SOVOS

Schedule

SECURITY

This Security Schedule describes safeguards and technical, physical and organizational precautions undertaken by Sovos Compliance, LLC ("Sovos") to ensure that data of our customers (each, a "Customer") is reasonably protected from unauthorized access and disclosure. This document constitutes the Security Schedule as referenced in the Sovos Software and Services Agreement or applicable cloud services agreement ("Agreement"). No products or services are sold, licensed or entitled under this document. The rights, responsibilities and undertakings set forth herein apply to Customer only to the extent Sovos is providing products and/or services to such Customer under a separate, current and effective written agreement between the parties that expressly governs Sovos' delivery of products and services. This Schedule replaces any prior version of the Security Schedule, regardless of name.

1. DEFINITIONS

"Business Contact Information" means Customer's own business contact information that Customer has provided for the purposes of communicating with them such as invoicing, support services, marketing etc.; this information may include: customer contact name, job title, business contact email address, telephone numbers and registered office address.

"Customer Protected Information" means PII; any similarly sensitive customer member, customer, employee, or workplace information, or information about the Customer; or any such other information required to be protected or encrypted by local, state, or federal law, regulation or statute, or mandatory industry standard and which is provided to Sovos for the purposes of processing under an executed Order Form, Statement of Work or other agreement. For the purposes of this Schedule, Customer Protected Information does not include Business Contact Information. For the avoidance of doubt, Customer Protected Information is included in the definition of Confidential Information.

"De-identification" or "de-identified" is defined as removing, obscuring, masking, or obfuscating enough Personally Identifiable Information from a record to ensure that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual and no less protections than the provisions of NIST – Draft Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information or its successor.

"Extended Workforce" is defined as any third party with access to Customer Protected Information or Information Processing Systems containing Customer Protected Information by, through, or under Sovos, including sub-contractors and sub-contractors of whatever tier.

"Information Processing System(s)" is defined as the individual and collective electronic, mechanical, and software components of Sovos' and Sovos' Extended Workforce's operations that store, access, process, or protect Customer's Protected Information.

"Information Security Event" is defined as any situation where Customer Protected Information is lost; is subject to unauthorized or inappropriate access, use, or misuse; the security, confidentiality, or integrity of the information is compromised; or the availability of Information Processing System(s) is compromised by attack or directed action.

"Personally Identifiable Information (PII)" means any information with can be used to distinguish or trace an individual's identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual as set forth in NIST – Draft Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) or its successor. PII is included in the definition of Confidential Information.

2. PURPOSE

Sovos has implemented and maintains a comprehensive security program covering all areas of Information Security and with the intention of providing defense in depth for the protection of Customer Protected Information. The program protects Information Processing System(s) and media containing Customer Protected Information from internal and external security threats, as well as Customer Protected Information from unauthorized disclosure. The purpose of this document is to describe the controls, methodologies, and guidelines that Sovos has deployed in the protection of Customer Protected Information.

3. SECURITY POLICY

3.1 Formal Security Policy. Sovos has an information security policy that is approved by Sovos' management and is published and communicated to all Sovos workforce personnel. Sovos will ensure that its Extended Workforce has a similar policy and process.

3.2 Security Policy Review. Sovos will review the information security policy at planned intervals, not to exceed one year since the prior approval date, or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. Sovos will ensure that its Extended Workforce has a similar policy review process. If this policy changes materially Sovos will notify Customer of these changes.

4. RISK MANAGEMENT

4.1 Risk Assessment. Sovos will perform, on at least an annual basis, a comprehensive assessment of the threats and vulnerabilities associated with all Sovos assets, including but not limited to physical, software, virtual, personnel, and intellectual property assets ("Risk Assessment"). The Risk Assessment will determine the likelihood of occurrence of a given threat, the potential impact to Sovos' operations, and any mitigating or compensating controls in place which lower the likelihood, impact, or both.

4.2 Risk Mitigation. Sovos will develop a remediation plan for all identified items from the Risk Assessment which are not adequately addressed and could result in a loss or breach of the confidentiality, integrity, availability, privacy, or overall security of Customer Protected Information or otherwise result in a degradation of the requirements identified within the Security Schedule.

4.3 Risk Assessment Report. The findings from the Risk Assessment, including all identified outstanding risks of an unacceptable level and the planned remediations, will be gathered into a report which will be made available for review by a Customer upon request.

5. ORGANIZATIONAL SECURITY

5.1 Principle of Least Privilege. Sovos will restrict access to Information Processing Systems and Customer Protected Information used in connection with the Agreement to only those Sovos employees or Extended Workforce required to fulfill the obligations under the Agreement and only grant the minimum rights required.

5.2 Access to data outside the region. Prior to allowing access to Customer Protected Information or Information Processing System(s) containing Customer

Protected Information by Sovos employees or Extended Workforce outside the region of origination Sovos will:

5.2.1 Perform a Risk Assessment to identify and mitigate risks to Customer Protected Information from this access.

5.2.2 Ensure data is prevented from leaving the original storage location or region.

5.2.3 Impose the same requirements on its Extended Workforce and remain fully responsible for compliance by its Extended Workforce.

5.3 Security Requirement Persistence. Sovos will include as part of its agreements with its Extended Workforce requirements no less stringent than those contained in this document, including all subsequent parties having access to Customer Protected Information or Information Processing System(s) containing Customer Protected Information.

5.4 Materiality of Organizational Security. Sovos agrees that the requirements listed under Organizational Security are material to its Agreements with Customers.

6. ASSET MANAGEMENT

6.1 Asset Inventory. Sovos will maintain an inventory listing containing at a minimum all Information Processing System(s) and media containing Customer Protected Information.

6.2 Acceptable Use. Sovos will maintain guidance on the acceptable use of information and assets which is no less restrictive than ISO/IEC 27001 or its successor. Such guidance is approved by Sovos' management and is published and communicated to all Sovos workforce personnel.

6.3 Portable Devices. Customer Protected Information, with the exception of Business Contact Information, may not be stored on portable devices including, but not limited to laptops, Personal Digital Assistants, MP3 devices, and USB devices. The foregoing does not prohibit the storage of Protected Information on portable media such as tapes within a data center or in secure offsite storage.

6.4 Personally Owned Equipment. Customer Protected Information, with the exception of Business Contact Information, may not be stored on personally owned equipment.

7. HUMAN RESOURCES SECURITY

7.1 Security Awareness Training. Prior to receiving access to Customer Protected Information, Sovos workforce members will receive security awareness training appropriate to their job function. Recurring security awareness training will be delivered at planned intervals and as required to mitigate significant changes to information security risk.

7.2 Removal of Access Rights. The access rights of all Sovos workforce members with access to Information Processing System(s) or media containing Customer Protected Information will be removed immediately upon termination of their employment, contract, or agreement, or adjusted upon change of job function.

7.3 Background Checks. Company will conduct pre-employment background checks of all global candidates for employment, including regular and temporary employees, independent contractors, or third-party temporary agency employees. Such background checks will include the following elements, to the extent allowed by local law: SSN/name verification, criminal record checks, OFAC, credit, education verification, and drug screening.

8. PHYSICAL AND ENVIRONMENTAL SECURITY

8.1 Secure Areas. All areas, including loading docks, holding areas, telecommunication areas, cabling areas, and off-site areas that contain Information Processing System(s) or media containing Customer Protected Information must be protected by the use of appropriate security controls to include, but not be limited to:

8.1.1 Access will be controlled by use of a defined security perimeter, appropriate security barriers, entry controls, and authentication controls as determined by Sovos' security risk assessment. A record of all accesses will be securely maintained for a minimum of 90 days.

8.1.2 All personnel are required to wear some form of visible identification to identify them as employees, contractors, visitors, etc.

8.1.3 Visitors to secure areas are supervised or cleared via an appropriate background check for non-escorted access. Date and time of entry and departure will be recorded and kept for a minimum of 90 days.

9. COMMUNICATIONS AND OPERATIONS MANAGEMENT

9.1 Protections Against Malicious Code. Sovos will use detection, prevention, and recovery controls which are no less current than ISO/IED 27001 or its successor to protect against malicious software and will train Sovos workforce personnel on the prevention and detection of malicious software.

9.2 Back-ups. Sovos will perform appropriate back-ups of Information Processing System(s) and media containing Customer Protected Information as required to protect the confidentiality, integrity, and availability of Customer Protected Information.

9.3 Media Handling. Sovos will control media containing Customer Protected Information to protect against unauthorized access or misuse.

9.4 Media Disposal. Sovos will securely dispose of media (including, but not limited to paper, disks, CDs, DVDs, optical disks, USB devices, and hard drives) containing Customer Protected Information by the maintenance of procedures to include, but not be limited to:

9.4.1 Disposal of media containing Customer Protected Information so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting similar to the methods described in NIST Special Publication 800-88 or its successors.

9.4.2 Maintenance of a disposal log that is secured and provides an audit trail of disposal activities. The log will be kept for a minimum of 90 days.

9.4.3 Purge of Customer Protected Information from all of Sovos' physical storage mediums (filing cabinets, drawers, etc.) and Information Processing System(s) within thirty (30) days of the latest occurrence of the following: (i) upon termination of this agreement; (ii) upon the completion of Sovos' performance obligations under this document; (iii) when no longer required by law or court order; or (iv) the destruction date specified in Sovos' documented record retention schedule.

9.4.3.1 Upon request, Sovos will provide a Certificate of Destruction to Customer certifying that all Customer Protected Information was purged as set forth in Section 9.4.3 or within thirty (30) business days following Customer's request.

9.5 Exchange of Information. To protect the confidentiality and integrity of Customer Protected Information in transit, Sovos will:

9.5.1 Perform an inventory and risk assessment of all data exchange channels used to transmit Customer Protected Information in order to identify and mitigate risks to Customer Protected Information from the use of these channels.

9.5.2 Monitor all data exchange channels to detect unauthorized information (including, without limitation, PII) releases.

9.5.3 Use appropriate security controls and approved data exchange channels when exchanging Customer Protected Information.

9.5.4 Use industry standard enhanced security measures where available (at a minimum 128-bit AES encryption if 256-bit AES is not available) to encrypt Customer Protected Information transmitted via open networks, including, but not limited to the Internet and wireless.

9.5.5 Prohibit the use of web tracking technologies including, but not limited to web beacons, web bugs, invisible GIFs, and persistent cookies from being used to gather information about Customer or Customer's customers, except as agreed to in writing by Customer and as necessary for Sovos to perform its obligations under the Agreement.

9.6 Protection of Information. To protect the confidentiality and integrity of Customer Protected Information at rest, Sovos will:

9.6.1 Encrypt all Customer Protected Information wherever it resides on Sovos systems.

9.6.2 Encrypt all Customer Protected Information on all backup and removable media.

9.6.3 Utilize industry-standard encryption algorithms and mechanisms (AES-256 at a minimum and wherever possible, off-system key storage) for all at-rest encryption implementations.

9.6.4 Develop and implement a full key lifecycle management program and subsequent processes designed to fully protect encryption keys.

9.7 Vulnerability Management. To protect against system, network, and application vulnerabilities and exploitation, Sovos will:

9.7.1 Regularly monitor vulnerability and patch notification lists and repositories for new and updated system vulnerability information.

9.7.2 Regularly scan internal and external networks and applications for the existence of potential security weaknesses and gaps, on a period not to exceed thirty (30) days between cycles.

9.7.3 Perform penetration testing of networks, systems, and applications on an annual basis that includes testing to exploit identified security weaknesses and gaps as well as faulty business and processing logic.

9.7.4 Perform risk assessment of all disclosed and relevant vulnerability information as it applies to Sovos systems, networks, and applications.

9.7.5 Test all planned updates and mitigations prior to deployment into production environments.

9.7.6 Update systems, networks, and applications to protect against vulnerabilities on a defined and continuous cycle, not to exceed thirty (30) days in total duration for standard updates.

9.7.7 Utilize a process to categorize, prioritize, and deploy vulnerability remediations based on Sovos defined risk management standards.

9.8 Monitoring. To protect against unauthorized access or misuse of Customer Protected Information residing on Information Processing System(s), Sovos will:

9.8.1 Employ security controls which are no less restrictive than ISO/IEC 27001 or its successor and tools to monitor Information Processing System(s) for unusual or suspicious activities, exceptions, and Information Security Events.

9.8.2 Protect logging functions and log information against tampering and unauthorized access and keep critical logs for a minimum of thirteen (13) months.

9.8.3 Perform, at a minimum, quarterly reviews of access logs and take immediate actions necessary to mitigate issues found.

9.8.4 At Customer's request, make redacted logs available to Customer to assist in investigations.

9.8.5 Synchronize the clocks of all relevant Information Processing System(s) using a national or international time source.

10. ACCESS CONTROL

10.1 User Access Management. To protect against unauthorized access or misuse of Customer Protected Information, Sovos will:

10.1.1 Employ a formal user registration and de-registration procedure for granting and revoking access rights to all Information Processing System(s).

10.1.2 Employ a formal password management process, including setting of minimum password complexity, length, validity period, reuse, and reset requirements, based on current industry practices as identified by leading cybersecurity organizations and regulatory bodies.

10.1.3 Perform a recurring review of users' access and access rights to ensure that they are appropriate for the users' role.

10.2 User Responsibilities. To protect against unauthorized access or misuse of Customer Protected Information residing on Information Processing System(s), Sovos will:

10.2.1 Train Information Processing System(s) users on current security practices.

10.2.2 Use appropriate controls to protect unattended equipment from access and use by unauthorized individuals.

10.2.3 Use appropriate controls to protect Customer Protected Information contained in all work areas from inappropriate access, including, but not limited to paper and on display screens.

10.3 Network Access Control. Access to internal, external, and public network services that allow access to Information Processing System(s) will be controlled. In order to mitigate the risk of unauthorized access, Sovos will:

10.3.1 Protect all Informational Processing Systems and related networks with edge firewall devices.

10.3.2 Use authentication controls that are no less restrictive than ISO/IEC 27001 or its successor. Require that all administrator access utilize multi-factor authentication.

10.3.3 Employ network access controls that are no less restrictive than ISO/IEC 27001 or its successor.

10.3.4 Tightly control access to physical and logical diagnostic and configuration ports.

10.3.5 Segregate internal networks and network segments based on their sensitivity.

10.4 Operating System Access Control. To protect against unauthorized access or misuse of Customer Protected Information residing on Information Processing System(s), Sovos will:

10.4.1 Control access to operating systems by use of a secure log-on procedure and multi-factor administrator access.

10.4.2 Use unique identifiers (e.g. user IDs) to individually identify Information Processing System(s) users.

10.4.3 Monitor and control access to utility programs that are capable of overriding system and application controls.

10.4.4 When technically possible, shut down inactive sessions after a defined period of time.

10.4.5 When technically possible, employ restrictions on connection times to high risk applications.

10.5 Mobile Commuting and Remote Working. To protect Customer Protected Information residing on Information Processing System(s) from the risks inherent in mobile computing and remote working, Sovos will:

10.5.1 Perform a risk assessment which, at a minimum, identifies and mitigates risks to Customer Protected Information from mobile commuting and remote working.

10.5.2 Maintain policies and procedures for managing mobile commuting and remote working.

10.5.3 Use security controls to manage authentication of mobile and remote users which are no less restrictive than ISO/IEC 27001 or its successor. Require that all remote access utilize multi-factor authentication.

11. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

11.1 Security of System Files. To protect Information Processing System(s) and system files containing Customer Protected Information, Sovos will restrict access to source code to authorized users who have a direct need to know.

11.2 Security in Development and Support Processes. To protect Information Processing System(s) and system files containing Customer Protected Information, Sovos will:

11.2.1 Ensure development systems are segregated from production environments and areas.

11.2.2 Use a formal change control process to implement Information Processing System(s) changes.

11.2.3 Use security controls which are no less restrictive than ISO/IEC 27001 or its successor to minimize information leakage.

11.2.4 Perform quality control and security management oversight of outsourced software development.

11.2.5 Require that all developers, including any subcontractors, successfully complete secure code training based on the Open Web Application Security Project ("OWASP"), its successor, or a similar industry-standard program.

12. INFORMATION SECURITY INCIDENT MANAGEMENT

12.1 Reporting Information Security Events and Weaknesses. To protect Information Processing System(s) and Customer Protected Information, Sovos will:

12.1.1 Maintain a process to ensure that Information Security Events are reported through appropriate management channels as quickly as possible. Sovos will ensure that its Extended Workforce has a similar process.

12.1.2 Perform initial and recurring training of all Sovos employees and Extended Workforce on how to report any observed or suspected Information Security Event. Sovos will ensure that its Extended Workforce has a similar process.

12.1.3 Notify Customer by email within forty-eight (48) hours of all Information Security Events which affect Customer Protected Information or environments that store, transmit, or process Customer Protected Information. Following any such event, Sovos will promptly notify Customer whether or not Customer Protected Information was compromised or released to unauthorized parties, the Customer Protected Information that was affected, and details of the event. Sovos will work with Customer on response and remediation efforts.

13. BUSINESS CONTINUITY MANAGEMENT

13.1 Business Continuity Management Program. In order to protect the confidentiality, integrity, and availability of Customer Protected Information, Sovos will:

13.1.1 Develop lines of business disaster recovery programs which are designed to meet or exceed the established recovery point objectives (RPOs) and recovery time objectives (RTOs) for each line of business.

13.1.2 Maintain a business continuity management program that ensures that security controls that meet or exceed the requirements of this document are maintained in test and actual business continuity scenarios.

13.1.3 Update and test Business Continuity Plans at planned intervals, to occur no less than on an annual basis, and as required to mitigate significant changes to information security risk.

14. CUSTOMER SECURITY ASSESSMENTS

14.1 Initial and Recurring Security Assessments. Prior to the release of Customer Protected Information and each year throughout the Term of the Agreement, Sovos will permit Customer representatives to perform an on-site or virtual assessment no more than 30 days from initial request of the physical and logical security controls used at Sovos' data processing and business facilities. Assessments will be performed during regular business hours, at a date and time agreed to by both parties and will not require online access to Information Processing System(s). Such assessments shall occur no more often than once per year,

14.2 Security Assessments Following Information Security Events. Following the occurrence of an Information Security Event, Sovos will permit Customer representatives to perform an on-site or virtual assessment of the physical and logical security controls used at Sovos' data processing and business facilities in order to assess the impact of the event, even if an assessment has been completed within the year.

14.3 Security Assessment Findings. Upon completion of an assessment, Customer will provide Sovos with an assessment completion letter or report that summarizes Customer's findings. These findings may identify critical security deficiencies identified as "Mandatory" that require immediate correction before Customer can release, or continue to release, Customer Protected Information to Sovos. Sovos will implement and continue to maintain all mutually agreed upon "Mandatory" security findings. If mutual agreement to "Mandatory" security findings cannot be reached, then these issues may be escalated using the dispute resolution provisions contained within the underlying Agreement.

15. DE-IDENTIFICATION OF CUSTOMER PROTECTED INFORMATION USED IN NON-PRODUCTION ENVIRONMENTS

15.1 De-Identification Requirement for Non-Production Environments. Customer Protected Information will be de-identified prior to being transferred to a non-production environment.

15.2 Exclusions to the De-Identification Requirement.

15.2.1 De-identification is not required if the security controls used in the environment are equivalent to the security controls used in the production environment and the security controls used to meet or exceed the requirements of this document.

15.2.2 De-identification is not required if de-identification would interfere with the resolution of a current production failure. De-identification will be performed to the extent possible and the Customer Protected Information that has not be de-identified will be removed from the non-production environment as soon as the failure has been resolved.

15.2.3 De-identification is not required if de-identification would interfere with an atypical, short-term, non-production activity (e.g. near-production final testing) where de-identification would distort the results of the activity. De-identification should be performed to the extent possible and the Customer Protected Information that has not been de-identified should be removed from the non-production environment as soon as the activity has been completed.

15.2.4 If Customer PII is required to be used in non-production environments and the requirement does not meet one of the exceptions listed above, Sovos will obtain written permission from Customer prior to the use.

16. PRIVACY

16.1 Segregation. All Customer data is segregated, either through logical or physical methods, from data of other Customers, as well as internal data from Sovos.

16.2 Data Usage. Sovos will not use Customer data for any purpose other than in support of the obligations described herein and within any additional services agreement.

16.3 Legal Compliance. Sovos maintains compliance with all privacy laws and regulations applicable to the performance of its obligations under the Agreement.

16.4 Testing Restrictions. Sovos does not use Customer Protected Information, in whole or in part, in connection with any testing in system development.

17. VENDOR MANAGEMENT

17.1 Vendor Assessment. Sovos conducts on-site reviews and risk assessments of all vendors processing, storing, or transmitting Customer Protected Information.

17.1.1 Such assessments will occur prior to engagement with new vendors and then afterwards on a reoccurring schedule based on the risk associated with the engagement.

17.2 Vendor Risk Assessment. Information gathered from the vendor review is used as inputs to the Sovos risk assessment process which is used to generate a metrics-based narrative report identifying all areas of concern and the associated potential impact and likelihood.

17.3 Vendor Risk Remediation. Sovos works with the vendor to identify a plan of action for remediation of all identified risks and the successful completion of the remediation plan.

18. INDEPENDENT ASSESSMENT

18.1 Reoccurring Testing. Sovos will, on at least an annual basis, engage an independent external auditor to conduct a review of the Sovos security program, its controls, practices, and processes, against one of the following: ISO 27001, SSAE 16/18, ISAE 3402, their successors, or a similar industry-standard security control framework.

18.2 Remediation of Findings. Sovos will address any finding identified within an independent assessment judged to be of a medium-level risk or higher in accordance with the Sovos risk management program.

18.3 Assessment Report. Sovos will, upon request, make available for review by Customer, the results of any such relevant independent assessment, including the treatment plans for any identified risks or findings.

19. BUSINESS CONTACT INFORMATION

19.1 Sensitivity. Sovos recognizes that certain elements of Business Contact Information may be considered PII under a given governing regulation and that security and data privacy controls may be required for the protection of such information.

19.2 Protection. Sovos will implement controls utilized to provide protection against the unauthorized modification, deletion, access, or disclosure of Business Contact Information. These controls may be similar to the controls described herein for the protection of Customer Protected Information and will be designed to comply with the requirements and obligations of the governing law.

19.3 Transfers. Customer agrees that the Business Contact Data may be transferred to other Sovos Affiliates (including overseas transfers) for the purposes of administration and performing the contract.

20. CHANGES

Sovos may, from time to time and in our discretion, make changes to this document or the terms and conditions set forth herein, provided however, in no event shall Sovos make any changes that will degrade the safeguards and/or technical, physical and organizational precautions undertaken by Sovos without prior written notice to the Customer. When Sovos makes changes hereto which do not degrade the safeguards and/or precautions undertaken by Sovos, Sovos will provide notice as appropriate under the circumstances, e.g., by displaying a notice within the applicable Sovos products or services, by updating the Schedule located at https://sovos.com/customer-legal-data-sheets/ or by sending Customer an email.