RingCentral Security Addendum

1. Scope

This document describes the Information Security Measures ("Measures") that RingCentral has in place when processing Protected Data through RingCentral Services.

2. Definitions

For purposes of this Security Addendum only, capitalized terms, not otherwise defined herein, have the meaning set forth in the Agreement.

a. "**RingCentral Services**", or "**Services**", means services offered by RingCentral and acquired by the Customer.
b. "**Customer**" means the entity that entered into the Agreement with RingCentral.
c. "**Protected Data**" means Customer and partner data processed by RingCentral Services, as defined in the applicable RingCentral DPA or Agreement, including "personal data" and "personal information" as defined by applicable privacy laws, confidential data as defined in the Agreement, account data, configuration data, communication content including messages, voicemail, and video recording.
d. "**Agreement**" means the agreement in place between RingCentral and the Customer for the provision of the Services.
e. **"Personnel"** means RingCentral employees, contractors or subcontracted Professional Services staff.

3. Information Security Management

a. Security Program.

RingCentral maintains a written information security program that:

i. Includes documented policies or standards appropriate to govern the handling of Protected Data in compliance with the Agreement and with applicable law.
ii. Is managed by a senior employee responsible for overseeing and implementing the program.
iii. Includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Protected Data.
iv. Is appropriate to the nature, size, and complexity of RingCentral's business operations.

b. Security Policy Management.

RingCentral's security policies, standards and procedures:

i. Align with information security established industry standards.
ii. Are subject to ongoing review.
iii. May be revised to reflect changes in industry best practices.

c. Risk Management.

RingCentral:

i. Performs cybersecurity risk assessments to identify threats to their business or operations at least annually.
ii. Updates RingCentral policies, procedures and standards as needed to address threats to RingCentral's business or operations.

4. Independent security assessments

a. External Audit.

RingCentral:

i. Uses qualified independent third-party auditors to perform security audits covering systems, environments and networks where Protected Data is processed, including
    a. SOC2 Type II
    b. IES/ISO 27001.

ii. maintains additional audits and compliance certifications as appropriate for RingCentral's business and as identified at www.ringcentral.com/trust-center.html .

b. Distribution of Reports.

Copies of relevant audit reports and certifications

i. Will be provided to Customer on request,
ii. Are subject to Non-Disclosure Agreement.

c. Annual Risk Assessment Questionnaire.

Customer may, on one (1) occasion within any twelve (12) month period, request that RingCentral complete a third-party risk assessment questionnaire within a reasonable time frame.

In case of conflict between this section and the equivalent section in the RingCentral DPA, the DPA takes precedence.

5. Human Resource Security

a. Background Checks.

RingCentral requires pre-employment screenings of all employees. RingCentral ensures criminal background searches on its employees to the extent permitted by law. Each background check in the US includes:

i. An identity verification (SSN trace).
ii. Criminal history checks for up to seven (7) years for felony and misdemeanors at the local, state, and federal level, where appropriate.
iii. Terrorist (OFAC) list search, as authorized by law.

Internationally, criminal history checks are conducted as authorized by local law.

Background checks are conducted by a member of the National Association of Professional Background Screeners or a competent industry-recognized company in the local jurisdiction.

b. Training.

RingCentral will ensure that all employees including contractors:

i. Complete annual training to demonstrate familiarity with RingCentral's security policies.
ii. Complete annual training for security and privacy requirements, including CyberSecurity awareness, GDPR, and CCPA.
iii. Have the reasonable skill and experience suitable for employment and placement in a position of trust within RingCentral.

c. Workstation Security.

RingCentral ensures that:

i. RingCentral employees either use RingCentral owned and managed devices in the performance of their duties or Bring Your Own Device (BYOD) device.
ii. All devices, whether RingCentral owned and managed or Bring Your Own Device (BYOD) device, are enrolled in the full RingCentral managed device program.

d. Data Loss Prevention.

RingCentral employs a comprehensive system to prevent the inadvertent or intentional compromise of RingCentral data and Protected Data.

e. Due Diligence over Sub-Contractors.

RingCentral will:

i. maintain a security process to conduct appropriate due diligence prior to engaging sub-contractors.

ii. assess the security capabilities of any such sub-contractors on a periodic basis to ensure subcontractors' ability to comply with the Measures described in this document.
iii. apply written information security requirements that oblige sub-contractors to adhere to RingCentral's key information security policies and standards consistent with and no less protective than these Measures.

f. Non-disclosure.

RingCentral ensures that employees and contractors/sub-contractors who process Protected Data are bound in writing by obligations of confidentiality.

6. Physical Security

a. General.

RingCentral:

i. Restricts access to, controls, and monitors all physical areas where RingCentral Services process Protected Data ("Secure Areas").
ii. Maintains appropriate physical security controls on a 24-hours-per-day, 7-days-per-week basis ("24/7").
iii. Revokes any physical access to Secure Areas promptly after the cessation of the need to access buildings and system(s).
iv. Performs review of access rights on at least an annual basis.

b. Access and Authorization Processes.

RingCentral maintains a documented access authorization and logging process. The authorization and logging process will include at minimum:

i. Reports detailing all access to Secure Areas, including the identities and dates and times of access.
ii. Reports to be maintained for at least one year as allowed by law.
iii. Video surveillance equipment to monitor and record activity at all Secure Areas entry and exit points on a 24/7 basis to the extent permitted by applicable laws and regulations.
iv. Video recording to be maintained for at least 30 days or per physical location provider's policies.

c. Data Centers.

To the extent that RingCentral is operating or using a data center, RingCentral ensures that physical security controls are in alignment with industry standards such as ISO 27001 and SSAE 16 or ISAE 3402 or similar standard including:

i. Perimeter security including fencing/barriers and video surveillance.

ii. Secure access including security guard/reception.
iii. Interior access controlled through RFID cards, 2FA, anti-tailgating controls.
iv. Redundant utility feeds and support for continuous delivery through backup systems.
v. Redundant network connection from multiple providers.

Physical access to the data centers housing RingCentral's production servers, backup media, and related hardware is restricted to operations employees with specific job functions to address operational needs.

7. Logical Security

a. User Identification and Authentication.

RingCentral:

i. Maintains a documented user management lifecycle management process that includes manual and/or automated processes for approved account creation, account removal and account modification for all Information Resources and across all environments.
ii. Ensures that RingCentral users have an individual accounts for unique traceability.
iii. Ensures that RingCentral users do not use shared accounts; where shared accounts are technically required controls are in place to ensure traceability.
iv. RingCentral user passwords are configured aligned with current NIST guidance.

For the customer facing applications, Customers may choose to integrate with SSO (Single Sign on) so that Customer retains control over their required password settings including Customer's existing MFA/2FA solutions.

b. User Authorization and Access Control.

RingCentral:

i. Configures remote access to all networks storing or transmitting Protected Data to require multi-factor authentication for such access.
ii. Revokes access to systems and applications that contain or process Protected Data promptly after the cessation of the need to access the system(s) or application(s).
iii. Has the capability of detecting, logging, and reporting access to the system and network or attempts to breach security of the system or network.

RingCentral employs access control mechanisms that are intended to:

i. Limit access to Protected Data to only those Personnel who have a reasonable need to access said data to enable RingCentral to perform its obligations under the Agreement.
ii. Prevent unauthorized access to Protected Data.
iii. Limit access to users who have a business need to know.
iv. Follow the principle of least privilege, allowing access to only the information and resources that are necessary; and

v. Perform review access controls on a minimum annual basis for all RingCentral's systems that transmit, process, or store Protected Data.

8. Telecommunication and Network Security

a. Network Management.

RingCentral:

i. Maintains network security program that includes industry standard firewall protection and two-factor authentication for access to RingCentral's networks.
ii. Deploys an Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) to generate, monitor, and respond to alerts which could indicate potential compromise of the network and/or host.
iii. Monitors web traffic from the Internet and from internal sources to detect cyber-attacks including Distributed Denial of Service (DDoS) attacks against web sites / services and to block malicious traffic.

b. Network Segmentation.

RingCentral:

i. Implements network segmentation between the corporate enterprise network and hosting facilities for Services.
ii. Ensures separation between environments dedicated to development, staging, and production.
iii. Restricts access between environments to authorized devices.
iv. Controls configuration and management of network segregation and firewall rules through a formal request and approval process.

c. Network Vulnerability Scanning.

RingCentral:

i. Runs internal and external network vulnerability scans against information processing systems at least quarterly.
ii. Evaluates findings based on (where applicable) CVSS score and assessment of impact, likelihood and severity.
iii. Remediates findings following industry standard timelines.

9. Operations Security

a. Asset Management.

RingCentral:

i. Maintains an accurate and current asset register covering hardware and software assets used for the delivery of services.

ii. Maintains accountability of assets throughout their lifecycle.
iii. Maintains processes to wipe or physically destroy physical assets prior to their disposal.

b. Configuration Management.

RingCentral:

i. Maintains baseline configurations of information systems and applications based on industry best practices including
    a. Removal of all vendor-provided passwords
    b. Remove/disable unused services and settings
    c. Anti-malware/endpoint protection as technically feasible.
ii. Enforces security configuration settings for systems used in the provision of the Services.
iii. Ensures that clocks of all information processing systems are synchronized to one of more reference time sources.

c. Malicious Code Protection.

i. To the extent practicable, RingCentral has endpoint protection in place, in the form of Endpoint Detection and Response (EDR) and/or antivirus software, installed and running on servers and workstations.
ii. EDR alerts are monitored and immediate action is taken to investigate and remediate any abnormal behavior.
iii. Where used, antivirus software will be current and running to scan for and promptly remove or quarantine viruses and other malware on Windows servers and workstations.

d. Vulnerability, Security Patching.

RingCentral:

i. Monitors for publicly disclosed vulnerabilities and exposures for impact to Supplier's information systems and products.
ii. Ensures quality assurance testing of patches prior to deployment.
iii. Ensures that all findings resulting from network vulnerability scanning and relevant publicly disclosed vulnerabilities and exposures are remediated according to industry best practices, including CVSS score and assessment of impact, likelihood and severity and are remediated following industry standard timelines.

e. Logging and Monitoring.

RingCentral shall ensure that:

i. All systems, devices or applications associated with the access, processing, storage, communication and/or transmission of Protected Data, generate audit logs.
ii. Access to Protected Data is logged.
iii. Logs include sufficient detail that they can be used to detect significant unauthorized

activity.

iv. Logs are protected against unauthorized access, modification and deletion.

v. Logs are sent to a centralized location for aggregation and monitoring.

10. Software Development and Maintenance

a. Secure development lifecycle.

RingCentral:

i. Applies secure development lifecycle practices, including, during design, development and test cycles.

ii. Ensures that products are subject to security design review including threat considerations and data handling practices.

iii. Ensures that Services are subject to a secure release review prior to promotion to production.

b. Security Testing.

As part of the secure development lifecycle, RingCentral:

i. Performs rigorous security testing, including, as technically feasible,
   a. static code analysis,
   b. source code peer reviews,
   c. dynamic and interactive security testing and
   d. security logic, or security "QA" testing.

ii. Ensures that Internet-facing applications are subject to application security assessment reviews and testing to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities, CWE/SANS Top 25 vulnerabilities).

iii. For all mobile applications (i.e. running on Android, Blackberry, iOS, Windows Phone) that collect, transmit or display Protected Data, conducts an application security assessment review to identify and remediate industry-recognized vulnerabilities specific to mobile applications.

iv. Does NOT use Protected Data for testing.

v. Makes all reasonable effort to identify and remediate software vulnerabilities prior to release.

c. Annual Penetration Testing.

RingCentral:

i. Engages qualified, independent third-party penetration testers to perform annual penetration test against its Products and environments where Protected Data is hosted.

ii. Requires sub-processors to perform similar penetration testing against their systems, environments and networks.

iii. Ensures remediation of all findings in a commercially reasonable period of time.

d. Product Vulnerability Management.

RingCentral:

i. Uses commercially reasonable efforts to regularly identify software security vulnerabilities in RingCentral Services.
ii. Provides relevant updates, upgrades, and bug fixes for known software security vulnerabilities, for any software provided or in which any Protected Data is processed.
iii. Ensures that all findings resulting from internal and external testing are evaluated according to industry best practices, including CVSS score and assessment of impact, likelihood and severity and are remediated following industry standard timelines.

e. Open Source and Third-Party Software.

RingCentral:

i. Uses commercially reasonable efforts to ensure the secure development and security of open source software and third-party software used by RingCentral.
ii. Uses commercially reasonable efforts to evaluate, track and remediate vulnerabilities of open source software (OSS) and other third party libraries that are incorporated into the Services.

11. Data Handling

a. Data Classification

RingCentral maintains data classification standards including:

i. Public data, data that is generally available or expected to be known to the public.
ii. Confidential data, data that is not available to the general public.

Protected Data is classified as RingCentral Confidential Data.

b. Data Segregation.

RingCentral:

i. Ensures physical or logical segregation of Protected Data from other customers' data.
ii. Ensures physical separation and access control to segregate Protected Data from RingCentral data.

c. Encryption of Data.

RingCentral:

i. Shall ensure encryption of Protected Data in electronic form in transit over all public wired networks (e.g., Internet) and all wireless networks (excluding communication over Public Switch Telephone Networks).
ii. Excepting the Engage Communities feature of Engage Digital, shall ensure encryption of Protected Data in electronic form when stored at rest.
iii. Uses industry standard encryption algorithms and key strengths to encrypt Protected Data in transit over all public wired networks (e.g., Internet) and all wireless networks.

d. Destruction of Data.

RingCentral shall:

i. Ensure the secure deletion of data when it is no longer required.
ii. Ensure that electronic media that has been used in the delivery of Services to the Customer will be sanitized before disposal or repurposing, using a process that assures data deletion and prevents data from being reconstructed or read.
iii. Destroy any equipment containing Protected Data that is damaged or non-functional.

12. Incident Response

RingCentral's incident response capability is designed to comply with statutory and regulatory obligations governing incident response. As such, RingCentral

i. Maintains an incident response capability to respond to events potentially impacting the confidentiality, integrity and/or availability of Services and/or data including Protected Data.
ii. Has a documented incident response plan based on industry best practices.
iii. Has a process for evidence handling that safeguards the integrity of evidence collected to including allowing detection of unauthorized access to, and
iv. Will take appropriate steps and measures to comply with statutory and regulatory obligations governing incident response.

When RingCentral learns of or discovers a security event which impacts Protected Data, RingCentral will notify Customer without undue delay and will take commercially reasonable steps to isolate, mitigate, and/or remediate such event.

13. Business Continuity and Disaster Recovery

a. Business Continuity.

RingCentral:

i. Ensures that responsibilities for service continuity are clearly defined and documented and have been allocated to an individual with sufficient authority.
ii. Has a business continuity plan (BCP) in place designed to provide ongoing provision of the Services to Customer.
iii. Develops, implements, and maintains a business continuity management program to address the needs of the business and Services provided to the Customer. To that end, RingCentral completes a minimum level of business impact analysis, crisis management, business continuity, and disaster recovery planning.
iv. Ensures that the scope of the BCP encompasses all relevant locations, personnel and information systems used to provide the Services.
v. Ensure that its BCP includes, but is not limited to, elements such location workarounds, application workarounds, vendor workarounds, and staffing workarounds, exercised at minimum annually.
vi. Reviews, updates and tests the BCP at least annually.

b. Disaster Recovery.

RingCentral:

i. Maintains a disaster recovery plan, which includes, but is not limited to, infrastructure, technology, and system(s) details, recovery activities, and identifies the people/teams required for such recovery, exercised at least annually.
ii. Ensures that the disaster recovery plan addresses actions that RingCentral will take in the event of an extended outage of service.
iii. Ensures that its plans address the actions and resources required to provide for (i) the continuous operation of RingCentral, and (ii) in the event of an interruption, the recovery of the functions required to enable RingCentral to provide the Services, including required systems, hardware, software, resources, personnel, and data supporting these functions.