SECURITY ADDENDUM

This Trintech Security Addendum ("**Addendum**") is made a part of the Subscription Services Agreement (the "**Agreement**") between Trintech and Subscriber found at https://www.trintech.com/terms-and-conditions/cadency/. All capitalized terms used but not defined herein will have the meanings assigned to them in the Agreement. This Addendum may be updated from time to time by Trintech in its sole discretion provided that such updates will not materially reduce the security of the Services provided to Subscriber by Trintech.

1. STANDARD TRINTECH SECURITY & AUDIT REQUIREMENTS

1.1 Certification and Compliance Standards. Trintech is subject to the following certifications and compliance standards as provided in the table below:

Standard	Activities	Evidence
SOC 1 & SOC 2 Audited	Ongoing annual third-party audits to maintain SSAE 18 (or then current standard as evolved by AICPA) SOC 1 (Type II) and SOC 2 (Type II) attestations and reports.	Reports and bridge letters are available upon written request to Trintech Support.
ISO 27001 (Cadency Only)	Ongoing annual third-party audits to maintain ISO 27001 compliance for Cadency Services only.	Upon request, Trintech will provide Subscriber with the ISO 27001 certification and the Statement of Applicability.
HIPAA Compliant	Ongoing annual third-party audits to maintain HIPAA compliance.	Confirmation is available upon request to Trintech Support. Ability to execute Business Associate Agreements (BAAs) with covered entities.

1.2 Audit Reports. Trintech will provide SOC 1 and SOC 2 reports to Subscriber upon request to Trintech Support provided that any request will be limited to the most recent applicable audit and will be requested no more than once in a rolling twelve (12) month period, except in the case of a security breach with the potential to expose Subscriber's Data.

1.3 Security Breach Notification. Trintech will notify Subscriber within 48 hours of becoming aware of a security breach with the potential to expose Subscriber Data (**"Security Breach Notification"**). As such information becomes available and without undue delay, Trintech will provide Subscriber with relevant root cause detail, forensics, and logs upon removal of information that may identify other Subscribers.

1.4 Audit Rights. To assist Subscriber with security questionnaires, audits, or compliance activities, Trintech will permit an onsite audit at Trintech's Addison, Texas corporate headquarters upon written request to Trintech Support. During the audit, Subscriber's authorized employees, auditors and agents will be permitted to view but not copy or retain the complete table of contents of confidential and proprietary documents relevant to audited operating controls and security policies subject to a non-disclosure agreement. In the absence of a security breach, audits may be requested no more than once per rolling twelve (12) month period and require at least thirty (30) days' prior written notice to Trintech for scheduling. Additional audits may be requested following any Security Breach Notification. Questionnaires, security reviews, and other information or documentation requested by Subscriber may only be provided as part of a formal audit. Trintech will have no obligation to respond to such requests and any information or documentation provided outside of the Subscriber's annual audit right will be at Trintech's sole discretion.

2. CLOUD DATA CENTER SECURITY & AUDIT REQUIREMENTS

2.2 Certification and Compliance Standards. The Subscription Services are delivered from a data center operated by a third-party hosting provider ("**Hosting Provider**") that maintains the following certifications and compliance standards:

Standard	Activities	Evidence
SOC 1 & SOC 2 Audited	Ongoing annual third-party audits to maintain SSAE 18 (or then current standard as evolved by AICPA) SOC 1 (Type 2) and SOC 2 (Type 2) attestations and reports.	SOC 1 and SOC 2 reports and bridge letters are available upon request to Trintech Support.
HIPAA Compliant	Ongoing annual third-party audits to maintain HIPAA compliance.	Confirmation is available upon request to Trintech Support. Ability to execute Business Associate Agreements (BAAs) with covered entities.

2.3 Audit Reports. SOC 1 and SOC 2 reports of Trintech's Hosting Provider will be provided to Subscriber upon request to Trintech; provided that any request will be limited to the most recent, applicable audit, capable of being secured by Trintech within a commercially reasonable amount of time from the Hosting Provider, and will be requested no more than once in a twelve (12) month

calendar period, except in the case of a security breach with the potential to expose Subscriber's Data, or if Trintech is notified of such a breach by the Hosting Provider.

2.4 Data Center Location. Unless requested by Subscriber (e.g., through a Support escalation) in writing, Trintech will not migrate, transfer, or otherwise move Subscriber Data to a data center of Hosting Provider located in a different country from the original data center in which the applicable production environment is established (**"Data Center Location"**). If Trintech initiates a change to the Data Center Location, it will notify Subscriber promptly, without undue delay, provided that Trintech may initiate a change in Data Center Location, without notice, if: (i) Trintech deems such move reasonably necessary to prevent, mitigate, or remedy, a critical security vulnerability; or (ii) in the event of a disaster recovery event.

2.5 Subscriber Data Center Access. Subscriber will not be permitted access to Hosting Provider locations at any time during the term of the Agreement, including Subscriber's auditors, agents, service providers, or other representatives.

3. ENCRYPTION OF SUBSCRIBER DATA

3.1 Trintech will provide Subscriber with an industry standard level of encryption for Subscriber Data both in transit and at rest (**"Encryption"**). Encryption at rest encompasses all Subscriber Data (disk, tape, and offsite) at the primary site, secondary site (i.e., maintained for BC/DR), and any offsite locations used by the hosting provider for vaulting of backup media. The standard level of encryption that Subscriber receives, pursuant to the applicable Order is:

Data in Transit	Encryption of all Subscriber data in transit using industry standard secure protocols (e.g., HTTPS, SFTP, etc.).
Data at Rest	Encryption of all Subscriber data at rest (disk, tape, and offsite) including database data, reporting data, file attachments, and integrations using industry standard encryption (e.g., public/private key, AES 256).
Dedicated Keys	Client-specific public/private keys, symmetric keys, and integrations (e.g., GPG/PGP).
Key Rotation	Premium option to support online rotation of keys on schedule defined by Subscriber.

3.2 Premium Encryption. If indicated in the applicable Order, the level of Encryption may be upgraded by Subscriber to a premium plan that includes online rotation of encryption keys on a schedule defined by Subscriber for additional security.

4. BUSINESS CONTINUITY AND DISASTER RECOVER ("BC/DR")

4.1 Trintech provides comprehensive BC/DR for Subscriber production environments to ensure that Subscription Services remain available in the event of a non-Force Majeure disaster with the potential to impact Subscription Services.

RPOs: 1 hour	In the event of a disaster, all production data will be current to within one (1) hour.
RTOs: 4 hours	In the event of a disaster, all production services will be available from the secondary site within four (4) hours.
Backup Strategy	Daily differential/incremental and weekly full backups are performed for all production systems. Hourly transaction log and daily full database backups are performed for all production databases.
Annual Testing	Annual third-party audits including full BC/DR testing to validate RPOs, RTOs, and backup strategy.

4.2 Backup Recovery Testing. To ensure the integrity of Subscriber Data and the availability of the Subscription Services, Trintech's audited operating controls include annual BC/DR testing to validate Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and Backup Strategy. Full BC/DR plans are confidential and proprietary and may be viewed subject to audit requirements contained within **Section 1**. Subscribers will not schedule or participate in Trintech's BC/DR testing.

4.3 Backup Retention and Termination. Trintech retains backups of Subscriber Data for up to twenty-eight (28) days to ensure that BC/DR requirements are met. Trintech will remove Subscriber Data, inclusive of third-party Hosting Provider managed backups, and all encryption keys within thirty (30) days of receipt of written request and/or notice of termination. Upon request from Subscriber, Trintech Support can provide confirmation that Subscriber encryption keys and Subscriber Data have been removed.

4.4 Test Environments. The requirements contained within this **Section 4** are applicable to Subscriber production environments only, and not applicable to Subscriber's test environment unless otherwise described in the applicable Order.

5. SECURE CODING GUIDELINES & MALWARE DETECTION

5.1 Trintech follows industry standard secure coding guidelines and takes appropriate measures to protect the Subscription Services against unauthorized modifications to the Subscription Services or the Subscriber Data without the consent of Subscriber or Trintech.

- Prior to release, both Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) is conducted to identify potential vulnerabilities in the Trintech Software.
- Access to systems is controlled by an industry standard authentication method leveraging strong authentication and a unique User ID and strong password.
- Remote access (if applicable) is secured through multi-factor authentication.
- Passwords are required to be changed on a periodic basis
- Passwords may never be stored in clear text.
- Secure Coding Guidelines, aligning to Microsoft SDL and OWASP

5.2 Application Security Training. Trintech provides its software development team with industry leading application security training on secure development and other protocols.

5.3 Malware Detection. Trintech uses commercially reasonable, and industry standard malware detection measures to prevent the distribution of malware upon implementation or delivery of Subscription Services. Subscriber is expected to maintain a secure internal network for its own purposes outside the Subscription Services. malware, harmful code, or other invasive or unauthorized programs are not sanctioned by Trintech (**"Malware"**). Trintech will not be liable to Subscriber or any third-party if harm is caused by the failure of Subscriber's internal network to detect Malware originating from Third-Party Products, Subscriber's internal network, or not otherwise within the reasonable control of Trintech.

6. GENERAL USER TERMS

6.1 Definition of Terms. Any industry standard non-defined terms in this **Section 6**, will default to those in the NIST glossary of standard information security terms, available at https://csrc.nist.gov/glossary.

6.2 User Misuse & Credentials. The Parties agree that Trintech does not provide onsite credentials management for Subscriber, and that Subscriber, it's Users, or holders and handlers of credentials are collectively responsible for the damage or harm caused by: (i) the use or distribution of User credentials or (ii) the misuse of Services. Subscriber agrees and understands that completion of annual security awareness training is necessary to prevent the harmful, unlawful, or improper release of User credentials by Subscriber Users, and any harms caused by improper release of Subscriber credentials or access to the Services will be the sole responsibility of Subscriber.

6.3 Authentication & Credentials Management. The Parties agree that, during the term of any Services, Subscriber will maintain up-to-date credentials management practices and safeguards that meet single-factor authentication. If Subscriber chooses to use single-factor authentication for the Services, Subscriber understands and agrees to the risks associated with the lack of multi-factor authentication The Parties agree to reference NIST SP800-63B (**"Authentication Definitions"**) for definitions, and that any Trintech Software under the applicable Order may use AAL1 (as defined in the Authentication Definitions) unless noted otherwise.

6.4 Memorized Secret (i.e. Password, PIN, etc.). Subscribers will ensure that passwords and password policies meet or exceed current NIST password guidance which recommends the following:

- An eight-character minimum and 64-character maximum length
- The ability to use all special characters but no special requirement to use them
- Restrict sequential and repetitive characters (e.g. 12345 or aaaaaa)
- Restrict context specific passwords (e.g. the name of the site, etc.)
- Restrict commonly used passwords (e.g. p@ssw0rd, etc.)
- Passwords obtained from previous breach corpuses.

END OF DOCUMENT