NEXTHINK

INFORMATION SECURITY ADDENDUM

All capitalized terms not defined in this Information Security Addendum ("**ISA**") have the meaning given to them in other parts of the Agreement.

1. SECURITY PROGRAM

While providing the Services, Nexthink will maintain a written information security program of policies, procedures and controls aligned to ISO27001, or substantially equivalent standard, governing the processing, storage, transmission, and security of Customer Data (the "**Security Program**"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Nexthink updates the Security Program to address new and evolving security technologies, changesto industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

1.1 SECURITY PROGRAM REQUIREMENTS. The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Nexthink shall: (a) maintain, monitor, and enforce appropriate organizational, administrative, technical, and physical safeguards to protect the security, integrity, confidentiality, and availability of Customer Data and Nexthink information systems processing Customer Data ("**Nexthink Information Systems**"); and (b) protect against: (i) anticipated threats and hazards; and (ii) Security Incidents. The Security Program shall include, with respect to Customer Data and Nexthink Information Systems: (a) the security principles of segregation of duties and least privilege, including a process by which user accounts are only created with proper management approval, timely deleted, have an auditable history of changes, and have an annual review and removal of excess access authorization; (b) retention policies for all reports, logs, audit trails, and other documentation that provides evidence of data privacy, data security, systems, and audit processes and procedures; (c) policies documenting consequences for violations of the Security Program; (d) a risk-based patch and vulnerability management and penetration testing program that deploys appropriate patch and vulnerability management controls to all Nexthink Information Systems as necessary to comply with this ISA and applicable information security law and regulation under the Agreement ("**Applicable Law**"); (e) once Nexthink no longer needs Customer Data, including upon Agreement termination, providing written confirmation of secure disposal, and, at Customer's request, secure return, of all Customer Data (except if legally restricted, require Nexthink to retain Customer Data, in which case Nexthink may retain only the Customer Data required to be legally retained by Applicable Law, and the ISA survives the Agreement and continues to apply to the extent and for the duration of such retention); (f) a periodic risk assessment process (conducted at least annually) that reviews technology developments and evolving threats, including: (i) risks to the Nexthink's business operations; (ii) effectiveness of controls to protect Customer Data and Nexthink Information Systems; and (iii) how identified risks are mitigated; (g) a process to evaluate new and emerging security risks to modify and/or enhance the Security Program, including a review of cyber threat intelligence information; and (h) an appropriate Security Incident response plan and procedure for identifying, managing, and mitigating Security Incidents and for notifying customers and other appropriate parties. Nexthink updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

1.2 DATA LOSS PROGRAM. Nexthink shall maintain, monitor, and enforce a data loss prevention program that is designed to detect transfers of Customer Data, if such transfers do not comply with the Agreement or Applicable Law.

1.3 SECURITY ORGANIZATION. Nexthink shall designate a responsible information security officer (presently the Director of Information Security and Compliance) responsible for coordinating, managing, and monitoring Nexthink's information security function, policies, and procedures.

1.4 THIRD-PARTY VENDORS OR SUB PROCESSORS. Nexthink will evaluate all third-party vendors or sub processors to ensure that they maintain adequate physical, technical, organizational, and administrative controls, based on the risk tier appropriate to their services, that support Nexthink's compliance with the requirements of the Agreement and this ISA. All

third-party vendors or sub processors fall into scope for independent audit assessment as part of, or maintain an independent audit assessment which conforms to, Nexthink's ISO 27001 audit or an equivalent standard, where their roles and activities are reviewed per control requirements. Nexthink will remain responsible for the acts and omissions of its Subcontractors as they relate to the services performed under the Agreement as if it had performed the acts or omissions itself and any subcontracting will not reduce Nexthink's obligations to Customer under the Agreement.

1.5 POLICIES. Nexthink's information security policies shall be (i) documented; (ii) reviewed and approved by management, including after material changes to the Services; and (iii) published, and communicated to personnel, contractors, and third parties with access to Customer Data, including appropriate ramifications for non- compliance.

1.6 RISK MANAGEMENT. Nexthink shall perform information security risk assessments as part of a risk governance program that is established with the objective to regularly test, assess, and evaluate the effectiveness of the Security Program. Such assessment shall be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats. Nexthink shall have the risk program audited annually by an independent third-party in accordance with Section 2.1 (Certifications and Attestations) of this ISA.

2. INDEPENDENT CERTIFICATIONS AND AUDITS

2.1 INDEPENDENT CERTIFICATIONS AND ATTESTATIONS. Nexthink shall establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO 27001, ISO 27017, ISO 27018 (or equivalent standards) for the Security Program supporting the Services. At least once per calendar year, Nexthink shall obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer.

2.2 THIRD PARTY AUDITS. Nexthink shall allow for and contribute to audits that include inspections by granting Customer (through a third-party representative(s) credentialed in such reviews) access to all reasonable and industry recognized documentation evidencing Nexthink's policies and procedures governing the security and privacy of Customer Data and its Security Program, excluding any third party proprietary information or documentation expressly excluded from disclosure by such party or by Applicable Law ("**Audit**"); provided that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with Nexthink). The Audit disclosure will include documentation evidencing Nexthink's Security Program, as well as Nexthink's privacy policies and procedures regarding personal information processed within the Services, copies of certifications and attestation reports (including Audits) listed above. Without limiting the foregoing, the Audit shall demonstrate that the Company has and maintains a comprehensive Security Program, including by completing information security questionnaires and, if requested, providing: (a) all privacy, data processing, data protection, data security, encryption, and confidentiality related: (i) Company policies, procedures, and standards (including escalation procedures for non-compliance and training materials); (ii) available third party assessments, audits, and reviews, and other equivalent evaluations, and (iii) evidence that Scanning Assessments and Pen Tests were performed in accordance with Section 6.2; (b) to the extent permitted, individuals' requests under Applicable Law with respect to their Personal Data processed in connection with the Services provided hereunder; (c) the public Internet Protocol ranges associated with Nexthink Information Systems used in connection with the Services provided hereunder; and (d) relevant information and documentation to verify compliance with this ISA.

2.3 REGULATORY AUDITS. If Customer's governmental regulators require that Customer perform an on-site audit of Security Program, as supported by evidence provided by Customer, Customer may at Customer's expense, through a third-party independent, credentialed auditor, selected by Customer, conduct an on-site audit of the Security Program, to the extent required by Applicable Law ("Regulatory Audit"). Customer must submit any requests for an onsite Regulatory Audit to the Director of Information Security and Compliance. Nexthink may, at its discretion, charge Customer an audit fee at Nexthink's then-current rates.

2.4 TERMS OF AUDITS. Audits conducted pursuant to this ISA must: (i) be conducted during reasonable times and be of reasonable duration; (ii) not unreasonably interfere with Nexthink's day-to-day operations; and (iii) be conducted under mutually agreed upon terms and in accordance with Nexthink's security policies and procedures. Nexthink reserves the right to limit an Audit of configuration settings, sensors, monitors, network devices and equipment, files, or other items if Nexthink, in its reasonable discretion, determines that such an Audit may compromise the security of the Nexthink Security Program or the data of other Nexthink customers. Third party auditors must enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Nexthink's confidential

information.

2.5 OUTPUT. Upon completion of the Audit, Nexthink and Customer may schedule a mutually convenient time to discuss the output of the Audit. Nexthink may in its sole discretion, consistent with industry and Nexthink's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Nexthink's Security Program. The Audit and the results derived therefrom are deemed to be the Confidential Information of Customer and Nexthink, as applicable. Customer must promptly provide Nexthink with any Audit, security assessment, compliance assessment reports and associated findings prepared by it or its third-party contractors for comment and input prior to formalization and/or sharing such information with a third party. If any Audit performed pursuant to this ISA reveals or identifies any non-compliance by Nexthink of its obligations under the Agreement and this ISA, then (a) Nexthink will work to correct such issues; and (b) Customer may request feedback and information regarding corrective and remedial actions taken in relation to such audit for no more than sixty (60) days after the date upon which such audit was conducted.

3. PHYSICAL, TECHNICAL, AND ORGANIZATIONAL SECURITY MEASURES

3.1 PHYSICAL SECURITY MEASURES.

3.1.1. GENERAL. Nexthink will maintain appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that process Customer Data. Nexthink will utilize commercial grade security software and hardware to protect the Service.

3.1.2. FACILITY ACCESS. Nexthink will ensure that: (a) physical access to Nexthink's corporate facilities is tightly controlled; (b) all visitors to its corporate facilities sign in (or are notified to office management by their hosts for record-keeping), agree to confidentiality obligations relevant to their access, role and purpose of visit, and be escorted by Nexthink personnel while on premises at all times; and (c) on a real time basis Nexthink's security team is alerted to any physical breach of the facilities. Nexthink will revoke Personnel's physical access to Nexthink corporate facilities upon termination of employment.

3.1.3. DATA CENTER ACCESS. Nexthink will ensure that its commercial-grade data center service providers used in the provision of the Services maintain an on-site security operation that is responsible for all physical data center security functions and formal physical access procedures in accordance with SOC1 and SOC 2, or equivalent, standards. Nexthink's data centers are included in Nexthink's ISO 27001 or equivalent certification.

3.1.4. PROPRIETARY SYSTEMS, MACHINES AND DEVICES. Proprietary systems, machines and devices are further managed by way of (a) physical protection mechanisms; and (b) entry controls to limit physical access.

3.1.5. MEDIA. Nexthink shall use industry standard (or substantially equivalent) destruction of Customer Data, before such media leaves Nexthink's data centers for disposition. Upon request, Nexthink shall provide specifics as to the destruction measures applicable to any media used in connection with Customer Data.

3.2 TECHNICAL SECURITY MEASURES.

3.2.1. ACCESS ADMINISTRATION. Access to the Services by Nexthink employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Individuals are assigned a unique user account. Individual user accounts shall not be shared. Access privileges are based on job requirements using the principle of least privilege access and are revoked upon termination of employment or consulting relationships. Access entitlements are reviewed regularly and no less than annually in the Security Program examination process. Infrastructure access includes appropriate user account and authentication controls, which will include the required use of VPN connections, complex passwords account lock-out enabled, and a multi-factor authenticated connection.

3.2.2. SERVICE ACCESS CONTROL. The Services provides user and role-based access controls. Customer is responsible for configuring such access controls within its instance.

3.2.3. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected, are secured in an effort to prevent tampering, and are monitored for anomalies by a trained security team. Nexthink shall provide a logging capability in the platform that captures login and actions taken by users in the Nexthink application. Customer has full access to application audit logs within its instance(s), including successful and failed access attempts to Customer's instance(s). Customer is responsible for exporting application audit logs to Customer's syslog server through available built-in platform features.

3.2.4. FIREWALL SYSTEM. An industry-standard firewall is installed and managed to protect Nexthink systems

by residing on the network to inspect all ingress connections routed to the Nexthink environment. Nexthink managed firewall rules are reviewed quarterly. Customer shall be responsible for reviewing any Customer managed firewall rules on its instance(s).

3.2.5. VULNERABILITY MANAGEMENT. Nexthink regular to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed, Nexthink will determine the most effective and time-sensitive solutions for shorter-term and longer-term remediation impacts, which approaches may be required when vendor patches or other commercially available solutions are not immediately available. As appropriate to the situation, Nexthink will obtain the patch from the applicable vendor and apply it in accordance with Nexthink's then-current vulnerability management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

3.2.6. ANTIVIRUS. Nexthink updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

3.2.7. CHANGE CONTROL. Nexthink evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following Nexthink's standard operating procedure.

3.2.8. DATA SEPARATION. Customer Data shall be maintained within a cloud infrastructure that is logically and physically separate from Nexthink's corporate infrastructure.

3.2.9. CONFIGURATION MANAGEMENT. Nexthink shall implement and maintain standard hardened configurations for all system components within the Services. Nexthink shall use industry standard hardeningguides, such as guides from the Center for Internet Security, when developing standard hardening configurations.

3.2.10. DATA ENCRYPTION IN TRANSIT. Nexthink shall use industry standard encryption, and in compliance with Applicable Law, to encrypt Customer Data in transit over public networks to the Services.

3.2.11. DATA ENCRYPTION AT REST. Nexthink shall provide industry standard encryption, and in compliance with Applicable Law, at rest capability for Customer Data at the storage level.

3.2.12. SECURE SOFTWARE DEVELOPMENT. Nexthink shall implement and maintain secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent standard). All personnel responsible for secure application design and development will receive appropriate training regarding Nexthink's secure application development practices.

3.2.13. SECURE CODE REVIEW. Nexthink shall perform a combination of static and software-component testing of code prior to the release of such code to Customers. Vulnerabilities shall be addressed in accordance with its then current software vulnerability management program. Software patches are regularly made available to Customers to address known vulnerabilities.

3.2.14. ILLICIT CODE. The Services shall not contain viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of the Services; or (b) any interruption, interference with the operation of the Services (collectively, "**Illicit Code**"). If the Services is found to contain any Illicit Code that adversely affects the performance of the Services or causes a material security risk to Customer Data, Nexthink shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Illicit Code or to advise and assist Customer to remove such Illicit Code.

3.3 ORGANIZATIONAL SECURITY MEASURES.

3.3.1. DATA CENTER REVIEW. Nexthink performs routine reviews of data center measures to confirm that the data centers continue to maintain appropriate security controls necessary to comply with the Security Program.

3.3.2. PERSONNEL SECURITY. Nexthink performs or requires background screening on Nexthink personnel who have access to Customer Data in accordance with Nexthink's then-current applicable standard operating procedure, requirements, and subject to applicable law and regulation.

3.3.3. SECURITY AWARENESS AND TRAINING. Nexthink maintains a security and privacy awareness program that includes appropriate training and education of Nexthink personnel that may access Customer Data. Such training is conducted at time of hire and at least annually throughout employment at Nexthink.

3.3.4. VENDOR RISK MANAGEMENT. Nexthink maintains a vendor risk management program that assessesall vendors that access, store, process, or transmit Customer Data for appropriate security and privacy controls and business disciplines.

3.3.5. SOFTWARE AND ASSET INVENTORY. Nexthink shall maintain an inventory of all software components (including, but not limited to, open-source software) used in the Services, and inventory all media and equipment where

Customer Data is stored. Nexthink reviews the legal terms and requirements of all software components and updates, as applicable, and includes references to source materials or any such relevant terms in its inventory.

3.3.6. WORKSTATION SECURITY. Nexthink shall implement and maintain security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. Nexthink shall restrict personnel from disabling security mechanisms.

4. SERVICE CONTINUITY

4.1 DATA MANAGEMENT; DATA BACKUP. The Services will be hosted only in data centers that attained SOC 2 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations or certifications). Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database systems are replicated in near real time to a mirrored data center in a different geographic region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. Nexthink backs up all Customer Data in accordance with Nexthink's standard operating procedure.

4.2 DISASTER RECOVERY. Nexthink shall (i) maintain a disaster recovery ("**DR**") related plan that is consistent with industry standards for the Services; (ii) test the DR plan at least once every year; (iii) upon request, make available summary test results; and (iv) document any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the Services from being recovered in accordance with the DR plan.

4.3 BUSINESS CONTINUITY. Nexthink shall maintain a business continuity plan ("**BCP**") to minimize the impact to its provision and support of the Services from an event. The BCP shall: (i) include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein; and (ii) be tested annually and updated based on any deficiencies, identified during such tests.

4.4 PERSONNEL. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a Nexthink telephone support representative, geographically distributed to ensure business continuity for support operations.

5. MONITORING AND INCIDENT MANAGEMENT

5.1 MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1. INCIDENT MONITORING AND MANAGEMENT. Nexthink will monitor, analyze, and respond to security incidents (each, a "**Security Incident**"), and where practicable within forty-eight (48) hours, following determination by Nexthink that an Incident has occurred (unless otherwise legally restricted). Nexthink's security group will escalate and engage response teams as may be necessary to address a Security Incident.

5.1.2. BREACH NOTIFICATION. Nexthink will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data without undue delay in accordance with Applicable Law (a "**Security Breach**"), and where practicable within forty-eight (48) hours, following determination by Nexthink that a Security Breach has occurred (unless otherwise legally restricted). Nexthink's security group will escalate and engage response teams as may be necessary to address a Security Breach.

5.1.3. REPORT. The initial report will be made to Customer security contact(s) (or if no such contact(s) are designated within the Customer profile, to the primary technical contact designated by Customer). As information is collected or otherwise becomes available, unless otherwise provided by Applicable Law, Nexthink shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected individuals, government agencies, and data protection authorities in accordance with applicable law and regulation. The report will include the name and contact information of the Nexthink contact from whom additional information may be obtained. Nexthink shall inform Customer of the measures that Nexthink will adopt to mitigate the cause of the Breach and to prevent future Breaches. Notwithstanding the foregoing, the procedures that may be defined by Applicable Law shall govern and take precedence.

5.1.4. CUSTOMER OBLIGATIONS. Without limiting any obligations under the Agreement or DPA, Customer will cooperate with Nexthink by providing any information that is reasonably requested by Nexthink to resolve any Security

Incident, including any Security Breaches, identify its root cause(s), and prevent a recurrence. To the extent consistent with Applicable Law and the DPA, Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

6. VULNERABILITY SCANNING AND PENETRATION TESTS

6.1 BY NEXTHINK. Nexthink shall: (a) regularly monitor and test to ensure the ongoing effectiveness of its Security Program; and (b) promptly remediate all vulnerabilities and findings detected during such monitoring and testing. Subject to scheduled maintenance activities, Company shall conduct vulnerability scanning assessments using a reputable third-party tool at least monthly for the relevant sampling of internet facing infrastructure and applications and the relevant sampling of Company's internal infrastructure and applications (collectively, "**Scanning Assessments**").

6.2 BY A THIRD-PARTY. Nexthink contracts with external, industry recognized organizations to perform a penetration test on the internet and internal infrastructure and applications on Company Information Systems ("**Pen Testing**") to identify risks and remediation options that help increase security. Nexthink shall make executive reports from the Pen Testing available to Customer within its service communications or upon Customer request.

7. SHARING THE SECURITY RESPONSIBILITY

7.1 PRODUCT CAPABILITIES. The Services allow Customer to: (a) authenticate users before accessing the Customer's instance; (b) integrate with SAML solutions; (c) encrypt passwords; (d) allow users to manage passwords; and (e) prevent access by users with an inactive account. Customer manages each user's access to and use of the Services by assigning to each user a credential and user type that controls the level of access to the Services. Customer is solely responsible for reviewing Nexthink's Security Program and making an independent determination as to whether it meets Customer's requirements, taking into account the type and sensitivity of Customer Data that Customer processes within the Services. Customer shall be responsible for implementing access control, encryption and anonymization functionalities, to the extent available within the Services for protecting all Customer Data. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Services. Customer shall be responsible for implementing Nexthink's documented best practices.

7.2 SECURITY CONTACT. Customer agrees to identify and maintain appropriate security contact(s) for all information security incident and information security-related communication. Customer must report to Nexthink any failure of the Services to function materially in accordance with its Documentation (currently via Nexthink's Support Portal at the Nexthink Site or email at support@nexthink.com). Where the Customer cannot report via the Support Portal or email (or other means provided under Documentation), then Customer will report by telephone. Nexthink will provide Customer with its assigned support contact telephone.

7.3 LIMITATIONS. Notwithstanding anything to the contrary in this ISA or other parts of the Agreement, Nexthink's obligations herein are only applicable to the Services. This ISA does not apply to: (a) information shared with Nexthink that is not Customer Data; (b) data in Customer's VPN or a third-party network; and (c) any data processed by Customer or its users in violation of the Agreement or this ISA.

7.4 REGULATORY. Nexthink will comply with those standards agreed in advance in writing that are relevant to the Services; and solely to the extent that the Services are expressly amended to include the storage and processing of specific categories of Customer Data: (a) Nexthink does not store or process credit card information, and Customer shall not provide credit card information in connection with the Services; and (b) Nexthink does not store or process health, financial or regulated information as part of its Services, and Customer shall not any such information in connection with the Services. In the event that Nexthink agrees in writing, as part of an express change the Documentation of the Service,s to process any specific categories of transaction information or personal data, then Nexthink will agree to be subject to the relevant standards and requirements (including applicable industry security standards and reporting requirements). For the avoidance of doubt, these may include the PCI DSS standards on behalf of Customer as mutually agreed; and those requirements applicable to financial institutions (such as The Financial Services Modernization Act of 1999, or GLBA) and health care providers (such as The Health Insurance Portability and Accountability Act of 1996 or HIPAA), as examples.