SUMMARY OF ORGANISATIONAL AND TECHNICAL SECURITY MEASURES

This document is a high level summary of the technical and organizational security measures and controls implemented in Keyloop's organisation, Products and Services in order to protect Personal Data. These measures and controls will be updated from time to time. Defined Terms have the meanings given in Keyloop's Standard Terms and Conditions and applicable Product Specifications.

1. Keyloop's Global Security Organisation

1.1. Keyloop employs personnel with full-time responsibility for information security.

1.2. Keyloop has a comprehensive set of information security policies, which are disseminated to all personnel and are reviewed regularly.

1.3. Keyloop regularly trains personnel on information security measures.

1.4. Keyloop's Global Security Organisation's functions include:

1.4.1. maintaining the effectiveness of Keyloop's security policy, standards, guidelines, practices, procedures and technical controls for the organization, including the review of policy, standards, training and documentation on a regular basis;

1.4.2. managing and investigating any security incidents or violations of company security and notifying Customer within 72 hours of confirmed incidents in relation to personal data or otherwise where the incident is reasonably likely to cause harm to Customer;

1.4.3. security testing and product evaluation of security elements of technologies, systems and applications deployed within Keyloop;

1.4.4. maintaining an incident response plan and appropriate perimeter protection for networks;

1.4.5. applying reasonable mechanisms to ensure secure communication of Customer's Information;

1.4.6. ensuring all access to the Customer's Information is authorized, authenticated and logged (including without limitation use of unique identifiers for users);

1.4.7. securing the Customer's Information against unintended information disclosure at rest and in motion;

1.4.8. disposing of Customer's Information using industry accepted data destruction methods and retaining Certificates of Destruction;

1.4.9. preventing Customer's Information from being in open view and implementing a least privilege model for access to Customer's Information;

1.4.10. administrative, technical, and physical safeguards (including without limitation measures taken at Keyloop's premises)to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction; and

1.4.11. timely patching and treatment of vulnerabilities identified from application testing.

2. Physical Access Controls

2.1. Keyloop data centres use physical controls including access control mechanisms, controlled delivery and loading areas and surveillance. Only authorized personnel have access to the data center premises.

2.2. Equipment at Keyloop's data centers is protected from power failures and other disruptions caused by failures in supporting utilities, and is correctly maintained.

2.3. Customer is responsible for physical security for non-hosted products and services.

3. System Access Controls

3.1. Access to Customer Data by Keyloop is only by approved, authenticated personnel as required by those personnel to fulfil their function.

3.2. Keyloop's measures include unique user IDs, password policies requiring regular changes, and processes for removing access rights for departing personnel.

3.3. Keyloop's DMS Software allows Customers to manage access parameters, roles and permissions.

4. Incident Response

4.1. Keyloop's Global Security Organisation maintains a detailed incident response plan, which is continually reviewed and revised where appropriate.