SECURITY ADDENDUM

This Security Addendum contains the information security, and third-party audited controls that apply to the Adra Services and forms part of the Adra Service Agreement ("Agreement"). Any capitalized terms not defined in this Security Addendum are found in the Agreement. If an industry-standard term is used in this Security Documentation, but not defined here or in the Agreement, it will default to those definitions in the National Institute of Standards and Technology ("NIST") glossary of standard information security terms, available at https://csrc.nist.gov/glossary.

STANDARD TRINTECH SECURITY & AUDIT REQUIREMENTS

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.
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.

Trintech will provide SOC 1 and SOC 2 reports to Subscriber upon request to Trintech Support. Subscriber agrees 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.

Trintech will notify Subscriber within seventy-two (72) 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.

To assist Subscriber with security questionnaires, audits, and/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/or 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.

CLOUD DATA CENTER SECURITY & AUDIT REQUIREMENTS

The Subscription Services are delivered from a data center operated by a third-party hosting provider ("**Hosting Provider**"). Information regarding the Hosting Provider can be found at https://www.microsoft.com/en-us/trustcenter/Compliance/soc.

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"**) without Subscriber's prior consent. If Trintech initiates a change to the Data Center Location, it will notify Subscriber promptly, without undue delay, and Subscriber will have the one-time right to terminate the Agreement within 30 days from receipt of such notice from Trintech; 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; *provided further that* Subscriber may not terminate if the purpose of 2.4 (i) or (ii) above was initiated to protect Subscriber's Data, and Trintech returns Subscriber Data to the original Data Center Location within a reasonable time.

ENCRYPTION OF SUBSCRIBER DATA

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, SSL, TLS (1.2 or greater), 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, FIPS 140-2 Level 2.

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY ("BCP/DR")

Trintech provides comprehensive BCP/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.

RPO: 4 hours	In the event of a disaster, all production data will be current to within 4 hours.
RTO: 12 hours	In the event of a disaster, all production services will be available from the secondary site within 12 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.

Full BCP/DR plans are confidential and proprietary and may be viewed subject to audit requirements contained within this Security Documentation. Subscribers will not schedule or participate in Trintech's BCP/DR testing.

Trintech retains backups of Subscriber Data for up to 30 days to ensure that BCP/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.

The requirements contained within this Security Documentation are applicable to Subscriber production environments only, and not applicable to Subscriber's test environment unless otherwise described in the applicable Order.

SECURE CODING GUIDELINES & MALWARE DETECTION

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 may never be stored in clear text.
- Secure Coding Guidelines, aligning to Microsoft SDL and OWASP

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, and, 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 software, or Subscriber's internal network not within the reasonable control of Trintech.

GENERAL USER TERMS

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.

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.

Subscribers will ensure that passwords are aligned with 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