)(ies) means a flaw (or flaws) or a weakness (or weaknesses) in an information system, security procedures, internal controls or their implementation that could be accidentally triggered or intentionally exploited and result in a Threat being realised.

2 Security Policy

Avaya establishes and maintains a formal documented framework of policies, processes and controls for Information Security, business continuity in accordance with industry standards (such as ISF SOGP, ISO 27000, BCI's GPG, ISO22301), legislation and regulatory requirements applicable to Avaya, or Good Industry Practice.

3 Organization of Information Security

3.1 Avaya identifies an organization responsible for Information Security direction, policy management, reporting and escalation.

3.2 Avaya establishes a proactive risk management framework for Information Security, which includes processes for identifying mitigating actions that are tracked, monitored and reported for risks identified by Avaya.

3.3 Where any breach of the obligations set out in this ISA is uncovered, Avaya will take remedial steps to ensure compliance with this ISA.

3.4 Avaya identifies and manages Information Security risks throughout the provision of the Services.

4 Asset Management

Avaya maintains an information classification scheme based on the sensitivity of information.

5 Human Resource Security

5.1 Avaya employs qualified and experienced Information Security employees to effectively discharge the obligations of Avaya pursuant to this ISA.

5.2 Avaya undertakes security awareness programmes, training and development including but not limited to Information Security, so that all personnel involved in delivering Services to Company have the necessary awareness and competence to fulfil their security roles and contribute to an effective security culture.

5.3 Avaya ensures that its employees are vetted in accordance with Avaya policies and regularly trained and understand their obligation to comply with the requirements of this ISA.

5.4 Avaya ensures that its employees comply with Avaya security policies.

6 Physical & Environmental Security

Avaya ensures that

(a) all critical information Processing facilities (including locations hosting IT systems such as data centres, telecommunication equipment, wiring / cabling closets, HVAC equipment, sensitive physical media and bulk storage and filing areas) are appropriately protected against accident or attack, unauthorised physical access, power outages and natural hazards; and

(b) it physically protects all Avaya facilities in accordance with documented policies and standards.

7 Communications and Operations Management

7.1 Avaya designs computer systems, networks and telecommunications installations (e.g. data centers, labs, etc) to be protected using a defense-in-depth approach of overlapping levels of security controls.

7.2 Avaya:

(a) has documented standards / procedures for information systems, network and telecommunication installation designs, which leverage security by design, defense in depth, and Least Privilege and are subject to change management controls;

(b) configures information systems, networks and telecommunication installations securely, and to the degree possible, manages them centrally and monitors with minimal manual intervention;

(c) backups information in accordance with a defined backup and retention cycle and ensure that it is capable of being restored in accordance with applicable service levels. Backups shall be secure, encrypted where applicable, and available.

(d) documents, defines, and adheres to a data leakage protection (DLP) requirement;

(e) only uses mobile computing devices, such as laptops, using standard technical configurations and subject to Avaya security policies to protect Sensitive Data against unauthorised disclosure, loss, or theft;

(f) uses documented processes to grant access to employees who may use employee-owned (non-corporate) devices for business purposes and apply technical security controls to protect business information;

(g) protects electronic communication systems, including email systems, electronic file systems, instant messaging systems and electronic collaboration applications, systems and services by a combination of policy, awareness, procedural and technical security controls;

(h) ensures that information transfers with Company and to third parties are undertaken securely and governed by standards, processes and controls commensurate with the associated level of sensitivity and criticality of the information being transferred;

(i) configures and manages networks to maintain security for the systems and applications using the network (fixed / wireless, internal / external and VoIP) including but not limited to protection against Denial of Service Attacks where reasonable;

(j) implements adequate and effective network level segregation and policy-based filtering mechanisms, to consistently protect Company Content against unauthorised access or disclosure through external or untrusted networks;

(k) configures firewalls to produce logs and implements as “deny all traffic excepting that which is specifically permitted”, reviewed regularly and subject to change control;

(l) ensures each external network connection is assessed for risk, logged, and governed appropriately;

(m) uses a current and secure communications protocol for data transfers involving Sensitive Data across public or untrusted networks including into and from Company networks;

(n) deploys formal documented processes and mechanisms for the identification and remediation of system and Software Vulnerabilities in business applications, information systems and Network Devices;

(o) installs, configures and maintains effective Malware protection mechanisms in accordance with Good Industry Practice throughout the organisation. This shall include referencing to reputable sources for information on Information Security Threats and Vulnerabilities;

(p) engages third party or internally operated Vulnerability assessments to identify Vulnerabilities and address them in a timely manner;

(q) uses reasonable endeavours to ensure that no Malware is, has been or shall be coded or introduced to systems that process information assets;

(r) applies new Software including patches, service packs and other updates in a manner that does not adversely affect the production environment;

(s) records Security Events in logs that are monitored, stored centrally and protected against unauthorised change;

(t) analyses the logs on a regular basis to identify and investigate anomalies;

(u) retains the logs as per legal and regulatory requirements and Avaya policies; and

(v) identifies and configures applications and Technical Infrastructure systems on which Security Event logging must be enabled to help identify Security Events.

8 Access Control

8.1 For the purposes of this paragraph 8 the term access management refers to a method or combination of methods by which user is granted access to a business application, information system or supporting infrastructure (network or computing device) i.e. a user ID and password, passphrase, passcode, PIN, token, digital certificate or biometrics.

8.2 Avaya:

(a) ensures access to business applications and supporting infrastructure is allocated on a Least Privilege basis and is role based where technically possible;

(b) assigns to each individual who needs to have access to Avaya systems, a unique user ID and authentication method to access the relevant system, in line with a formally documented process;

(c) segregates critical access control roles such as access authorisation, access administration, and system administration;

(d) suspends or disables user IDs which are inactive after a reasonable period of time; and

(e) operates a password policy which is aligned with Good Industry Practice.

8.3 Avaya ensures that:

(a) remote access requires multi-factor authentication;

(b) the number of unsuccessful log-on attempts is limited to five;

(c) users are notified of the terms and conditions for accessing the system; and

(d) any error messages generated during the sign-on process contain only minimal information needed without disclosing the actual cause of an authentication failure.

8.4 Avaya maintains a record of all users permitted to access and use systems and has regular validation processes in place.

8.5 Avaya implements formal documented processes for granting, managing and monitoring Privileged Access to production systems with robust change control procedures. Privileged Access user shall not be granted privileges to move files such as program source code, binaries, libraries or patches between production and non-production environments without appropriate emergency change or exception approvals and in alignment with appropriate controls.

8.6 Avaya establishes and monitors emergency change control (any fix applied directly to data or systems outside the usual established change management process) for any exceptional access requirements such as investigation and resolution of incidents and:

(a) revokes emergency access and does password reset upon the resolution of the production problem(s) or completion of the change control activity;

(b) does not employ emergency access for extended use or to bypass routine procedures; and

(c) logs each request for an emergency ID with user ID, date, time and dataset name(s).

8.7 Avaya employs a protected channel (e.g. utilising encrypted protocols or VPN tunnels) for remote system, network and security administration activities over insecure networks to mitigate the risk from unauthorised interception and eavesdropping Threats.

8.8 Avaya ensures the segregation of duties for critical and sensitive roles and reduce reliance on key individuals.

8.9 Avaya operates a joiners, movers and leavers process to grant, amend or revoke access privileges promptly.

9 Information systems acquisition, development and maintenance

9.1 Avaya:

(a) carries out system development and maintenance activities in accordance with a documented secure and quality assured system development lifecycle methodology;

(b) physically or logically segregates production environments from test or development environments to reduce the risk of unauthorised access or changes and minimise the impact of any potential incidents; and

(c) conducts risk assessments to identify and prioritise risks, enumerate Vulnerabilities and understand the impact that particular attacks might have on critical business applications used to deliver Services.

9.2 Avaya:

(a) ensures that a Security by Design and Privacy by Design approach is adopted, such that security and privacy shall be an integral part of systems to sufficiently manage risk whether developed internally, externally or acquired and security and privacy requirements shall be explicitly identified and documented during the initiation phase of a development effort, product acquisition or system maintenance;

(b) utilises formal change control procedures with appropriate authorisation and comprehensive audit trails for all changes to system and application source code, program libraries and configuration;

(c) does not use production databases or applications for testing purposes unless mutually agreed to resolve specific issues;

(d) removes or modifies beyond recognition (sanitize) all production data which is personal or confidential business data before copying to a non-production system, protect and control such data as in the production environment, or implement other applicable controls to protect such data;

(e) where unsanitized production data (personal information and / or confidential business information residing within the production environment) is required for addressing an exceptional testing or troubleshooting requirement, follows a formal process for undertaking controlled testing using such data;

(f) develops applications using secure coding principles and best practices;

(g) ensures that all application systems shall provide audit trails and activity logs consistent with Good Industry Practice;

(h) ensures that applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g. OWASP for web applications);

(i) embeds application security testing within the Software development life cycle to ensure security requirements are fully addressed; and

(j) embeds automation, where possible, of security practices into the Software development life cycle.

9.3 If a cryptographic mechanism such as encryption or hashing is used, Avaya uses current and publicly proven cryptographic algorithms, Cryptographic Protocols and key lengths with a long term protection outlook.

9.4 Avaya uses a secure method for managing keys, including activation only in accordance with formalized processes. In addition to the foregoing Avaya will:

(a) use a secure method for storing keys and ensure that access to keys requires authorization, and

(b) securely backup or escrow encryption keys.

9.5 Avaya stores securely or encrypts files, scripts or code containing passwords for system IDs or process IDs used by processes for application or data transmission (e.g. file transfer).

9.6 Avaya protects business applications and supporting components and platforms such as databases and middleware by using sound Security Architecture principles aligned to appropriate architectural frameworks.

9.7 Avaya maintains an accurate and up to date inventory of business applications.

10 Information Security Incident Management

10.1 An Information Security incident is an event that that has been confirmed to result in a breach of Sensitive Data (including Company's), or is otherwise reasonably suspected to result in such a breach.

10.2 Avaya will:

(a) as part of the Information Security management process, identify, communicate, respond to and recover from security incidents including cybercrime (including targeted attacks using a range of vectors such as Malware or social engineering against organisations or individuals) and business disruption. A formal documented process shall be established for conducting forensic investigations where applicable;

(b) promptly report to Company any Information Security incident, in alignment with contractually and mutually agreed terms;

(c) ensure that investigations of Information Security incidents comply with relevant legal requirements. These investigations shall provide, and retain, full documentary substantiation of the investigation; and

(d) manage Threats proactively to reduce service disruption and business impact.

10.3 Avaya carries out any reasonable and necessary investigation in relation to any such incidents or breaches. Subject to confidentiality restrictions in respect to non-Company Sensitive Data, Avaya may share summary reports of such investigations that impact Company's Sensitive Data.

11 Security of Business Continuity Management

11.1 Avaya applies the security and privacy controls specified in this ISA to all the business continuity and disaster recovery arrangements and activities, to ensure consistent protection for Company Content.

11.2 Avaya establishes and maintains an overview of its business continuity and disaster recovery programs, setting out contingency arrangements to avoid or minimise the impact to the continuing performance of Avaya's obligations under this ISA in the event of any incident or event which materially affects the performance of Avaya's obligation under this ISA.

11.3 Avaya tests and reviews at least once in each calendar year its business continuity and disaster recovery plan.

11.4 Avaya regularly takes and tests backups in accordance with a defined and documented schedule to ensure timely recovery of Company Content.