Loopio UK Data Security Exhibit

Last Updated: October 2023

This Data Security Exhibit (this "**Exhibit**") is incorporated by reference into the existing Master Services Agreement, the ("**Agreement**") entered into by and between Loopio UK Ltd., previously Avnio Ltd. ("**Loopio UK**" "**we**" "**our**", or "**us**") and the customer that is a party to such Agreement ("**Customer**").

In the event of any conflict between this Exhibit and the Agreement, this Exhibit shall prevail to the extent of any inconsistency. In the event of any conflict between this Exhibit and any Order executed hereunder, this Exhibit shall prevail to the extent of any inconsistency, except with regard to any provision of any Order that specifically identifies a conflicting provision of this Exhibit and states that the conflicting provision of this Exhibit does not prevail.

Loopio UK may periodically amend this Exhibit by posting an amended version on its website, available at: https://www.avnio.com/legal-data-security/, so long as such amended version does not materially degrade the terms herein. Revisions will become effective on the date the updated Exhibit is posted by Loopio UK, and Customer's continued use of or access to the Loopio Solution after the date the updated Exhibit is posted will constitute Customer's acceptance of those terms. If Customer reasonably objects to the revisions, Customer may do so within 30 days by sending an email to legal@loopio.com, in which case the previous terms will continue to apply for the remainder of Customer's subscription term. Upon renewal, the current Exhibit terms will govern.

1. Additional Definitions

Capitalised terms used in this Exhibit, and not otherwise defined, shall have the meaning set out below:

- "**Law(s)**" means all applicable laws, regulations, ordinances, rules and orders of any court or government body.
- "**Personnel**" means employees and contractors who perform activities in connection with the handling of Customer Data.
- "**Security Incident**" means the reasonable suspicion of, discovery by, or notice to, Customer or Loopio UK that:
    - Customer Content has been disclosed, accessed or obtained by an unauthorised person;
    - Systems have been compromised; or
    - A person has threatened the unauthorised disclosure, access to or obtaining of any Customer Data.

2. General Obligations

2.1 Security Program. Loopio UK agrees to maintain a comprehensive data security program that contains administrative, technical and logical safeguards designed to protect the confidentiality, integrity, and availability of Customer Content and protect it from disclosure, improper alteration, or destruction.

2.2 Risk Assessment and Treatment. Loopio UK maintains a risk assessment program pertaining to the treatment and handling of Customer Content that has been approved by management, and has been communicated to all employees.

2.3 Access Controls. Customer has the ability to limit access to the Services to authorised Personnel to prevent unauthorised access to Customer Data. Services access logs are maintained andServices support identity verification, including multi-factor authentication.

2.4 Encryption. All Customer Content is encrypted while "in transit".

2.5 Restrictions. Loopio UK will not, except as necessary to perform its obligations set forth in the Agreement:(a) use or disclose any Customer Content for any purpose other than as is strictly necessary to perform its obligations as set forth in the Agreement; (b) copy, use, reproduce, display, perform, modify, destroy or transfer any Customer Content or works derived from Customer Data; nor (c) sell any Customer Data, or anything that includes any Data, to any person.

2.6 Backups. Loopio UK does not backup Customer Content due to the nature of the Services and the SFDC platform, however, Customer may extract Customer Content from the SFDC platform to perform its own backups.

2.7 Physical Security of Data Centers. Loopio UK employs restricted access and visitor logs, electronic controlled access system; and CCTV on sensitive areas, unless prohibited by law, at all physical locations of its Data Centers

3. Compliance with Application Law

3.1 Regulatory Cooperation. If Loopio UK collects, accesses, receives, stores or otherwise handles any Customer Content that becomes subject to a regulatory inquiry, notification or other action required by all applicable Laws, Loopio UK agrees to assist and cooperate to meet any obligation to the relevant regulatory authority.

3.2 Right of Access. In accordance with our Privacy Policy, Loopio UK will reasonably cooperate with and assist Customer, as necessary, to enable any individual exercising their right of data access, correction, deletion or blocking of Personal Data under any applicable Law.

3.3 Personal Data. If Loopio UK collects, uses or transfers Personal Data, it will be handled in accordance with its Privacy Policy.

4. Disclosure by Law

4.1 Mandatory Disclosure. If Loopio UK is required by any Law to disclose any Customer Data, Loopio UK will:(a) to the extent permitted by applicable Law, give Customer prior notice of the obligation as soon as practical after becoming aware; and(b) take all steps to enable Customer an opportunity to prevent or limit the disclosure of the Customer Data.

5. Security Awareness Training

5.1 Security Training. Loopio UK has developed a mandatory security awareness and training program for all members of Loopio UK cloud service operations, which includes: (a) training on how to implement and comply with its Information Security Program; and (b) promoting a culture of security awareness through periodic communications from senior management with employees.

6. Scans and Assessments

6.1 Scans. In order to maintain the security of the Services, regular network and system scans are performed, including non-intrusive network scans on customer-facing infrastructure.

6.2 Assessments. Loopio UK utilises external service providers to perform an application vulnerability assessment biannually.

6.3 Patching. A software patching process is in place to remedy vulnerabilities in a timely manner based on scans and assessments.

6.4 Summary. A summary of the results of the most recent vulnerability assessments will be made available to Customer upon request.

7. Security Incidents and Response

7.1 Security Response. Loopio UK has a response plan that includes procedures to be followed in the event of a Security Incident, including: (a) **Formation** of an internal incident response team assessing the risk the incident poses and determining who may be affected, and mitigate additional risk or impact; (b) **Notification**. Internal reporting as well as Customer notification in the event of unauthorised disclosure of Customer Content in accordance with the Agreement; (c) **Recordkeeping**. Customer Content is managed according to the Agreement (including this Exhibit); and (d) **Audit**. Conducting and documenting root cause analysis and remediation plans.

8. Contingency Planning and Disaster Recovery

8.1 Availability and Recovery. Excluding components of the Services operated by SFDC, Loopio UK infrastructure and, where applicable, Customer Content maintained and stored for the purposes of assuring availability or recoverability in the event of a disaster is maintained with the same data security standards as in production environments.

8.2 Recovery Time Objective. Recovery Time Objective ("**RTO**") is Loopio UK's objective for the maximum period of time between Loopio UK's decision to activate the disaster recovery processes to failover the Services

to a secondary site due to a declared disaster and the point at which our customers may resume production operations at a secondary site. If the decision to failover is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade. The RTO is 24 hours.

8.3 Recovery Point Objective. Recovery Point Objective ("**RPO**") is the objective for the maximum period of data loss measured as the time from which the first transaction is lost until Loopio UK's declaration of the disaster. There is no RPO associated with the Services.

9. Audit Controls

9.1 Audit Controls. Hardware, software and/or procedural mechanisms are maintained to record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements.

10. Portable Media

10.1 Portable Media. Loopio UK does not store Customer Content on desktops, laptops or other removable storage devices which are housed outside of a secured data centre. Portable media access on all Loopio UK managed desktops and laptops are disabled by default.

11. Secure Disposal

11.1 Secure Disposal. Upon Customer request, Loopio UK will dispose of tangible property containing Customer Data, using available technology, such that Customer Content cannot be practically read or reconstructed.

12. Testing

12.1 Testing. Loopio UK will periodically test and evaluate the key controls and operations against relevant compliance frameworks to validate that they are properly implemented and effective in addressing the threats and risks identified.

13. Monitoring

13.1 Monitoring. Loopio UK will monitor network and production systems, including error logs on servers, disks and security events for any potential problems, including: (a) reviewing changes affecting systems handling authentication, authorization; and (b) reviewing User and privileged (e.g. administrator) access to Loopio UK production systems.

14. Change and Configuration Management

14.1 Change Management. Loopio UK will maintain policies and procedures for managing changes to production systems, applications, and databases, including: (a) a process for documenting, testing and approving the promotion of changes into production; and (b) acceptance testing and approval processes specifically related to standard bug fixes, updates, and upgrades made available for the Services.

15. Background Checks

15.1 Employee Background Checks. Loopio UK shall perform background checks for its employees who will have access to Customer Data. Such background checks shall include:(a) for all employees, a criminal record search for the previous seven years; (b) for U.S.-based employees, verification of social security number for the previous five years; and (c) verification of eligibility to lawfully work in the applicable jurisdiction.