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 (including Subscriber Personal Data) and Personal Data processed for iCIMS Business Operations (collectively, "**Protected Data**") that are processed pursuant to or in connection with the Subscription Agreement and Data Processing Addendum, 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, ISO 27701, & SOC2 standards. The following identifies key controls used to protect Protected 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 anonymization/pseudonymization and encryption of Protected Data

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

a. Protected Data at rest: Shall use at least the AES 256-bit or stronger for encryption. Data at rest includes Backups, as defined in iCIMS' Support & Maintenance Policy.

b. Protected Data in transit: Shall use TLS 1.2 or better for encryption.

c. Hashed data: Hashed data shall use bcrypt or stronger (as aligned to industry standards, including File Intrusion Prevention Systems (FIPS) approved and/or NIST recommended algorithms).

d. Key exchange and digital signatures:

i. Key exchange shall use RSA, DH, or stronger cryptographic algorithms with a minimum key length of 2048 bits.

ii. Digital signatures shall use specifications defined in the DSS with a minimum key length of 2048 bits and minimum digest length of 256.

e. Anonymization and pseudonymization: iCIMS has an internal data analytics policy that requires iCIMS to use some or all of the following safeguards and techniques to render Subscriber Personal Data anonymous, de-identified, and/or non-personal, as applicable:

i. Suppression - removes the identifying values from a record (e.g., removing the first and last name from a record).

ii. Generalization - replaces a data element with a more general element (e.g., 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 (e.g., 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 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, National Insurance number, Personal Public Service number, or other national identification number.

      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 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: During onboarding and at least once per calendar year thereafter, iCIMS shall require all iCIMS personnel with access to Protected Data to complete training on iCIMS' information security and privacy policies.

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 response policy and process to be followed in the event of any security or privacy incident, including any Personal Data Breach. iCIMS' incident response policy and process includes:

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

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

         1. Preparation: Establish an incident response capability aimed at preventing incidents by ensuring effective control frameworks and compliance.

         2. Detection & Analysis: Identify security or privacy event(s) and determine potential impact to iCIMS and subscribers.

            After consulting with iCIMS leadership and when warranted or required by judicial action, applicable law, regulation, or like jurisdictional requirement, iCIMS shall use reasonable efforts to provide notice to applicable iCIMS personnel and/or affected subscribers about a security or privacy incident. Additionally, notification is required within 24 hours of identification of a confirmed Personal Data Breach or Abnormal Activities. "**Abnormal Activities**" means unsuccessful attacks that appear particularly significant based on iCIMS' understanding of the risks it faces.

3. Containment Eradication & Recovery: Mitigate the root cause of the security or privacy incident to prevent further damage or exposure. Remove vulnerabilities causing the security or privacy incident, and any associated compromises. Restore the affected system(s) to operation after the issues that gave rise to the security or privacy incident, and the consequences of the security or privacy incident, have been corrected.
4. Post-incident Activities: Address notification and communication requirements, cooperate with external parties, information sharing, follow-up lessons learned, record keeping, and improvements.

b. Disaster recovery and business continuity: 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. Access controls:
   i. iCIMS shall:
      1. Follow the principles of least privilege through a role-based access control model when granting iCIMS personnel access to Protected Data.
      2. Limit access to Protected Data to iCIMS personnel with a legitimate need to access Protected Data to provide the services in accordance with the Subscription Agreement.
      3. Periodically (no less than quarterly) review iCIMS personnel's access to Protected Data.
      4. Promptly terminate an iCIMS personnel's access to Protected Data if such individual's access is no longer required.
      5. Review and disable user accounts after 90 days of inactivity.

b. Network controls: Access to internal and external network services that contain Protected Data shall be controlled through a combination of the following types of controls:
   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. Vulnerability management and patch management: 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 Protected Data. The program shall include:
   i. Penetration tests, conducted by an accredited third party selected by iCIMS, of iCIMS products and infrastructure that contain Protected Data occur 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.
   ii. Routine vulnerability scans on all iCIMS products and infrastructure that contain Protected Data or that are used by iCIMS to gain access to Protected 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 a critical and or security patch release.
4. Zero-day patches shall be applied on all systems containing Protected 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 iCIMS 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 agile teams are performing testing 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 source code vulnerability scanning in the CI/CD pipeline and conduct risk appropriate remediation activities based on business impact and subsequent prioritization of the findings prior to software release as appropriate to the priority.
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. Conducting awareness training regarding secure coding at least once per calendar year.

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

f. Security and privacy assessments: Upon written request of Subscriber no more than once in any twelve (12) month period, the Subscriber may reassess iCIMS' information security and privacy program. iCIMS agrees to provide reasonable cooperation with respect to any such assessment by providing reasonable and appropriate documentation; provided, however, responses to assessment requests may take up to forty-five (45) days for iCIMS to complete. Assessments described in this Section: (i) should not be considered an audit, and as such, iCIMS may not provide information that is customarily provided in an audit; and (ii) do not include and shall not permit Subscriber to conduct vulnerability/penetration tests.

g. Security certification and attestation: See Section 12 of this Security Addendum.

5. Measures of user identification and authorization

a. Access control: iCIMS personnel 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 Protected Data shall always be authenticated.
iv. Ensure all logins to the Subscription are 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. "**Principal of Least Privilege**" means restricting access to systems and data based on job role or function while ensuring that no additional, unneeded access is granted.
vi. Control addition, deletion, and modification of usernames, credentials, and other identifier objects.
vii. Ensure users (including temps, consultants, and contractors) formally request access to systems with only the rights necessary to perform their job functions.
viii. Ensure that a manager or above and the system owner 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. Conduct periodic review of users' access and access rights to ensure that they are appropriate for the users' role.
x. Use two-factor authentication (TFA) or multi-factor authentication (MFA) for any services remotely accessible by iCIMS personnel and/or authorized third parties

b. Intrusion detection and performance assurance: iCIMS shall monitor production networks, systems, and applications that store or process Protected Data for unauthorized access using traffic and activity-based monitoring systems.
c. Passwords: iCIMS will manage passwords in alignment with NIST 800-63b standards, for iCIMS managed digital identity at iCIMS.
d. See Section 9.a.v of this Security Addendum for alerting and monitoring.

6. Measures for the protection of Protected Data during transmission

a. Encryption: As specified in Section 1 of this Security Addendum.

7. Measures for the protection of data during storage

a. Encryption: As specified in Section 1 of this Security Addendum.
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 Protected 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.
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. All on-site visitors (to iCIMS site locations) 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 Protected 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 (including security information and event management (SIEM)) 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. Anti-virus/anti-malware protection for iCIMS managed assets.

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 Protected 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.
iii. A process for iCIMS to perform security assessments of changes into production.
iv. Hardening standards based on industry best practice (e.g., Center for Internet Security standards)
v. A vulnerability management program to audit and verify appropriate configuration (See Section 4.b of this Security Addendum).
vi. Mobile device management policies and processes to ensure devices shall comply with iCIMS internal acceptable use policy, employee handbook, and information security policies if used to access Protected 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 to Subscriber.
ii. Where applicable, are consistent with iCIMS' then current SOC-2 statement.
iii. Where applicable, 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, for the processing of Subscriber Data.
   ii. ISO 27701 certification, or equivalent, ensuring that iCIMS privacy information management system (PIMS) continues to perform in alignment with the standard, for the processing of Subscriber Data.
   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), for the processing of Subscriber Data.
   iv. Penetration testing attestations regarding the performance, findings, and remediation resulting from internal and external penetration tests.

13. Measures for ensuring data minimization

a. Subscriber Data: 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. iCIMS' 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.
b. Personal Data Processed for iCIMS Business Operations**:** Personal Data processed for iCIMS Business Operations is limited to the context of data generated to assist in iCIMS Business Operations incident to administration and delivery of the Subscription. iCIMS' access to Personal Data processed for iCIMS Business Operations is limited to those individuals and teams who need to know / access the relevant data, as necessary for iCIMS' legitimate business operations incident to administration and delivery of the Subscription to Subscriber, and for its other legitimate purposes relating to iCIMS' business operations. iCIMS will only process such Personal Data for the purposes that are compatible with those contained in the definition of iCIMS Business Operations and not use the Personal Data for any other purpose. Personal Data processed for iCIMS Business Operations is retained in accordance with iCIMS' documented data storage and retention policies and procedures.

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: Unless specified otherwise in the Data Processing Addendum or Subscription Agreement, Subscriber Data in iCIMS' possession or under its control shall be deleted within thirty (30) days after termination or expiration of the Subscription and, with respect to Backups, no more than twelve (12) months after the month in which the Subscription Agreement terminates or expires.

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

d. Vendor Audit: iCIMS maintains a review process for vendors that process Protected Data.

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 Protected Data that includes sensitive data shall be encrypted at rest and in transit (See Section 1 of this Security Addendum).