slido

SECURITY APPENDIX

Technical and Organizational Measures

During the provision of the Service, Slido implements and maintains the following security measures to ensure confidentiality, integrity and availability of Customer Data, including personally identifiable information (PII).

1. INFORMATION SECURITY PROGRAM AND ORGANISATION

1.1. Slido maintains and will continue to maintain a written Information Security Program that includes policies, procedures, and controls, including the Information Security Policy.

1.2. The Information Security Program is maintained in accordance with ISO 27001 standards or equivalent standards to ISO 27001.

1.3. Slido uses independent external auditors to test and verify the adequacy of its Information Security Program. A dedicated team is responsible for the Information Security Program at Slido.

1.4. Slido appoints a DPO (Data Protection Officer).

1.5. The security of Customer Data is a shared responsibility of Slido and the Customer:

(a) Slido is responsible for the implementation and operation of the Information Security Program described in this document; and

(b) Customer is responsible for secure management of access credentials of Users and using controls and configuring certain features and functionalities of the Slido Services the Customer considers adequate to maintain appropriate security, protection, deletion, and backup of Customer Data.

2. HUMAN RESOURCES SECURITY

2.1. Slido conducts reasonable and appropriate background checks on all Slido staff in accordance with applicable laws and regulations as a part of the hiring process.

2.2. Slido staff access to Customer Data is bound by confidentiality and non-disclosure agreements.

2.3. Slido conducts security awareness and data protection training for all Slido staff at least once per year.

2.4. Slido has a formal disciplinary process in place to take action against employees who have committed an information security breach.

3. PHYSICAL SECURITY CONTROLS

3.1. Slido is hosted on certified Tier 4+ data centres with a defined and protected physical perimeter, strong physical controls including but not limited to access control mechanisms, controlled delivery and loading areas, surveillance, security guards, uninterrupted power supply or fire protection in accordance with SOC 2, ISO 27001 or equivalent standards.

3.2. Slido ensures that access to corporate facilities is tightly controlled to ensure only authorized personnel are allowed access. All visitors are escorted by Slido staff while on the premises.

4. ACCESS CONTROLS

4.1. Slido maintains a formal access control policy and employs a centralized access management system to control Slido staff access to Customer Data and to support the secure creation, amendment and deletion of user accounts.

4.2. Slido regularly reviews the access rights to ensure that all user accounts and user accounts privileges are allocated on a need-to-know basis. Upon a change in scope of employment or termination of employment, access rights are removed or modified as appropriate.

4.3. Access to highly sensitive systems such as data centres is controlled by secure log-on procedures including MFA or VPN technology.

5. PROCESSORS

5.1. Slido performs due diligence on its Processors that access, process or store Customer Data to ensure that Processors maintain adequate physical, technical, organizational, and administrative controls based on the risk appropriate to their services provided.

6. OPERATIONAL SYSTEM SECURITY AND ENCRYPTION

6.1. Slido maintains a formal software development life cycle that includes secure coding practices based on OWASP recommendations and related standards and will perform both manual and automated code reviews before the code is released into a production environment.

6.2. Slido performs an external penetration test of applications on an annual basis to assess the security of the Service.

6.3. Slido logically separates Customer Data from the data of other customers.

6.4. Slido maintains an isolated production environment that includes commercial-grade network management controls such as load balancer, firewall, and intrusion detection system.

6.5. Slido Services supports the latest recommended secure cipher suites and protocols (such as SHA-256 with RSA Encryption) to encrypt all traffic in transit.

6.6. Slido encrypts Customer Data at rest using AWS RDS Encryption - AES-256 or stronger.

7. INCIDENT RESPONSE AND BREACH NOTIFICATION

7.1. Slido maintains procedures that ensure an appropriate response to security incidents addressing monitoring, investigation, response, and notification.

8. BUSINESS CONTINUITY AND DISASTER RECOVERY

8.1. Slido stores Customer Data redundantly at multiple locations in its hosting provider's data centres to ensure availability. Slido maintains backup and restoration procedures, which will allow recovery from a major disaster.

8.2. Slido maintains a business continuity/disaster recovery plan ("BC/DR Plan"). The BC/DR Plan provides for the restoration of access to Customer Data, a continuation of operations and Slido Services during a range of short-term and long-term disaster events. The BC/DR Plan covers re-establishment of information technology environment(s) following an unplanned event impacting the data centre, infrastructure, data or systems.

8.3. The BC/DR Plan and related procedures are tested at least annually.