INFORMATION SECURITY ADDENDUM

EFFECTIVE DATE: October 24, 2023

This Information Security Addendum ("**ISA**") sets forth the administrative, technical, and physical safeguards ChurnZero takes to protect Customer Data as part of its Information Security Program ("**ISP**"). We may update this ISA from time to time to reflect changes in our ISP, provided such changes do not materially diminish the level of security herein provided.

This ISA is made a part of your Subscription Service Agreement (the "**Agreement**") with ChurnZero. Any capitalized terms used, but not defined herein, shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this ISA, the terms of this ISA will apply. This ISA does not apply to Third-Party Offerings purchased or acquired through ChurnZero or the Subscription Service, or to any evaluation, beta, or free use of the Subscription Service.

During the Subscription Term, ChurnZero agrees to maintain an ISP in conformance with the requirements set forth below.

1. **PURPOSE.** This ISA describes the information security standards that we maintain to protect Customer Data, in addition to any requirements set forth in the Agreement (collectively, the "**Security Measures**"). The ISA is designed to protect the confidentiality, integrity, and availability of Customer Data against anticipated or actual threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction, or damage in accordance with laws applicable to the provision of the Subscription Service.

2. **SECURITY PROGRAM.**

2.1. **Scope and Content.** Our ISP: (a) complies with industry recognized information security standards; (b) includes administrative, technical, and physical safeguards (i.e., the Security Measures) designed to protect the confidentiality, integrity, and availability of Customer Data; and (c) is appropriate to the nature, size, and complexity of the Subscription Service and our business operations.

2.2. **Security Policies, Standards, and Methods.** ChurnZero maintains security policies, standards, and methods (collectively, "**Security Policies**") designed to safeguard the processing of Customer Data, by employees and contractors in accordance with this ISA.

2.3. **Security Program Office.** Our Director of Technology Operations leads ChurnZero's ISP, including the development, review, and approval, together with appropriate stakeholders, of our Security Policies.

2.4. **ISP Updates.** Security Policies are available to employees via the corporate intranet. We review, update, and approve the Security Policies at least annually to maintain their continuing relevance and accuracy.

2.5. **Security Training & Awareness.** Our employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with our Security Policies, as well as other corporate policies, such as their continuing confidentiality obligations. To evaluate the effectiveness of this ongoing training, we conduct periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to foster a secure workplace.

3. **RISK MANAGEMENT.** We manage cybersecurity risks in accordance with recognized risk assessment methods, which determines how we identify, prioritize, and manage material risks to

our information assets and the likelihood and impact of such risks occurring. Our senior management reviews identified and documented risks to understand the potential impact on our business and determine appropriate risk levels and viable mitigation options.

4. **CHANGE MANAGEMENT.**

4.1. We deploy changes to the Subscription Service during maintenance windows, details of which are posted to our website or communicated to customers as set forth in the Support Service Policy.

4.2. We follow industry-recognized documented change management policies and procedures for requesting, testing, and approving application, infrastructure, and product related changes. Changes undergo appropriate levels of review and testing, including security and code reviews, regression testing and user acceptance prior to approval for implementation.

4.3. Software development and testing environments are maintained and logically separated from the production environment.

5. **INCIDENT RESPONSE AND BREACH NOTIFICATION.**

5.1. We have adopted an industry-recognized incident response plan and team to assess, respond, contain, and remediate (as appropriate) identified security issues, regardless of their nature (*e.g.,* physical, cyber, product). We review and update our incident response plan at least annually to reflect emerging risks and "lessons learned."

5.2. We notify customers without undue delay after becoming aware of a Personal Data Breach (as such term is defined in our Data Processing Agreement. Further, if a customer reasonably determines notification of a Personal Data Breach is required by law, we will provide reasonable assistance to the extent required for the customer to comply with applicable data breach notification laws, including assistance in notifying the relevant supervisory authority and providing a description of the Personal Data Breach.

5.3. In the event of a conflict between the breach notification provisions in this ISA and those set forth in an applicable Business Associate Agreement (BAA) with ChurnZero, the BAA breach notification terms will apply.

6. **GOVERNANCE AND AUDIT.** We conduct internal control assessments on an ongoing basis to validate that controls are designed and operating effectively. Issues identified from assessments are documented, tracked, and remediated as appropriate. Third-party audits are performed as part of our certification process (more below) to validate the ongoing governance of control operations and their effectiveness. Issues identified are documented, tracked, and remediated as appropriate.

7. **ACCESS AND USER MANAGEMENT.**

7.1. We have implemented and update as necessary reasonable controls to manage user authentication for our employees or contractors with access to Customer Data, including without limitation, assigning each employee or contractor with unique and/or time limited user authorization credentials for access to any ChurnZero System on which Customer Data is accessed and prohibiting employees or contractors from sharing their user authorization credentials.

7.2. We allocate ChurnZero System privileges and permissions to users or groups on a “least privilege” principle and reviews user access lists and permissions to critical systems on a quarterly basis, at minimum.

7.3. All new users must be pre-approved before we grant access to ChurnZero Systems. Pre-approval is also required before changing existing user access rights. Conversely, we promptly disable application, platform, and network access for terminated users upon notification of termination.

8. **PASSWORD MANAGEMENT AND AUTHENTICATION CONTROLS.** Authorized users must identify and authenticate to the ChurnZero Systems and other ChurnZero network, applications, and platforms using their user ID and password. Our enterprise password management system requires minimum password parameters, and authorized users are required to change passwords at pre-defined intervals consistent with industry standards. Multi-factor authentication (MFA) is required for remote access and privileged account access for Customer Data production systems.

9. **ENCRYPTION AND KEY MANAGEMENT.**

9.1. We use industry-standard encryption techniques to encrypt Customer Data in transit; specifically, the ChurnZero Systems are configured by default to encrypt Customer Data files using transport layer security (currently, TLS 1.2+) encryption for web communication sessions. We further rely on policy controls to help ensure sensitive information is not transmitted over the Internet or other public communications unless it is encrypted in transit.

9.2. We use encryption at rest with a minimum encryption protocol of Advanced Encryption Standard (AES) 256-bit encryption. We utilize encryption key management processes to help ensure the secure generation, storage, distribution, and destruction of encryption keys.

10. **THREAT AND VULNERABILITY MANAGEMENT.**

10.1. We have a program to continuously monitor for threats and vulnerabilities that are discovered internally through vulnerability scans, offensive exercises (red team), and employees; or externally reported by vendors, researchers, or others. We document such vulnerabilities and rank them based on severity level as determined by the likelihood and impact ratings assigned by our information security team and then assigns appropriate team(s) to conduct remediation and track progress to resolution as needed.

10.2. We utilize external vendors to conduct security penetration tests on the ChurnZero Systems and Subscription Service environments at least annually to detect network and application security vulnerabilities. Findings from these tests are evaluated, documented, and assigned to the appropriate teams for remediation based on severity level.

11. **LOGGING AND MONITORING.** Monitoring tools and services are used to monitor systems across ChurnZero (to include the ChurnZero Systems and Subscription Service) for application, infrastructure, network and storage events, performance, and utilization. Event data is aggregated and stored using appropriate security measures designed to prevent tampering. Logs are stored in accordance with our data retention policy, and our information security team continuously reviews the logs for alerts and follows up on suspicious events as appropriate.

12. **SECURE DEVELOPMENT.** Our software development life cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components. For Changes and other product releases, we use a

risk-based approach when applying our standard SDLC methodology, which includes such things as performing security architecture reviews, open source security scans, code review, dynamic application security testing, network vulnerability scans and external penetration testing. We perform security code review for critical features if needed; and perform code review for all features in the development environment. We scan packaged software to ensure it's free from trojans, viruses, malware, and other malicious threats. We utilize a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized employees. The SDLC methodology does not apply to Third-Party Offerings.

13. **NETWORK SECURITY.** We use industry standard technologies to prevent unauthorized access or compromise of ChurnZero Systems and our other network, servers, or applications. These technologies include such things as logical and physical controls to segment data, systems, and networks according to risk. We monitor demarcation points used to restrict access such as firewalls and security group enforcement points. Users must authenticate with two-factor authentication prior to accessing ChurnZero Systems containing Customer Data.

14. **VENDOR SECURITY.** We conduct security due diligence and risk assessments of our vendors and thereafter manage vendor security through its risk management program, including reviewing the documented risks associated with vendors to understand the potential impact to our business, implementing mitigation plans to address material risks to business operations, and entering into written agreements with vendors that impose security obligations on them which are necessary for us to maintain our security posture as set forth in this ISA. Customer Confidential Information is shared only with those vendors who are subject to appropriate confidentiality terms with ChurnZero.

15. **PHYSICAL SECURITY.** Our Subscription Service is hosted on Amazon Web Services infrastructure (AWS), an industry leading provider of data centers. AWS provides a rich set of security and compliances for their data centers as explained on their website. This includes physical security and environmental controls to ensure the data is kept safe from human attack and environmental hazards. Access to ChurnZero facilities is granted based on role, reviewed periodically, and removed once access is no longer necessary (*e.g.,* upon termination). We also employ additional measures to protect our employees and assets, including video surveillance systems, onsite security personnel, and such other technologies deemed industry best practice.

16. **DISASTER RECOVERY PLAN.** We have a written disaster recovery plan to manage significant disruptions to the Subscription Service operations and infrastructure, which is reviewed, assessed and (to the extent necessary) updated periodically. We employ industry-recognized data backup, replication, and recovery systems/technologies to support resilience and protection of Customer Data. All backup systems are configured to encrypt backup media.

17. **ASSET MANAGEMENT AND DISPOSAL.** We maintain and regularly update an inventory of Subscription Service infrastructure assets and reconcile the asset list periodically. We also maintain documented data disposal policies to guide personnel on the procedure for disposal of Customer Data. Upon expiration or termination of the Agreement, we will return or delete Customer Data in accordance with the terms of the Agreement. If deletion is required, Customer Data will be securely deleted, except that Customer Data stored electronically in our backup or email systems may be deleted over time in accordance with our records management practices. We retain Customer Data stored in Subscription Service for at most thirty (30) days after the expiration or termination of the Agreement.

INFORMATION SECURITY ADDENDUM

18. **HUMAN RESOURCE SECURITY.** ChurnZero personnel sign confidentiality agreements and acknowledge our ISP and other information security policies during the new employee onboarding process. We also conduct background verification checks for potential ChurnZero personnel with access to Customer Data, in accordance with relevant laws and regulations. The background checks are commensurate to an individual's job duties.

19. **COMPLIANCE ATTESTATIONS.**

19.1. At least once a year, our Subscription Service undergoes a System and Organizational Control (SOC 2), Type 2) audit in accordance with the Attestation Standards under Section 101 of the codification standards (AT 101) by an independent third party that attests to the effectiveness of the controls we have in place to safeguard the systems and operations where Customer Data is processed, stored, or transmitted. At a minimum, the audit covers the security, confidentiality, and availability control criteria developed by the American Institute of Certified Public Accountants (AICPA). Upon request, we will supply Customer with a summary copy of our annual audit reports, which will be deemed Confidential Information under the Agreement.

19.2. In the case of HIPAA, we comply with the HIPAA security rule and data breach notification requirements for the processing of protected health information (PHI). Upon request, we will supply Customer with proof of our compliance with HIPAA.