CLOUDNOSYS INFORMATION SECURITY FRAMEWORK

Cloudnosys maintains a formal information security program and dedicated information security team focused on protecting the confidentiality, integrity and availability of the information assets of both our Subscribers and our company. This group's responsibilities include establishing security standards, identifying reasonably foreseeable security risks, minimizing risks through risk assessment and regular testing, and enforcing internal policies and procedures at Cloudnosys.

Cloudnosys applies reasonable and appropriate administrative, technical, physical, organizational, and operational safeguards and processes to protect Subscriber Data against accidental and unlawful destruction, alteration, and unauthorized or improper disclosure or access. Cloudnosys has based its security framework on ISO 27001 standards, which is an international practice standard for information security management. At least annually, Cloudnosys will (i) conduct an ISO 27001 review; and (ii) have a review of SSAE 18 SOC 2 (Type 2) as well, (or the applicable prevailing national or international standard(s)), in each case of Cloudnosys's facilities and operations providing hosting of the Subscriber Data. Such report will include a description and assessment of the system and control structure in place at Cloudnosys.

Cloudnosys will comply with the following safeguards in connection with the Subscription Services.

Personnel Background Checks & Training

All Cloudnosys personnel go through a background screening process prior to start. Further, all Cloudnosys personnel go through security and privacy awareness training on start, as well as annually thereafter. They are required to sign non-disclosure agreements and sign off that they have read and agree to adhere to Cloudnosys's security policies which include security and privacy safeguards of Subscriber Data.

Network Security

Cloudnosys takes commercially reasonable measures in compliance with best industry practices to prevent disclosure or dissemination of Subscriber Data to any person not having a need to know of or access to such information. Cloudnosys maintains access controls and policies to manage access from each network connection including the use of firewalls or functionally equivalent technology. Least privilege based authentication and authorization controls are maintained and periodically reviewed to ensure that access can only be granted to Cloudnosys personnel whose function and/or duties justifies such access. Some of the additional systems in place to maintain a strong and robust security infrastructure include IDS, centralized log management and comprehensive alerting. All Subscription Service traffic routes through limited public interfaces via Cloudnosys's demilitarized zone (DMZ), which is firewalled. All inbound traffic is routed and filtered to more secure network segments.

Intrusion Detection, Logging & Monitoring

Cloudnosys creates, protects and retains information system log records to the extent needed to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity, including successful and unsuccessful account logon events, account management events, security events, object access, policy change, administrator account creation/deletion and other administrator activity, data deletions, data access and changes, IDS/IPS logs, firewall logs, and permission changes. Cloudnosys monitors for and conducts regular reviews for indications of

inappropriate or unusual activity, and Cloudnosys protects log records from unauthorized access, unauthorized release, loss, modification, falsification, and deletion.

Physical Security

Cloudnosys only uses public clouds to run its operations and subscription services. All Public data center environments such as AWS, GCP and Azure in which Subscription Services are delivered are ISO 27001 or SOC1 / SOC2 compliant and include physical barrier controls designed to prevent unauthorized entrance to each facility and access to Cloudnosys assets. They also require electronic access control validation via card access systems and/or human security personnel. All production environments within which Cloudnosys stores Subscriber Data have deployed a multilayered physical security approach as informed by and consistent with industry standards. Individuals that work in the data center(s) are assigned entry via secondary form factors of authentication such as biometric factors. Any visitors to these facilities are required to sign in with designated personnel, present government issued identification, and are continuously identified as a visitor and escorted by an authorized worker for the duration of their visit.

Cloudnosys operates in a manner that reduces the external surface area of its environments to the extent practical. For example, in Amazon AWS and GCP based environments, Cloudnosys deploys, customizes and secures a Virtual Private Cloud (VPC) and a customized set of Amazon Managed Instances (AMIs) reducing surface area of running services to only what is required to provide the Subscription Service.

Application Security

Cloudnosys utilizes a multi-tier architecture which segregates the web service and application layers from the database layer, with each layer firewalled and limited from other layers via access control lists or security groups. Within the most secure segments, all Subscriber Data is encrypted at rest and logically isolated from other Cloudnosys subscribers.

Internet traffic in connection with our Subscription Services is encrypted with HTTPS/TLS with AES256 bit encryption and related application authentication is performed over this connection; weaker encryption ciphers are not supported. User identification and password transfer is at login only, after which a cryptographically strong random token is used. Account passwords are stored in the database using a strong, one-way cryptographic salted hash. Alternatively, integration with identity management platforms for authentication and authorization is supported and encouraged using standard protocols such as SAML (Single-Sign-On).

Anti-Virus/Anti-Malware

Cloudnosys uses virus and malicious code detection and protection products consistent with industry standards on all workstations and servers used to provide Subscription Services to Subscriber which are updated on a schedule.

Vulnerability Management and Penetration Testing

Cloudnosys conducts regular internal and external scans for network and system vulnerabilities of applications that contain Subscriber Data. Cloudnosys uses a risk-based approach to determine the

timing for remediation of the vulnerabilities, and remediates or mitigates critical or high risk vulnerabilities in accordance with Cloudnosys's NIST based policies.

Cloudnosys retains a qualified third party to conduct network penetration and application vulnerability testing of Cloudnosys's information technology infrastructure (including servers, network devices, applications and databases) ("Penetration Tests") on regular basis. The scope includes OWASP Top 10 among other potential threat vectors. All findings are assessed and remediated commensurate to the finding's severity level. Cloudnosys shall make these third-party executive summary Penetration Test reports available to Subscriber upon request, which test reports shall be Cloudnosys's confidential information pursuant to the confidentiality terms between the parties. The report shall contain any findings, Cloudnosys's remediation, and any risk acceptance. If the report identifies any deficiencies, Cloudnosys will provide Subscriber with Cloudnosys's plan of action to correct the deficiencies, which at a minimum will include: (i) details of actions to be taken by Service Provider and/or its subcontractors to correct the deficiencies, and (ii) target dates for successful correction of the deficiencies. Cloudnosys will provide the action plan within thirty (30) days of request.

Security Notifications

In the event Cloudnosys has actual, confirmed knowledge of any unauthorized or reasonably likely unauthorized access to or acquisition of Subscriber Data in a manner that renders misuse of the information reasonably possible, Cloudnosys will, subject to an any applicable laws, (a) promptly, without undue delay, notify affected Subscribers as required by applicable law and (b) take commercially reasonable measures to address the issue in a timely manner. On a timely basis, Cloudnosys shall provide all relevant information available to Cloudnosys to Subscriber in connection with such security incident, including the following: (i) a description of the nature of the incident; (ii) the name and contact information of a point of contact where additional information may be obtained; and (iii) a description of the measures taken or proposed to be taken to remedy the incident, including measures to mitigate negative effects. Cloudnosys will provide Subscriber with periodic updates about all developments in connection with the foregoing.

Third-Party Security Assessment

Subscriber Data is rated at the highest level of Cloudnosys's security classification. Cloudnosys does not permit third party access of any kind to Subscriber Data. Cloudnosys uses the public cloud (via a virtual private cloud) for infrastructure services only.

Prior to the use of any information system introduced into the Cloudnosys platform and production environments, the Information Security team is first consulted to ensure that new systems and technologies are appropriately vetted and approved for use. The vetting process may include conducting interviews with personnel supplying the equipment and/or researching vendor histories to best determine their security posture and potentially any issues with vulnerabilities and/or breaches of security.

Secure Application Development

Security is pervasive throughout the software development life cycle (SDLC). Cloudnosys's development and quality assurance engineering teams are required to attend secure software development training annually, focused on secure coding and OWASP Top 10 vulnerabilities. All code check-ins require a code

review by a qualified engineer, and code is also tested using static code analysis by a security engineer. During the quality assurance portion of the SDLC, all components are tested using both automated and manual means. Web application vulnerability scans are performed against all applications and the resulting findings are remediated prior to production deployment.

Data Destruction

Cloudnosys develops, implements and maintains appropriate measures designed to properly destroy or otherwise sanitize Subscriber Data prior to disposal, including release of technology infrastructure and assets used to process Subscriber Data out of organizational control, or release of such systems for reuse. Proper destruction or sanitization methods include compliance with NIST-800-88 developed standards for media sanitization, to ensure that Subscriber Data in digital form is not recoverable.

Audit and Assessment

Once per year upon reasonable prior written notice, Subscriber and its authorized representatives (including regulators and independent auditors) may, during normal business hours and subject to confidentiality obligations herein and reasonable access restrictions, conduct audits of Cloudnosys's records and facilities to verify Cloudnosys's compliance with the terms of this Framework Agreement. Cloudnosys will make personnel available as reasonably necessary to answer questions or otherwise assist Subscriber in connection with the same. Any such audit rights shall not permit Subscriber or its authorized representatives to require (i) physical or network access to any of Cloudnosys's systems, (ii) access to materials, data, or information that is (a) unrelated to the Services provided to Subscriber by Cloudnosys; (b) that by its disclosure would cause Cloudnosys or any of its affiliates to be in breach of any confidentiality obligation to any party; (c) such disclosure would be a violation by Cloudnosys of applicable laws; or (d) if such disclosure would hinder law enforcement's investigation into a security event, (iii) any action or disclosure that could reasonably result in a compromise to the efficacy of the information security program or security certifications of Cloudnosys, or (iv) any results of security vulnerability assessments identifying specific security vulnerabilities. Notwithstanding the foregoing, in lieu of an audit right relating to compliance by Cloudnosys of its security obligations pursuant to this Framework Agreement, Cloudnosys may provide (i) written responses to questions regarding its privacy and information security practices that apply to Subscriber Data; and (ii) SOC 2 Type 2 self audit report or equivalent issued by a third-party auditor if available.

Access Control

Cloudnosys employs the principle of least privilege in all cases, ensuring that only those who are responsible for, or working directly with, a resource have access to that resource at any given point in time. Systems hosting subscribers (and the associated Subscriber Data) fall into the highest tier of Cloudnosys's Data Classification and Handling policy, and as such, the highest due diligence and care is placed on them. Several controls are in place to prevent unauthorized access to Subscriber Data.

Encryption & Key Management

Cloudnosys uses industry-standard encryption and key management systems to protect Subscriber Data while in storage and during transmission between Subscriber's network and Cloudnosys's SaaS solution,

including through Transport Layer Encryption (TLS 1.2 or above) leveraging at least 2048-bit RSA server certificates and 256 bit symmetric encryption keys at a minimum. Additionally, all data, including Subscriber Data, is transmitted between data centers or Public Cloud Regions for replication purposes across a dedicated, encrypted link utilizing at least AES-256 encryption.

Continuous Evaluation

To help ensure security, integrity and availability for our Subscribers, Cloudnosys performs periodic, continuous evaluation of its policies and procedures directly and via third-party assessments. Certain certifications associated with currently applicable standards are available on Cloudnosys's certifications page (https://www.Cloudnosys.com/company/compliance-certifications/).

Cloudnosys's information security practices will evolve over time to keep pace with appropriate industry standards and as such this overview is subject to revision. Please refer back to this page to see the most current provisions applicable to the Subscription Service.