RingCentral Vendor Security Addendum

The RingCentral Vendor Security Addendum forms part of the Agreement between RingCentral and Vendor and sets out the minimal technical and organizational measures that Vendor will implement to protect RingCentral Data.

1. **Information Security Management**
   Vendor will maintain appropriate cybersecurity measures to safeguard the security of RingCentral Data. In no event shall Vendor take precautions any less stringent than those employed to protect its own proprietary and confidential information. In addition, Vendor agrees to develop and maintain any additional cybersecurity measures as may be required by applicable Privacy Laws. Vendor will maintain a cybersecurity and risk management program based on commercial best practices to preserve the confidentiality, integrity and accessibility of RingCentral Data with comprehensive administrative, technical, procedural and physical measures conforming to generally recognized industry standards and best practices that include the following:

   i. **Cybersecurity Program**

      Vendor must keep RingCentral Data secure from accidental, unauthorized or unlawful access, use, disclosure, alteration, destruction and / or loss by using administrative, technical, procedural, and physical safeguards that are reasonable and appropriate to the circumstances, taking into account the nature of RingCentral Data and the scope, context and purposes of the Processing (individually, a "**Safeguard**"; all Safeguards collectively, the "**Cybersecurity Program**").

   ii. **Documentation**
      Vendor will maintain documentation that describes in detail Your Cybersecurity Program and the specific Safeguards You employ ("**Written Security Policy, Procedure, and Standards, Technical implementation details**").

   iii. **Changes**
      Vendor will refrain from making any changes to Your Cybersecurity Program or specific Safeguards that reduce the level of security provided to RingCentral Data.

   iv. **System Security**
      a) Actively monitor industry resources (e.g., www.cert.org, pertinent software vendor mailing lists and websites, and information from subscriptions to automated notifications) for timely notification of applicable security alerts that pertain to Information Resource.
      b) Scan Information Resources at least quarterly with industry-standard security vulnerability scanning software to detect security vulnerabilities. remediate all critical, high, and moderate-risk security vulnerabilities as defined by FedRAMP. Scan must cover all Information Resources utilized to Process RingCentral Data.
      c) Install and use Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) that monitor all non-VoIP traffic entering and leaving Information Resources utilized for Processing RingCentral Data.
      d) Maintain and adhere to a documented Process to remediate security vulnerabilities that may impact Information Resources, including those discovered through industry publications, vulnerability scanning, virus scanning, IDS/IPS alerts, and the review of security logs, and apply appropriate security patches for critical, high, moderate (criticality and remediation timeline as defined by FedRAMP) risk security vulnerabilities. Security patches shall be tested prior to installation to ensure they will not be service impacting. If Vendor

determines that the patch will be service impacting, Vendor must contact RingCentral to mutually agree on a remediation plan.

e) Assign security administration responsibilities for configuring the security parameters of host operating systems to authorized users only

f) Harden Information Resources by establishing and utilizing a minimum-security baseline configuration based upon functional system needs and industry best practices to reduce available ways of attack. This typically includes changing default passwords, the removal of unnecessary software, UserIDs, usernames, and logins, and the disabling or removal of unnecessary services. Such hardening of the system's security configurations, operating system software, firmware and applications are to prevent exploits that attack flaws in the underlying configuration.

v. Network Security

a. Vendor agrees to maintain network security that includes industry standard firewall protection and periodic vulnerability scans for the relevant Computing Systems.

b. When providing Internet accessible services to RingCentral, have Denial of Service (DoS/DDoS) and gateway security protections in place. Web servers must reside in a DMZ and Information Resources storing RingCentral Data (such as application and database servers) must reside in a trusted internal network.

c. For the purpose of demonstrating compliance with certain Security Requirements applicable to network architecture and network topology, if requested by RingCentral, provide a high-level copy of their logical network diagram. The network diagram needs to provide information regarding placement of Information Resources and security devices (such as Security Gateways, servers, DMZs, IDS/IPS, DoS/DDoS protections, databases, application servers, virtual private clouds (VPCs), and instances, etc.) used by Vendor Entities to Process RingCentral Data. Vendor is not required to provide all information in a single diagram and may provide multiple diagrams to convey this information (such as a security diagram, an application service diagram, a network topology diagram, etc.)

d. Require Multi-Factor Authentication for administrative and/or management access to Security Gateways, including any access for the purpose of reviewing log files.

e. Maintain documented controls, policies, processes and procedures to ensure that unauthorized users do not have administrative and/or management access to Security Gateways, and that user authorization levels to administer and manage Security Gateways are appropriate.

f. At least annually, ensure that each Security Gateway rule was properly authorized and is traceable to a specific business purpose, and that all rule sets either explicitly or implicitly end with a "DENY ALL" statement.

g. Use monitoring tools to ensure that all aspects of Security Gateways (e.g., hardware, firmware, and software) are operational at all times. Ensure that all non-operational Security Gateways are configured to deny all access.

h. When using radio frequency (RF) based wireless networking technologies (e.g., Bluetooth and Wi-Fi) to perform or support RingCentral Data Processing, ensure that all RingCentral Data transmitted must use appropriate encryption technologies sufficient to protect the confidentiality of RingCentral Data; provided, however, in any event such encryption shall use no less than key lengths of 256-bits for symmetric encryption and 2048-bits for asymmetric encryption. The use of RF-based wireless headsets, keyboards, microphones, and pointing devices, such as mice, touch pads, and digital drawing tablets, is excluded from this requirement.

vi. Connectivity Requirements

In the event that Vendor has, or will be provided, connectivity to RingCentral's or RingCentral's customers' Nonpublic Information Resources in connection with RingCentral Data Processing, then Vendor shall not establish additional interconnections to RingCentral and RingCentral's customers' Nonpublic Information Resources without the prior consent of RingCentral and shall:

a. Use only the mutually agreed upon facilities and connection methodologies to interconnect RingCentral and RingCentral's customers' Nonpublic Information Resources with Vendor's Information Resources.

b. If the agreed upon connectivity methodology requires that Vendor implement a Security Gateway, maintain logs of all sessions using such Security Gateway. Such session logs must include sufficiently detailed information to assist with a security incident or a forensic investigation (e.g., identification of the end user or application accessing RingCentral). Such session logs must include origination IP address, destination IP address, ports/service protocols used and duration of access. Such session logs must be retained for a minimum of six (6) months.

vii. **Server and Endpoint Security**

a. Vendor agrees to ensure that Your Computing Systems are patched and up-to-date with all appropriate security updates as designated by the relevant manufacturer or authority (e.g. Microsoft notifications, etc.) and are free of known viruses, worms, spyware, adware, malware, and other malicious and unwanted software and programs.

b. Where commercially reasonable, configure end user devices to ensure users are restricted from the ability to install unauthorized software, or to disable required software; provided, there may be reasonable exceptions to foregoing requirements as approved by Vendor's management and as documented in Vendor's policy.

viii. **Application Security**

Vendor agrees to use commercially reasonable efforts to regularly identify software vulnerabilities and, in the case of known software vulnerabilities, to provide relevant updates, upgrades, and bug fixes for any software provided to RingCentral or RingCentral's customers, or in which any RingCentral Data is Processed, in the course of fulfilling their obligations under the Standard Terms of Use.

ix. **Independent security assessments**

Vendor agrees to use independent third parties to perform annual penetration tests, red team or purple team exercises, risk assessments and security audits covering the systems, environments and networks where RingCentral Data is Processed. Vendor agrees to remediate all medium and higher severity findings and observations from such assessments.

x. **Strong Authentication**

Vendor will enforce Strong Authentication for any remote access to RingCentral Data and any remote use of Nonpublic Information Resources. Additionally, Vendor will enforce Strong Authentication for any administrative and/or management access to Vendor security infrastructure and Vendor log data including but not limited to firewalls, Identity and Access Management systems, security monitoring infrastructure, and computing logs such as firewall logs, server logs, DNS logs, etc.

xi. **Physical and Environmental Security**

a. Vendor will have in place physical premise security and environmental protections for Your Computing Systems, meeting ISO 27001/27002 standards.

b. Ensure all Information Resources intended for use by multiple users are located in secure physical facilities with access limited and restricted to authorized individuals only.

c. Monitor and record, for audit purposes, access to the physical facilities containing Information Resources intended for use by multiple users.

xii. **Data Security and Data Transparency**

1. Upon request from RingCentral, Vendor agrees to provide RingCentral with an inventory or data map of RingCentral Data that is in Vendor's possession or control, including locations of such data, and control measures that are in place for the protection of RingCentral Data.
2. All RingCentral data will be stored inside dedicated physical hardware for RingCentral Information database (the RingCentral customer database), Vendor core application stack, registration database, and dedicated telco application servers.
3. Maintain documented processes and controls to detect and terminate unauthorized attempts to access, collect, modify, store, handle and/or dispose of RingCentral data.
4. Maintain and adhere to documented processes for:

   1. the backup and recovery of RingCentral data and Information Resources under Vendor's or Vendors's Entities control and utilized for Processing RingCentral Data in accordance with any disaster recovery requirements; and

   2. the timely destruction and/or return of RingCentral data under Vendor's or Vendor's Entities' control and utilized for Processing RingCentral Data in accordance with any retention, return, and/or destruction requirements under this Agreement.

5. In jurisdictions where unauthorized access to RingCentral Data is a violation of the law, add the following statement to the warning notice: "In many jurisdictions, unauthorized access is a violation of law" or similar warning language.

xiii. **Personnel confidentiality**

Vendor will ensure that any person that Vendor authorizes to Process RingCentral Data (including Your staff, agents and subcontractors) will be subject to a strict duty of confidentiality (whether contractual or statutory).

xiv. **Cybersecurity Awareness and Training**

Vendor will have a cybersecurity awareness and training program in place that includes how to implement and comply with the Cybersecurity Program and promote a culture of security awareness through periodic communications from the organization's senior leadership.

xv. **Contingency Planning**

Vendor will have policies and procedures for responding to emergencies, cybersecurity incidents and other events (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage or remove access to RingCentral Data.

xvi. **Storage and Transmission Security**

a. Use Strong Encryption to protect RingCentral Data when transmitted over untrusted networks not controlled by Vendor.
b. Use Strong Encryption to protect RingCentral Data when stored.

xvii. **Secure Disposal**

Vendor will have policies and procedures regarding the secure disposal of tangible property containing RingCentral Data, considering available technology, so that RingCentral Data cannot be practically read or reconstructed.

xviii. **Monitoring and Logging**

a. Vendor will have intrusion detection systems, full audit trail logging, and security event detection and monitoring in place for networks, servers, and applications where RingCentral Data is stored, Processed, or transmitted. Vendor will log and maintain for 12 months all physical and logical access to RingCentral Data, including command history logging of all logical access. Vendor will also log and store all security events for 12 months, including but not limited to ACL logs, IDS logs, and SIM/SIEM events.

b. Restrict access to security logs to authorized individuals, and protect security logs from unauthorized modification.

c. Review, on no less than a weekly basis, all anomalies from security and security-related audit logs and document and resolve logged security problems in a timely manner.
   a. Such reviews may initially be performed by automated processes that promptly issue alarms and/or alerts when such processes detect significant anomalies so that the issuance of such alarms and/or alerts causes prompt investigation and review by responsible individuals; and
   b. If automated processes successfully resolve a logged security problem, no further action by responsible individuals is required.

d. When presented with evidence by RingCentral of a threat to RingCentral or RingCentral's customers' Nonpublic Information Resources originating from the Vendor's network (e.g., worm, virus or other malware, bot infection, Advanced Persistent Threat (APT), DoS/DDoS attack, etc.), Vendor shall promptly cooperate with RingCentral and take reasonable and necessary steps to isolate, mitigate, and/or terminate all known threats.

e. When Vendor learns of or discovers a known critical, high or moderate threat/vulnerability to the product of which impacts RingCentral (including but not limited to notifications received from security researchers or industry resources, bug bounty program, etc.), Vendor must promptly notify RingCentral business contact, cooperate with RingCentral, and take commercially reasonable steps to isolate, mitigate, and/or remediate such known threat/vulnerability.

f. In the event Vendor discovers that it is non-compliant with, or RingCentral notifies Vendor in writing that Vendor is non-compliant with these Security Requirements, then Vendor shall take commercially reasonable efforts to commence appropriate corrective action in no more than ninety (90) days and to work with RingCentral to establish a mutually agreed upon timeline for implementation of the relevant remediation measures.

xix. Passwords

When passwords are used to access RingCentral Data, Vendor will enforce Strong Authentication in all instances. Where practicable, Vendor will use a second authentication factor before granting access to RingCentral Data with a password.

a. Passwords must be complex and meet the following password construction requirements:
   a. Be a minimum of eight (8) characters in length.
   b. Include characters from at least two (2) of these groupings: alpha, numeric, and special characters.
   c. Not be the same as the UserID with which they are associated.
   d. Non-random PINs must meet the following:
   e. Be a minimum of four (4) numbers; and
   f. Not contain more than two (2) sequential numbers.
   g. Require passwords and PIN expiration at regular intervals not to exceed ninety (90) calendar days.

b. When providing users with a new or reset password, or other authentication credentials, use a secure method to provide this information and maintain a written policy requiring reset at first login whenever a temporary credential is used.

xx. Encryption

Vendor agrees to use Strong Encryption with minimum key lengths of 256-bits for symmetric encryption and 2048-bits for asymmetric encryption to protect RingCentral Data:

a) when transmitted over any network;
b) when stored (at rest); or
c) whenever authentication credentials are stored.

xxi. Least privilege

a. Vendor agrees to enforce the rule of least privilege by requiring application, database, network and system administrators to restrict user access to only the commands, data and Information Resources necessary for them to perform authorized functions. Log all successful and unsuccessful login attempts along with logoffs.

b. Ensure that controls are in place to limit, protect, monitor, detect and respond to all Privileged User activities.
Examples of such controls include enforcing:

1. The rule of least privilege
2. Separation of duties
3. Individual accountability
4. Change management
5. Auditability of Privileged User accounts and their activities
6. Audit log retention for a minimum of (6) six months

xxii. Access Management

Vendor agrees to have formal processes in place to grant, prevent and terminate access to RingCentral Data. The access should be limited to users who are required this access to perform their job responsibilities. Vendor agrees to have documented Access Management procedures in place.

xxiii. Identification and Authentication

a. Assign unique UserIDs to authorized individual users and ensure that there is individual accountability for use of Privileged User UserIDs. Additionally, disable all root logins through SSH.

b. Maintain a documented UserID lifecycle management process that includes manual and/or automated processes for approved account creation, account removal within one (5) business days, and account modification for all Information Resources and across all environments. Such process shall include review of access privileges and account validity to be performed at least each calendar year.

c. Where technically supported, limit failed login attempts by no more than six (6) consecutive failed login attempts by locking the user account. Access to the user account can be reactivated through the use of a manual process requiring verification of the user’s identity or, where such capability exists, can be automatically reactivated after at least three (3) minutes from the last failed login attempt.

xxiv. Software, Software Code, and Data Integrity

1. Separate non-production Information Resources from Production Information Resources. Additionally, Vendor will not use Customer messages or personal data for testing. Vendor will de-personalize Customer personal data prior to any use for development or testing. Maintain a documented change control process including back-out procedures for all production environments.

2. For applications which utilize a database that allows modifications to RingCentral Data, logs for forensic analysis purposes shall be created as follows:
    i. where transaction logging is supported have database transaction logging features enabled; or
    ii. where transaction logging is not supported, have some other mechanism that logs all modifications to RingCentral Data stored within the database including timestamp, UserID and information modified.
3. Such logs shall be retained for a minimum of six (6) months either on-line or on backup media and at RingCentral's request made available to RingCentral without undue delay.
4. For all software developed or customized for RingCentral under the Agreement, review and, where such tools are commercially available, scan such software to find and remediate malicious code and/or security vulnerabilities prior to initial deployment, upon code changes and/or at least annually, based on potential risk that a given vulnerability is or can be exploited as follows:
    i. Source code vulnerability scanning must be performed where such tools are commercially available. Where such tools are not commercially available, automated and/or manual processes and procedures must be documented and used.
    ii. Scan results and remediation plans must be made available to RingCentral upon request.

    Where technically feasible, for all software used, furnished and/or supported under the Agreement, review and scan such software to find and remediate security vulnerabilities prior to initial deployment, upon code changes and/or at least annually based on potential risk that a given vulnerability is or can be exploited.

5. Perform quality assurance testing for the security components (e.g., testing of identification, authentication and authorization functions), as well as any other activity designed to validate the security architecture, during initial implementation and upon significant modifications and updates.

2.

i. Reporting Violations

a. Maintain a documented procedure to be followed in the event of a suspected attack upon, intrusion upon, unauthorized access to, loss of, or other security breach involving RingCentral Data in which Vendor shall:
    1. Promptly investigate and determine if such an attack has occurred; and
    2. If a successful attack has occurred involving RingCentral Data or it is impossible to determine whether a confirmed attack was successful in compromising RingCentral Data then the Vendor shall promptly notify RingCentral.

b. After notifying RingCentral whenever there is a successful attack upon, intrusion upon, unauthorized access to, loss of, or other breach of RingCentral Data, provide RingCentral with regular status updates, including, actions taken to resolve such incident, at mutually agreed intervals or times for the duration of the incident and, within seven (7) calendar days of the closure of the incident, provide RingCentral with a written report describing the incident, actions taken by the Vendor during its response and Vendor's plans for future actions to prevent a similar incident from occurring.

ii. Mobile and Portable Devices

a. Use Strong Encryption to protect all RingCentral Data stored on Mobile and Portable Devices.

b. Use Strong Encryption to protect all RingCentral Data transmitted using or remotely accessed by network-aware Mobile and Portable Devices.

c. Maintain documented policies, standards and procedures for Mobile and Portable Devices used to access and/or store RingCentral Data that include the following requirements:

1. All users must be authorized for such access and their identity authenticated;
2. Mobile and Portable devices must be physically secured and/or in the physical possession of authorized individuals;
3. Where technically feasible, use a remote wipe capability on such devices to promptly and securely delete RingCentral Data, when such devices are not in the physical possession of authorized individuals nor otherwise physically secured; and
4. Jail-broken or rooted smartphones cannot be used to process RingCentral Data.

d. Implement and maintain a documented policy that prohibits the use of any:

1. Vendor-issued Mobile and Portable Devices to access and/or store RingCentral Data unless the device is administered and/or managed by Vendor; and
2. Non-Vendor issued Mobile and Portable Devices to access and/or store RingCentral Data unless adequately segregated and protected by utilizing a Vendor administered and/or managed secure container-based and/or sandbox solution.

iii. Vendor Entity Compliance

a. Vendor shall:

1. Ensure all Vendor Entities performing RingCentral Data Processing are aware of these Security Requirements.
2. Ensure all Vendor Entities performing any Services are contractually obligated to comply with these Security Requirements, or in any event, requirements that are substantially similar or equivalent.

b. Upon RingCentral's request, Vendor will provide documentation and/or evidence to adequately substantiate such compliance.

iv. Cloud Services

When placing RingCentral Data in a Cloud Service, Vendor will use commercially available products to enforce:

1. Multi-Factor Authentication for all Privileged Users.
2. Strong Encryption for RingCentral Data when transmitted to and from a Cloud Service.
3. Strong Encryption to protect RingCentral Data when stored within a Cloud Service.

3. PCI DSS

Vendor agrees to maintain compliance with PCI DSS standards for all Processing, storage, or transmission of Cardholder Data and Sensitive Authentication Data on behalf of RingCentral or RingCentral customers.

4. Adequate Security Measures and Procedures

Upon RingCentral's request, and following all necessary confidentiality undertakings, Vendor will provide RingCentral, at Vendor's expense, a third-party certification, third-party audit report, or written statement of a Vendor officer certifying that Vendor and its affiliates, agents, contractors, consultants, joint ventures and other Third Parties having access to or control of RingCentral Data have complied with all of the requirements of this Security Attachment (the "Certification"). Such Certification must have been conducted within the last twelve (12) months of the request. If RingCentral believes such internal controls and cybersecurity measures as expressed in this documentation are inadequate to safeguard the RingCentral Data, RingCentral may require the adoption of additional reasonable controls, security measures, and procedures. If Vendor fails to do so within a reasonable time, such failure shall be deemed to be a material breach of the Agreement, and RingCentral shall be permitted to terminate the Agreement immediately.

5. Audit Rights

RingCentral may, on one (1) occasion within any consecutive twelve (12) month period, request with thirty (30) days prior written notice in accordance with the Agreement to perform a reasonable security audit of Vendor's security measures and security program in order to ascertain compliance with applicable law, these information security requirements, non-disclosure agreements, and any agreements between the Vendor and RingCentral with respect to RingCentral data. Any issues/findings noted from this activity/audit will be reviewed by RingCentral and RingCentral will determine the final plan for remediation of the issues/findings and communicate those to the Vendor. The vendor must fully cooperate during these audit activities and provide RingCentral (not limited to) documentation, required evidence and updates on remediation efforts for the findings noted from such audit activity. RingCentral may hire a third party to do these audits of the Vendor's security measures and security program. In the event of a security and/or data breach incident of RingCentral data, RingCentral reserves the right to initiate an audit listed under the "Audit Rights"section.

6. **Questionnaires and periodic due diligence**
   RingCentral will perform a periodic due diligence activity on Vendor's security program. As part of this activity, RingCentral may, on one (1) occasion within any consecutive six (6) month period, request the Vendor to complete a security questionnaire to allow RingCentral review and measure Vendor's security measures and security program, in order to ascertain compliance with this agreement. Any issues/findings noted from this activity will be reviewed by RingCentral. Vendor agrees to remediate the high-risk findings in a timely manner and share with RingCentral the remediation plans for the issues/findings noted. The vendor must complete the questionnaire within 45 days of request made by RingCentral. The vendor must fully cooperate during these due diligence/review activities and provide RingCentral (not limited to) documentation, required evidence and updates on remediation efforts for the findings noted from such activity. RingCentral may hire a third party to do these diligence/review activities of the Vendor's security measures and security program.

7. **Definitions. For the purposes of this Security Attachment:**

   a) **"RingCentral Data**" shall have the meaning given to the terms "personal data" and "personal information" under Privacy Laws. This shall also include confidential data, including Customer Proprietary Network Information (CPNI), intellectual property, proprietary data and/or trade secret data of RingCentral, general RingCentral internal operational information, network architecture and/or engineering information, software source code for software developed or customized for RingCentral, information security incident reports, nonpublic marketing and financial information, any and all data provided to RingCentral by or on behalf of a RingCentral Customer for Processing on Customer's behalf, and RingCentral end user customer contact lists.

   b) "**Cardholder Data**" means the most current PCI Security Standards Council definition, as updated or amended from time to time. In determining whether a breach of this Security Attachment has occurred, "Cardholder Data" shall mean the definition of the PCI Security Standards Council in effect at the time of the breach.

   c) "**Computing Systems**" shall be defined as networks, servers, computers (inclusive of smartphones and tablet computers), applications, and other technology infrastructure that Vendor uses to deliver services in fulfillment of their obligations under the Agreement.

   d) "**Information Resource(s)"** means systems, applications, websites, networks, network elements, and other computing and information storage devices, along with the underlying technologies and delivery methods (e.g., social networks, mobile technologies, cloud services, call and voice recording, Application Program Interfaces (APIs)), used for RingCentral Data Processing.

   e) "**Nonpublic Information Resources"** means those Information Resources used under the Agreement to which access is restricted and cannot be gained without proper authorization and identification.

   f) "**Sensitive Authentication Data**" means the most current PCI Security Standards Council definition, as updated or amended from time to time. In determining whether a breach of this Security Attachment has occurred, "Sensitive Authentication Data" shall mean the definition of the PCI Security Standards Council in effect at the time of the breach.

g) "**Strong Authentication**" means the use of authentication mechanisms and authentication methodologies stronger than the passwords required by the applicable requirements herein. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.

h) "**Security Gateways**" means a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.

i) "**Cloud Service**" is a service delivered via an "as a Service" cloud service model, e.g., Software as a Service (SaaS), Storage as a Service (STaaS), Database as a Service (DBaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). "Customer-Facing System" means an Information Resource accessible from public networks which is intended for use by Customers.

j) "**Demilitarized Zone**" or "**DMZ**" is a network or sub-network that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the Internet. A DMZ helps prevent outside users from gaining direct access to internal Information Resources. Inbound packets from the untrusted external network terminate within the DMZ and are not allowed to flow directly through to the trusted internal network. All inbound packets which flow to the trusted internal network originate within the DMZ.

k) "**Mobile and Portable Devices**" means mobile and/or portable computers, devices, media and systems capable of being easily carried, moved, transported or conveyed that are used in connection with the Services. Examples of such devices include laptop computers, tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and mobile phones, such as smartphones.

l) "**Multi-Factor Authentication**" (also known as Two-Factor Authentication and Strong Authentication) means the use of at least two of the following three types of authentication factors: • A physical or logical credential the user has, such as an electronically readable badge, a token card or a digital certificate; • A knowledge-based credential, such as a password or PIN; and • A biometric credential, such as a fingerprint or retina image.

m) "**Privileged User**" means a user with enhanced administrative permissions and/or expanded or super user access greater than that of a general user. Examples of such access includes system administration of accounts, logs, encryption, databases, Security Gateways, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), virtual machines (VM), networks, image instances, and APIs, Cloud Service Provider (CSP) management and security portal accounts (excluding read-only accounts), and development and operations (DevOps) privileged activities. Privileged access by privileged users is applicable regardless of the types of devices and environments managed, including environments that are production, development, and test, within Vendor's facilities and/or within CSP cloud environments.

n) "**Vendor Entity**" or "**Vendor Entities**" means Vendor, its affiliates and subcontractors.