Information Security Addendum

This Information Security Addendum ("**Addendum**") forms part of the agreement that references and incorporates this Addendum ("Agreement") entered into between the Convergint entity ("Convergint") and the customer specified in the Agreement ("Customer"). Notwithstanding any terms contained in the Agreement to the contrary, in the event of a conflict between the terms of the Agreement and the terms of this Addendum, the terms of this Addendum shall supersede and prevail.

Scope and Applicability: This document summarizes Convergint's information security controls and practices designed to protect the confidentiality, integrity, and availability of Customer's Confidential Information. Convergint is not the manufacturer or developer ("OEM") of certain products ("Third Party Products") delivered or serviced by Convergint, and such OEMs are not Convergint subprocessors. Accordingly, Convergint does not control and is not responsible for the information security of Third Party Products, except to the extent of processing performed directly by Convergint or its subcontractors. Customer remains responsible for maintaining the security of its own systems and environments, including those that interact with or are accessed by Convergint in connection with the services.

"**Customer Information**" means non-public data or information provided by or on behalf of Customer in connection with Convergint's services, including business, operations, financial, personally identifiable, and other proprietary or sensitive information. Convergint maintains an Information Security Program ("**Program**") designed to protect the confidentiality, integrity, availability, and security of Customer Information that includes the following measures.

Category	Details
Policies & Governance	Convergint maintains written information security policies and procedures designed to protect Customer Information from unauthorized access, use, disclosure, alteration, or destruction. These policies are reviewed and updated annually to address evolving security risks. Convergint maintains a dedicated information security team responsible for overseeing security governance, policy enforcement, risk management, and incident response across its operations, and this team reports regularly to executive leadership on information security risks, controls, and program effectiveness.
Standards for Information Security	Convergint's Program is defined with reference to recognized industry standards, frameworks, and practices.
Security Training & Awareness	Convergint provides information security training to its personnel at the time of hiring and annually thereafter. In addition, Convergint delivers ongoing security awareness through ad hoc and role-based training, including periodic phishing simulations, reminders, and other on-the-job reinforcement.
User Identification and Authorization	Convergint utilizes recognized, centralized identity and access management solutions to manage user authentication and access to systems that process Customer Information. Multi-Factor Authentication (MFA) is required for employee access to such systems. Convergint adheres to NIST 800-63B and 800-171 guidelines for employee password security, including passwords that are at least 12 characters in length. Convergint maintains restrictions on account access after repeated unsuccessful login attempts. Convergint conducts periodic reviews of user logs to detect unauthorized access and promptly revokes system access upon colleague termination.
Network Security	Convergint utilizes real-time malware detection, managed detection and response (MDR) for suspicious activity alerts, network segmentation, and firewalls for intrusion detection and prevention. Additionally, Convergint centrally

Category	Details
	tracks and analyzes security analytics to identify risks using a security information and event management system (SIEM), and has DDoS protection on its public web servers. Critical security threats are relayed to Convergint's network security team immediately for disposition. Log data is retained for 12 months.
Storage and Transmission Security	Convergint employs encryption both for data at rest and data in motion. Convergint utilizes Azure platform-managed keys to protect and control access to encryption keys.
Least Privilege	Access to Customer Information is limited to colleagues necessary for Convergint to perform under the Agreement. Customer Information is logically separated from information of other customers.
Erasure	Convergint follows secure erasure and destruction procedures for electronic media and paper shredding measures in accordance with industry standards.
Testing and Evaluating Security Measures	Convergint performs periodic internal and external vulnerability assessments, application penetration tests, and annual external application and network penetration tests.
Event Logging and Monitoring	Convergint maintains network, application, and endpoint logs for 1 year. Convergint engages in real-time monitoring using automated tools, with any potential incidents escalated by the tools for review by Convergint's network security team.
Vulnerability Patching	Convergint maintains a vulnerability management program designed to identify, assess, and remediate security vulnerabilities in systems that process or store Customer Information. Convergint monitors industry-recognized sources (such as the NIST National Vulnerability Database and vendor advisories) to stay informed of newly disclosed vulnerabilities and available patches. Patches and remediation measures are implemented based on a risk-based prioritization process that considers the severity of the vulnerability and potential impact. For user endpoints, patches for Critical vulnerabilities are generally implemented within 7 days, and patches for High vulnerabilities are implemented within 30 days.
Endpoint Security	Convergint implements a layered endpoint security program across all end-user devices. Endpoints are protected with anti-virus and anti-malware software with real-time detection and automatic updates based on global threat intelligence. Convergint personal computers are full disk encrypted, password/PIN protected, and configured for automatic security patching. Devices are uniquely assigned to individual users, monitored for compliance with security policies, and restricted from running prohibited software.
Mobile Security	Convergint maintains a mobile device security program that applies to both company-managed and personally owned (BYOD) devices used to access Customer Information. Company devices are managed through mobile device management (MDM), while business applications on BYOD devices are governed via mobile application management (MAM). Convergint's MDM and MAM include remote data wipe capabilities. Customer Information stored on mobile devices is encrypted.

Category	Details
Physical Security of Processing Locations	Convergint secures physical access to its facilities through industry-standard, layered security approaches, such as badge scanning, alarm systems, and guest check-in procedures. Only authorized individuals such as employees and authorized external parties are permitted to access our facilities.
Incident Response	Convergint maintains incident response plans and procedures, conducts "tabletop" exercises annually, and regularly reports to executive leadership regarding information security posture and risk management efforts. Convergint has a dedicated Cyber Security team on call to handle critical system events. Convergint's documented Incident Response Plan identifies key stakeholders responsible for handling the response to a security incident should one occur. Convergint updates the plan to address newly identified risks or legal and regulatory requirements. Convergint's plan calls for timely customer notifications and coordination with various internal stakeholders and outside resources to manage and resolve security incidents.
Backups, Business Continuity, and Disaster Recovery	Convergint's business applications are backed up periodically. Convergint maintains a business continuity and disaster recovery policy with specified RPOs and RTOs, geo-zone redundancy, standard recovery capabilities, designated personnel, and recovery procedures for key applications.
Remote Access	If applicable based on the requested services, Convergint may access Customer's information systems. Convergint will access Customer systems consistent with Customer's communicated policies and procedures, but is not responsible for losses or harms caused by Customer's own systems, by following Customer's instructions, or by third party or Customer-specified remote access software.