Subscriber Data Security Addendum

The obligations in this Subscriber Data Security Addendum ("**Security Addendum**") provide details about and are a part of iCIMS' technical and organizational measures to protect Subscriber Data processed under the Subscription Agreement and for assisting Subscriber Group Members with fulfilling their obligations to respond to Data Subjects' requests for exercise of their rights under Data Protection & Privacy Laws. iCIMS maintains a comprehensive set of policies and processes related to information security and privacy that comply with the ISO 27001 and ISO 27701 standards. The following identifies key controls used to protect Subscriber Data.

Unless otherwise defined below, all capitalized terms have the meaning given to them in the Subscription Agreement ("**Subscription Agreement**") and/or Data Processing Addendum ("**Data Processing Addendum**") between iCIMS and Subscriber. Any examples in this Security Addendum are illustrative and not the sole examples of a particular concept.

1. Measures of pseudonymization and encryption of Subscriber Data

All Subscriber Data shall be encrypted at rest and in transit by iCIMS or the iCIMS platform across any public network, using industry-standard measures,

a. Subscriber Data at rest: Shall use at least the AES 256-bit or better for encryption. Data at rest includes backups.
b. Subscriber Data in transit: Shall use TLS 1.2 or better for encryption.
c. Hashed data: Hashed data shall use bcrypt for the hashing algorithm.
d. Key exchange and digital signatures:
   - i. Key exchange shall use RSA or DSA cryptographic algorithms with a minimum key length of 2048 bits and minimum digest length of 256.
   - ii. Digital signatures shall use RSA, DSS with a minimum key length of 2048 bits and minimum digest length of 256

e. Pseudonymization: iCIMS has an internal Data Analytics Policy that requires iCIMS to use some or all of the following safeguards and techniques:
   - i. Suppression - removes the identifying values from a record (for example, removing the first and last name from a record)
   - ii. Generalization - replaces a data element with a more general element (for example, removing the day and month from a birthdate and leaving only the year)
   - iii. Noise Addition - replaces actual data values with other values that are selected from the same class of data (for example, the actual data may be salted to create a new value, where the salt value would be considered the addition of noise)
   - iv. Differential Privacy - requires the use of the k-anonymity method to ensure that within a dataset there are at least k individuals or customers who have exactly the same values for data elements that might become identifying for each individual or customer. iCIMS' policy requires a minimum value of k=20, which is consistent with current practices for public data release from other highly conservative organizations.
   - v. Outlier Removal - removes all outliers to minimize the extent to which those outliers allow for reidentification of an individual or customer.

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

    a. Background checks: Where required and/or permitted by applicable local law, iCIMS shall conduct a preemployment background and/or criminal records check on all new hires. Employment at iCIMS is contingent upon a satisfactory background and/or criminal records check, including where applicable:

        i. Social Security number trace.

        ii. Education.

        iii. Work Experience.

        iv. Criminal Background Check.

        v. Credit Check, if relevant to the position.

        vi. Reference Check.

        vii. Where required and/or permitted by applicable local law, iCIMS may also conduct background and/or criminal records checks on its employees throughout the course of their employment. Generally, this shall occur in circumstances involving transfer to a position of high-level security or responsibility.

    b. Ongoing confidentiality: Confidentiality obligations as specified in the Subscription Agreement.

    c. Security and privacy training: At least once per calendar year and during onboarding, iCIMS shall require all iCIMS Personnel with access to Subscriber Data to complete training on iCIMS' information security and privacy policies.

    d. Subscriber Data backup:

        i. iCIMS conducts a Backup at least daily and prior to any Update to the Subscription

        ii. CIMS maintains seven (7) days of encrypted daily Backups with high availability and transfers encrypted Backups to a secured storage location daily.

        iii. iCIMS also sends encrypted transaction logs to its disaster recovery facilities throughout the day.

        iv. In the event of a Disaster, iCIMS shall use commercially reasonable efforts to re-establish access to the Subscription within twenty-four (24) hours ("**Recovery Time Objective**").

        v. iCIMS shall use commercially reasonable efforts to recover Subscriber Data from a Backup made less than or equal to twenty-four (24) hours prior to the Disaster (the "**Recovery Point Objective**").

3. **Measures for ensuring the ability to restore the availability and access to Subscriber Data in a timely manner in the event of a physical or technical incident**

    a. Incident Management: iCIMS has in place an incident policy and process to be followed in the event of any Data Breach. iCIMS' incident response policy and process include:

        i. Roles and responsibilities: Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to Security Incidents, including formation of a security incident response team (SIRT) with an incident response leader.

        ii. Incident Response Process: Based on NIST 800-61 Rev.2, includes:

            1. Detection: Identification of a security or privacy event.
            2. Analysis: Determines whether a Security Incident or Privacy Incident has occurred. Notification is required within 24 hours of identification of a Data Breach or Abnormal Activities.
            3. Containment: Mitigates the root cause of the Security or Privacy Incident to prevent further damage or exposure.

4. <u>Eradication:</u> Removes vulnerabilities causing the Security or Privacy Incident, and any associated compromises, are removed from the environment.
5. <u>Recovery</u>: The Recovery Phase represents the SIRT's effort to restore the affected system(s) to operation after the problems that gave rise to the Security or Privacy Incident, and the consequences of the Security or Privacy Incident, have been corrected.
6. <u>Post-incident Activities</u>: Addresses notification and communication requirements, cooperation with external parties, information sharing, follow-up lessons learned, record keeping, and improvements.

b. <u>Disaster recovery and business continuity</u>: As specified in iCIMS' [Support & Maintenance Policy](#).

4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing

a. <u>Access controls:</u>

i. iCIMS shall:

1. Follow the principles of least privilege through a role-based access control model when granting iCIMS Personnel access to Subscriber Data.
2. Limit access to Subscriber Data to iCIMS Personnel with a legitimate need to access Subscriber Data to provide the Services in accordance with the Subscription Agreement.
3. Periodically (no less than quarterly) review iCIMS Personnel's access to Subscriber Data.
4. Promptly terminate an iCIMS Personnel's access to Subscriber Data if such individual's access is no longer required.
5. Review and disable user accounts after 90 days of inactivity.

b. <u>Network controls</u>: Access to internal and external network services that contain Subscriber's Data shall be controlled through:

i. Network access control lists (NACLs), or equivalent.
ii. Firewall policies, or equivalent.
iii. Security groups, or equivalent.
iv. IP whitelists, or equivalent.
v. A multi-tier architecture that prevents direct access to data stores from the internet.
vi. Usage of role-based access controls (RBAC) shall be implemented to ensure appropriate access to networks.
vii. Two-factor or multi-factor authentication (TFA or MFA) for remote access shall be implemented

c. <u>Vulnerability management and patch management</u>: iCIMS shall implement and maintain a vulnerability management program designed to identify and remediate vulnerabilities affecting production networks, systems, and applications that store or process Subscriber Data. The program shall include:

i. Penetration tests, conducted by an accredited third party, of iCIMS products and infrastructure that contain Subscriber Data are tested at least once per calendar year. Upon Subscriber's reasonable written request, iCIMS shall provide Subscriber an executive attestation of the test results. Subscriber shall treat such information as iCIMS' confidential information in accordance with 'Section 7 - Confidential Information' of the Subscription Agreement; and

ii. Routine vulnerability scans on all iCIMS products and infrastructure that contain Subscriber Data or that is used by iCIMS to gain access to Subscriber Data.

iii. If vulnerabilities are detected from such tests and scans, iCIMS shall remediate and apply applicable and necessary patches as follows:

1. Server operating systems shall be patched within 30 days of a critical and/or security patch release.
2. Workstations and Laptops shall be patched within 30 days of a critical and/or security patch release.

3. Network devices shall be patched within 30 days of the release of a critical and or security patch.
4. Zero-day patches shall be applied on all systems containing Subscriber Data and critical systems within 14 days, and all other systems within 30 days.
5. Patches shall be tested prior to rollout in the production environment. Less critical systems shall be patched first.
6. Application patches shall be applied in accordance with iCIMS' Support & Maintenance Policy.

d. iCIMS Software Development Practices: With respect to the software development lifecycle, iCIMS shall maintain and follow a written software development life cycle program based on the Open Web Application Security Project (OWASP) Top 10 standards.

Assigned Personnel who are responsible for secure application design, development, configuration, testing, and deployment receive appropriate training regarding iCIMS' secure application development practices. Development practices shall include:

i. Managing all code through a version control system to allow viewing of change history and content.
ii. Ensuring that a test engineering (i.e., quality assurance (QA)) methodology is followed using a multi-phase quality assurance release cycle that includes security testing.
iii. Delivering security fixes and improvements aligning to a pre-determined schedule based on identified severity levels.
iv. Performing vulnerability testing as a component of QA testing and address any severity 2 or higher findings prior to software release.
v. Ensuring that software is released only via production managed change control processes, with no access or involvement by the development and test teams
vi. Awareness training regarding secure coding shall be conducted at least once per calendar year.

e. Malware controls: iCIMS shall install and maintain reasonable and current controls designed to protect iCIMS networks, systems, and devices used by iCIMS to access Subscriber Data from malware and unauthorized software.

f. Security Assessments: Once per calendar year and upon reasonable notice no less than 45 days prior, Subscriber shall be entitled to perform a security and privacy assessment of the information security and privacy program.

g. Security certification and attestation: See Section 12.

5. Measures of user identification and authorization

a. Access Control: iCIMS shall:

i. Establish process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.
ii. Ensure that administrators shall only log into systems with user ids attributable to them or follow processes that would not break attribution.
iii. Ensure that Access to databases containing Subscriber Data, Personal Data, PII or SCI shall always be authenticated.
iv. All logins to the Subscription shall be secured through an encrypted connection (e.g., HTTPS) and appropriately authenticated.
v. Ensure that the Principle of Least Privilege using role-based access control (RBAC) is followed for all users.
vi. Control addition, deletion, and modification of usernames, credentials, and other identifier objects.
vii. Users (including temps, consultants, and contractors) shall formally request access to systems with only the rights necessary to perform their job functions.

viii. A manager or above and the system owner shall formally approve user roles and access requests. System administrators shall act as the final gatekeeper to ensure access is granted appropriate to the identified role.

ix. Performance of periodic review of users' access and access rights shall be conducted to ensure that they are appropriate for the users' role.

x. Two-factor authentication (TFA) or multi-factor authentication (MFA) shall be used for any services remotely accessible by personnel and/or authorized third parties

b. Intrusion detection and performance assurance: iCIMS shall monitor production networks, systems, and applications that store or process Subscriber Data for unauthorized access using traffic and activity-based monitoring systems.

c. See Section 9 of this Security Addendum for additional measures**.**

6. Measures for the protection of data during transmission

a. Encryption: As specified in Section 1 above.

7. Measures for the protection of data during storage

a. Encryption: As specified in Section 1 above.

b. Data segregation: iCIMS shall keep Subscriber Data at a minimum logically segregated from data belonging to iCIMS' other Subscribers and shall implement measures and controls designed to ensure that Subscriber Data is not accessible by iCIMS' other subscribers.

8. Measures for ensuring physical security of locations at which Subscriber Data are processed

a. Data center security: iCIMS uses data centers operated by third parties, for example Amazon Web Services, to provide the Subscription and, requires such third parties to maintain controls that provide reasonable assurance that access to physical servers at the data center is limited to authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

i. Logging and monitoring of all authorized and unauthorized access attempts to the data center by the data center security personnel.

ii. Camera surveillance systems at critical internal and external entry points to the data center.

iii. Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and

iv. Uninterruptible Power Supply (UPS) modules and backup generators, including fuel delivery services that provide back-up power in the event of a power failure.

v. Consideration taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster.

vi. Visitors shall always be accompanied by iCIMS Personnel.

vii. Requirement that data centers perform SOC 2 or equivalent audits on an annual basis while remediating any findings in a reasonable timeframe.

9. Measures for ensuring events logging

a. Auditing, logging, and monitoring controls: iCIMS shall implement and maintain measures designed to secure, control, and monitor iCIMS' networks, systems, and applications that process or store Subscriber Data, including:

i. Firewalls and related technology and authentication controls.

ii. Intrusion detection or prevention systems to monitor associated networks
iii. A centralized logging system controlled by iCIMS information security team, with log retention of one year.
iv. Secure, protected audit trails that cannot be modified.
v. Monitoring and alerting systems used to record login attempts/failures, successful logins and changes made to systems with associated alerting in place.
vi. Monitoring of all external ingress/egress connections.
vii. Security information and event management (SIEM) systems.
viii. Anti-virus/anti-malware

10. Measures for ensuring system configuration, including default configuration

a. Change and Configuration Management: iCIMS maintains policies and procedures for managing changes to iCIMS' production systems, applications, and databases which process Subscriber Data. Such policies and procedures include:
i. Processes for documenting, testing, and approving the promotion of changes into production.
ii. A security patching process that requires patching systems in a timely manner based on a risk analysis; and
iii. A process for iCIMS to perform security assessments of changes into production.
iv. Hardening standards based on industry best practice (e.g., CIS standards)
v. A vulnerability management program to audit and verify appropriate configuration (See Section 4.b).
vi. Mobile device management policies and processes to ensure devices shall comply to acceptable use and information security policies if used to access Subscriber Data.

11. Measures for internal IT and IT security governance and management

a. Governance: iCIMS shall designate one or more employees to maintain iCIMS' information security program.
i. iCIMS' senior leadership shall review and approve any material changes to the information security program.
ii. iCIMS shall review the information security program at least once per calendar year or upon a material change in iCIMS' business practices.

b. Information security measures: As specified in the "Data Security" section of iCIMS' Support & Maintenance Policy.

c. Modifications: iCIMS may modify its security controls and processes from time to time, so long as such modifications:
i. Do not materially reduce the overall level of protection afforded by iCIMS the Subscriber.
ii. Where applicable re consistent with iCIMS' then current SOC-2 statement.
iii. Remain compliant with the ISO 27001 and ISO 27701 standards.

12. Measures for certification/assurance of processes and products

a. Security certifications, audits, and attestations: iCIMS shall maintain the following industry standard certifications, audits, and attestations:
i. ISO 27001 certification, or equivalent, ensuring that iCIMS information security management system (ISMS) continues to perform in alignment with the standard.
ii. ISO 27701 certification, or equivalent, ensuring that iCIMS privacy information management system (PIMS) continues to perform in alignment with the standard.
iii. SOC 2, Type II attestation, ensuring that internal controls provided by iCIMS meet American Institute of Certified Public Accountants (AICPA) standards (i.e., SSAE-19, TPS-100).

iv. Penetration testing attestations regarding the performance, findings, and remediation resulting from internal and external penetration tests.

13. Measures for ensuring data minimization

a. Measures for ensuring data minimization: Subscribers control the nature and scope of the Subscriber Data that is transferred to iCIMS via the Subscription. The subject matter, duration, nature, purpose of the Processing of the Subscriber Personal Data, as well as the types of Subscriber Personal Data and categories of Data Subjects are set out in the Subscription Agreement and the Data Processing Addendum. Access to Subscriber Personal Data is strictly limited to those individuals who need to know / access the relevant Subscriber Personal Data, as strictly necessary for the purposes of the Subscription Agreement and to comply with Data Protection & Privacy Laws. Subscriber Personal Data is retained in accordance with any retention periods configured by Subscriber via the Subscription, or if such retention periods are not configured, in accordance with the Subscription Agreement. Where applicable (such as data analytics), the level of detail used for the Processing of Subscriber Personal Data is limited as described in Section 1.e of this Security Addendum.

14. Measures for ensuring data quality

a. Measures for ensuring data quality: The requirements for the conditions, scenarios, and responsibilities for processing Subscriber Data are specified in the Data Processing Addendum and the "Subscriber Data" section of the Subscription Agreement. The process for the exercise of data subject rights is specified in the Data Processing Addendum.

15. Measures for ensuring limited data retention

a. Deletion after termination or expiration of the Subscription: As specified in the Data Processing Addendum and Subscription Agreement.

b. Data destruction: Media containing Personal Data shall be disposed of so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting.

i. Subscriber Data in iCIMS' possession or under its control shall be deleted using techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization"), where possible.

ii. iCIMS shall certify the destruction of Subscriber Data by issuing a certificate of destruction, upon Subscriber's written request.

iii. Certificates of destruction shall be maintained for at least one year.

c. Retrieval of Subscriber Data: As specified in the Data Processing Addendum and Subscription Agreement.

16. Measures for ensuring accountability

a. Governance: iCIMS shall designate one or more employees to maintain iCIMS' privacy program.

i. iCIMS' senior leadership shall review and approve any material changes to the privacy program.

ii. iCIMS shall review the privacy program at least once per calendar year or upon a material change in iCIMS' business practices and/or Data Protection & Privacy Laws.

b. Liability for acts, errors, and omissions of sub-processors: As specified in the Data Processing Addendum and the Subscription Agreement.

c. Disciplinary policy: iCIMS shall maintain and enforce a disciplinary policy for violations of iCIMS' information security and privacy programs by iCIMS Personnel.

17. Measures for allowing data portability and ensuring erasure

a. Storage on portable devices: iCIMS shall not store any Subscriber Data on portable devices or removable media, including laptops, smartphones, and tablets, without Subscriber's prior written approval.

b. Data subject rights of erasure and portability: The process for the exercise of data subject rights is specified in the Data Processing Addendum.

18. Applied restrictions or safeguards for sensitive data (if applicable)

a. To provide data confidentiality in the event of accidental or malicious data loss, all Personal Data, PII, SCI or Subscriber Data shall be encrypted at rest and in transit (See Section 1).