Data Security and Privacy Principles for Acoustic SaaS Products

The technical and organizational measures provided in this Data Security and Privacy attachment (DSP) apply to Acoustic SaaS Products, including any underlying applications, platforms, and infrastructure components operated and managed by Acoustic in providing the SaaS Product (components), except where Customer is responsible for security and privacy and otherwise specified in writing between Acoustic and Customer. Customer is responsible for: a) determining whether the SaaS Product is suitable for Customer's use and; b) implementing and managing security and privacy measures for elements not provided and managed by Acoustic within the SaaS Product described in applicable attachments ("Attachments") to this document, the Data Protection Agreement (DPA) or the SaaS Agreement (such as systems and applications built or deployed by Customer upon an Infrastructure as a Service offering, or Customer end-user access control to Software as a Service offerings). The measures implemented and maintained by or on behalf of Acoustic within each SaaS Product will be subject to annual certification of compliance by IBM, Acoustic's sub-contractor in respect of the SaaS Product and/or by Acoustic with ISO 27001 or SSAE SOC 2 or both.

1. Data Protection

a. Security and privacy measures for each SaaS Product are designed in accordance with Acoustic's secure engineering and privacy- by-design practices to protect Content input into a SaaS Product, and to maintain the availability of such Content pursuant to the SaaS Agreement, including applicable Attachments and Transaction Documents. Customer is the sole controller for any personal data included in the Content and appoints Acoustic as a processor to process such personal data (as those terms are defined in Regulation (EU) 2016/679, General Data Protection Regulation). Acoustic will treat all Content as confidential by not disclosing Content except to Acoustic employees, contractors, and subprocessors, and only to the extent necessary to deliver the SaaS Product, unless otherwise specified in an Attachment.

b. Acoustic will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

c. Upon request, Acoustic will provide reasonable evidence of stated compliance and accreditation, which may, where available, comprise certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, and other industry standards as specified in an Attachment, and which may be held by IBM who for the time being operate the infrastructure, hosting, support and related services in respect of the SaaS Product and/or by Acoustic itself. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the SaaS Product's stated compliance and accreditation.

d. Additional security and privacy information specific to a SaaS Product may be available in a relevant Attachment (such as a product Data Sheet) or other standard documentation to aide in Customer's initial and ongoing assessment of a SaaS Product's suitability for use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. Acoustic will direct Customer to available standard documentation if asked to complete Customer-preferred questionnaires or forms and Customer agrees such documentation will be utilized in lieu of any such request. Acoustic may charge an additional fee to complete any Customer-preferred questionnaires or forms or to provide consultation to Customer for such purposes.

2. Security Policies

a. Acoustic will maintain and follow IT security policies and practices that are integral to Acoustic's business and mandatory for all Acoustic employees. The relevant CIO or equivalent will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. Acoustic will review its, and procure that IBM, whist acting as sub-contractor in respect of the SaaS Product, will review its IT security policies at least annually and amend such policies as Acoustic or IBM (as appropriate) deems reasonable to maintain protection of SaaS Products and Content processed therein.

c. Acoustic will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned Acoustic subsidiaries. In accordance with Acoustic internal process and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by Acoustic. Each Acoustic company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. Acoustic employees will complete security and privacy education annually and certify each year that they will comply with Acoustic's ethical business conduct, confidentiality, and security policies, as set out in Acoustic's Business Conduct Guidelines. Additional policy and process training will be provided to persons granted administrative access to SaaS Product components that is specific to their role within Acoustic's operation and support of the SaaS Product, and as required to maintain compliance and any certifications stated in the relevant Attachment.

3. Security Incidents

a. Acoustic will maintain and follow, and procure that IBM whilst acting as sub-contractor for the SaaS Product, will maintain and follow documented incident response policies consistent with NIST guidelines for computer security

incident handling and will comply with data breach notification terms of the Agreement.

b. Acoustic will investigate unauthorized access and unauthorized use of Content of which Acoustic becomes aware (security incident), and, within the SaaS Product scope, Acoustic will define and execute an appropriate response plan. Customer may notify Acoustic of a suspected vulnerability or incident by submitting a technical support request.

c. Acoustic will notify Customer without undue delay upon confirmation of a security incident that is known or reasonably suspected by Acoustic to affect Customer. Acoustic will provide Customer with reasonably requested information about such security incident and the status of any Acoustic remediation and restoration activities.

4. Physical Security and Entry Control

a. Acoustic will, and whilst IBM is sub-contractor, procure that IBM will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Acoustic facilities used to host the SaaS Product (data centers). Auxiliary entry points into data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to data centers and controlled areas within data centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a data center and controlled areas will be logged, and such logs will be retained for not less than one year. Acoustic will revoke or procure the revocation of access to controlled data center areas upon separation of an authorized employee. Acoustic will follow formal documented separation procedures that include, but are not limited to, prompt removal from access control lists and surrender of physical access badges.

c. Acoustic will ensure that, including by contractual commitments by relevant vendors, that any person duly granted temporary permission to enter a data center facility or a controlled area within a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

d. Acoustic will take precautions to protect the SaaS Product's physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. Access, Intervention, Transfer and Separation Control

a. Documented security architecture of networks managed by or on behalf of Acoustic in its operation of the SaaS Product will be maintained. Such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, will be reviewed for compliance with secure segmentation, isolation, and defense-in-depth standards prior to implementation. Wireless networking technology may be used in the maintenance and support of the SaaS Product and associated components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to SaaS Product networks. SaaS Product networks do not use wireless networking technology.

b. Measures for a SaaS Product will be maintained that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. Appropriate isolation of its production and non-production environments, will be maintained and, if Content is transferred to a non-production environment, for example in order to reproduce an error at Customer's request, security and privacy protections in the non-production environment will be equivalent to those in production.

c. To the extent described in the relevant Attachment, Content not intended for public or unauthenticated viewing will be encrypted when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for Customer's secure transfer of Content to and from the SaaS Product over public networks.

d. Content will be encrypted at rest when specified in an Attachment. If the SaaS Product includes management of cryptographic keys, documented procedures will be maintained for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

e. If access to Content is required, it will be restricted to the minimum level required. Such access, including administrative access to any underlying components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized personnel following the principles of segregation of duties. Measures will be maintained to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or the request of authorized personnel, such as the account owner's manager.

f. Consistent with industry standard practices, and to the extent natively supported by each component managed by or on behalf of Acoustic within the SaaS Product, technical measures will be maintained enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

g. Use of privileged access will be maintained and security information and event management measures will be maintained designed to: a) identify unauthorized access and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented policy.

h. Logs in which privileged access and activity are recorded will be retained in compliance with Acoustic's worldwide records management plan. Measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs will be maintained.

i. To the extent supported by native device or operating system functionality, computing protections for its end- user systems will

be maintained that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

6. Service Integrity and Availability Control

a. Acoustic will: a) ensure security and privacy risk assessments of its SaaS Products are carried out at least annually; b) ensure penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, are carried out before production release and annually thereafter; c) ensure a qualified independent third-party performs penetration testing at least annually; d) ensure automated management and routine verification of underlying components' compliance with security configuration requirements are carried out; and e) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact.

b. Acoustic will take reasonable steps to avoid SaaS Product disruption when performing tests, assessments, scans, and execution of remediation activities.

c. Acoustic will maintain policies and procedures designed to manage risks associated with the application of changes to its SaaS Products. Prior to implementation, material changes to a SaaS Product, including its systems, networks, and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the SaaS Product and its Customers, expected outcome, rollback plan, and documented approval by authorized personnel.

d. Acoustic will maintain an inventory of all information technology assets used in its operation of the SaaS Product. Acoustic will continuously monitor and manage the health, including capacity, and availability of the SaaS Product and underlying components.

e. Each SaaS Product will be separately assessed for business continuity and disaster recovery requirements pursuant to documented risk management guidelines. Each Acoustic SaaS Product will have, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for the SaaS Product, if provided, will be established with consideration given to the SaaS Product's architecture and intended use, and will be described in the relevant Attachment. Physical media intended for off-site storage, if any, such as media containing SaaS Product backup files, will be encrypted prior to transport.

f. Acoustic will maintain measures designed to assess, test, and apply security advisory patches to the SaaS Product and its associated systems, networks, applications, and underlying components within the SaaS Product scope. Upon determining that a security advisory patch is applicable and appropriate, Acoustic will implement the patch pursuant to documented severity and risk assessment guidelines. Implementation of security advisory patches will be subject to Acoustic change management policy.