C.H. Robinson Information Security Addendum

For the duration of the engagement and so long as the PROVIDER stores CH Robinson information, interacts with any CH Robinson data, networks or, carries any obligation to provide services or, support to CH Robinson, PROVIDER agrees to maintain and continuously improve upon a commercially reasonable information security program that at a minimum adheres to the following Security Requirements.

- This program should be based upon an industry recognized framework specifically addressing Information Security (in example: ISO, NIST, Cloud Security Alliance) and include comprehensive coverage, be formally managed and include industry standard security and availability controls.
- Areas of control including but, not limited to:
    - well-managed and updated antivirus across all compute and processing endpoints including automated, multiple daily signature updates and centralized administration
    - advanced host anti-malware capable of detecting advanced persistent threats and malicious software executing in memory
    - well-managed patch management and software update procedures ensuring comprehensive and timely deployments of software and operating system, firmware and 3rd party security patching across any connected devices and/or those hosting CH Robinson information (for example: all compute, storage and network equipment). Including accommodations for accelerated zero-day vulnerability patching and a 30 day remediation schedule for all critical and high findings
    - third party penetration testing of all PROVIDER internet-facing systems on at least an annual basis using independent testing professionals who are accredited. PROVIDER shall ensure that identified vulnerabilities are remediated promptly and per a documented schedule
    - role based and least privileged access including regular and comprehensive rights reviews
    - effective processes and controls covering administrative activities including regular reviews of elevated rights and accounts, reviews of administrative activity (log reviews) as well as secondary accounts for administrators to perform administrative duties
    - cyber security event/incident testing (malware/ransomware, DDOS, for example) should be conducted on a regular basis – at least annually – and include program improvement identification opportunities and implementations
    - management of a mature Secure Development Lifecycle program - where PROVIDER is developing software. At minimum the program should include threat modeling, vulnerability identification pre-deployment, procedures and SLA's to correct deployed software with identified vulnerabilities and processes to identify and remediate open source software vulnerabilities
    - source code should be secured and not include credential secrets or other information which, could create risk related to running PROVIDER software or utilizing PROVIDER services
    - code signing certificates must be secured at all times and procedures in place to ensure that they remain secured
    - established and documented configuration management policies and procedures ensuring that data, systems, networks, applications and any other items related to or, supporting the service(s) are protected from unauthorized disclosures or, use (for example, protections for data based on classification, limiting systems exposure to the internet, minimizing administrative access)
    - well-managed identity lifecycle management procedures including effective and timely account provisioning, role/access change and de-provisioning (access revocation at time of termination)
    - remote environment connectivity by PROVIDER users to PROVIDER's environment includes Multi Factor Authentication
    - identified and communicated responsibility and accountability for Information Security within PROVIDER and known to all employees
    - formalize Third Party Risk Management processes including pre-implementation assessments as well as ongoing either time based or, risk-based assessments of third

party risk. This should include 3rd party contractors, vendors (software, hardware, services, etc.) etc.

- established data lifecycle management processes covering the secure handling, storage and disposal of customer information and/or physical assets
- data at rest and in transit is encrypted and decryption keys are secured and access limited to a defined, least privileged group
- security events are analyzed for impact and risk and acted upon in a timely manner
- configuration change control and change management procedures are formalized. Including but not limited to: pre-deployment testing, rollback procedures, change approval and change related issue tracking
- employment agreements with enforcement mechanisms including employee obligations for protecting service availability and customer information
- security awareness training for all PROVIDER employees and contractors including phishing awareness, data classification and supporting processes and PROVIDER employee accountability (for example but not limited to, clear desk policies, proper disposal of media/information, etc.) including policy violation implications
- well-established processes to identify internal and external risk factors that may put CH Robinson information, contracted services or, any part of the relationship at risk to either unauthorized disclosure or, non-performance and, maintain procedures to manage and remediate the same risks
- formal continuity processes including Disaster Recovery (a tested disaster recovery program and N+1/concurrent maintainability coverage for all necessary systems and data within the scope of the service) and formal Business Continuity program addressing recovery of people and processes in case of incident
- demonstrable security program support and visibility across senior leadership (BOD/C-Suite/P/VP)
- immediately upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of CHR Data, PROVIDER will notify CHR then, expedite a full investigate the incident, and cooperate fully with the CHR's investigation of and response to the incident including sharing information and results coming from the PROVIDER investigation.

The above control coverage areas and processes will be part of an independent 3rd party assessment (SOC 2 Type 2 or, ISO/NIST accreditation assessment, as examples) with independent auditor reporting/assertions made available to CH Robinson by request at least annually.

The PROVIDER is responsible for all the consequences of non-compliance including non-compliance by any of its own vendors, employees, representatives, consultants, agents, and/or subcontractors (“Provider Personnel”). Should any non-performance, exception related to control, process performance detailed above, or across other security controls within PROVIDER’s Information Security program, be identified through PROVIDER’s internal risk identification and management processes or, 3rd party assessments PROVIDER agrees to notify CH Robinson within 48 hours. Additionally, PROVIDER and Provider Personnel are required to report suspected violations of the Security Requirements to the CHR business owner. Failure of PROVIDER to follow these Security Requirements will be considered a material breach of the Agreement.

These Security Requirements are subject to revisions by CHR from time to time as security requirements change, either by law or industry standard, or at CHR’s discretion.