

Technical and Organisational Security Measures

1.0 Purpose & Scope

- 1.1 This document (the “**Measures**”) is a high-level summary of the technical and organisational security measures and controls implemented within Keyloop in order to protect the confidentiality, integrity and availability of all Customer Data including Customer Personal Data processed by Keyloop on behalf of Customer.
- 1.2 Unless otherwise specified in this document and appendix 1, defined terms used in this document shall have the meaning given to them in the Standard Terms and Conditions or Data Processing Addendum, each being available at <https://www.keyloop.com/legal-documentation>.
- 1.3 These Measures will be updated from time to time as Keyloop continuously reviews its measures and operational effectiveness, to take into account developments in information security and to mitigate against new risks and threats that may arise. In updating the Measures, Keyloop will ensure that the level of protection it affords to Customer Personal Data shall be no less than the controls set out in the previous version of the Measures.
- 1.4 The Measures are applicable to all Keyloop owned or developed Systems.
- 1.5 These Measures do not contain detailed architecture or specific measures that are confidential and would not be appropriate for Keyloop to share without compromising Keyloop or third parties it works with.

2.0 Information Security Framework

- 2.1 Keyloop works towards the standards set out in ISO27001:2013 and aligns with Good Industry Practice. The implementation of our Information Security Framework is proportionate to the scale and complexity of the services we provide, the risks relevant to the type and nature of Customer Personal Data we process and the cost of implementation.
- 2.2 The Information Security Framework is assessed by an independent third party on a regular basis (at least annually). There are Keyloop internal cross functional committees that operate to regularly review matters affecting information security.

Information Security Policies

- 2.3 Keyloop has adopted a high-level Information Security Policy which sets out how information security operates within Keyloop. The Policy is reviewed at least annually, is owned by Keyloop's Security

Office (“KSO”) and is approved by the Keyloop Leadership Team sponsor and the Keyloop Risk Committee.

2.4 Underneath the high-level policy there are several other specific Keyloop policies and technical processes which are connected to information security. These include:

- 2.4.1 Acceptable Use - covering matters such as: access to Systems, internet and email usage, external storage, mobile devices, software usage and clear desk policy.
- 2.4.2 Data Classification - covering Keyloop’s standard classification of data.
- 2.4.3 Incident Management - covering at a high-level how Keyloop responds to Security Incidents.

The Keyloop Security Office (KSO)

2.5 The KSO team includes authorised, skilled and qualified individuals who have overall responsibility for information security within Keyloop. The KSO team is led by the Keyloop Information Security Director.

2.6 The KSO team have several responsibilities and these are summarised briefly below:

- 2.6.1 maintaining the effectiveness of Keyloop’s Information Security Framework, including its policies, standards, guidelines, practices, procedures and technical controls;
- 2.6.2 liaising with customers, suppliers, partners and other interested third parties on matters concerning information security (such as customer due diligence requests and audits);
- 2.6.3 working with other Keyloop departments to ensure that Keyloop remains compliant with Applicable Laws concerning the protection of Customer Personal Data;
- 2.6.4 managing and investigating Security Incidents or violations of Keyloop’s Information Security Policies;
- 2.6.5 security testing and the evaluation of products and security elements in technologies, Systems and applications deployed within or procured by Keyloop;
- 2.6.6 maintaining an incident response plan and appropriate perimeter protection for networks;
- 2.6.7 applying reasonable mechanisms to ensure the secure transfer and/or communication of Customer Personal Data;
- 2.6.8 ensuring that there are secure methods available for the disposal or destruction of Customer Personal Data;
- 2.6.9 ensuring that the control measures set out in this document and deployed around the business are effective, kept up to date with industry standards and appropriate to Keyloop operations.

Risk Management

2.7 Keyloop operates a business-wide risk governance framework with a risk register and risk treatment plans in place where necessary. Functional areas, such as the KSO, also have functional risk registers which are regularly reviewed.

3.0 Minimum Controls

Mobile Devices & Remote Working

- 3.1 Keyloop has certain security measures in place to manage the risks posed by the use of mobile devices and when working remotely. Such measures include:
- 3.1.1 Bring Your Own Device policy and procedures;
 - 3.1.2 secure access via VPN;
 - 3.1.3 device registration if Keyloop-owned;
 - 3.1.4 operating system updates;
 - 3.1.5 restricted access to only Keyloop-approved applications and information services;
 - 3.1.6 secure wireless access;
 - 3.1.7 access controls;
 - 3.1.8 malware controls;
 - 3.1.9 remote disabling erasure or lockout;
 - 3.1.10 device encryption.
- 3.2 Use of removable storage devices (such as USB) is discouraged but if it is the only option, they are treated as confidential information (or secret), stored securely, should be Keyloop devices which are protected with encryption and only when authorised by the KSO.

Human Resources Security

- 3.3 *Screening.* Keyloop has a robust recruitment process and screening is conducted by a third-party provider who confirms the employee has a right to work in the country, educational record and suitable references covering at least the previous 3 years.
- 3.4 *Contracts.* Employees and contractors enter into binding written contracts with Keyloop covering the requirements of their work and the duty to ensure the confidentiality of all information and data they may come into contact with that is not public. They are required to comply with all applicable Keyloop policies.
- 3.5 *Awareness & Training.* Keyloop ensures that its employees (and contractors where relevant) undergo training on onboarding and annually to refresh knowledge. Awareness campaigns are also used throughout the business to highlight and promote areas of interest, such as phishing and cyber-attacks.
- 3.6 *Disciplinary Procedures.* A formal disciplinary process exists to take action against employees who violate any Keyloop Information Security Policies. If a contractor is involved, action may be taken to terminate their contract if necessary.
- 3.7 *Termination & Change of Employment.* If an employee or a contractor leaves Keyloop, we take action to ensure that they are reminded of their ongoing duties of confidentiality and will enforce it if we discover the obligations are not upheld. All access to Keyloop Systems is revoked as soon as possible, ID passes are returned and any physical assets are also either collected or returned to Keyloop without undue delay.
-

Asset Management

- 3.8 Responsibility for Assets.** Physical asset registers are drawn up and owned by the IT department. Assets are owned and managed by the functional departments. Acceptable use of such assets is set out in the Keyloop Acceptable Use Policy. All Keyloop assets must be returned to Keyloop on termination or expiry of employment or other contract with Keyloop.
- 3.9 Information Classification.** Keyloop's Data Classification Policy sets out three levels of classification (Public, Confidential and Secret). Customer information is classified as "Confidential" unless there are particular requirements for additional secrecy agreed with Keyloop or it is public information already.
- 3.10 Asset Handling.** Keyloop has procedures which govern the handling of data in accordance with its classification. Customer Personal Data is only processed to the extent necessary to provide the services and as outlined in the Agreement. Keyloop does not permit the transfer of Customer Personal Data to personal email accounts or personal storage locations, or on unapproved or unauthorised storage media.
- 3.11 Data /Media Erasure & Disposal.** Keyloop ensures that equipment and data storage media is erased and disposed in accordance with industry standards, such as Infosec level 5 for the reuse of information storage devices and destruction DIN66399 level 5. Confidential paper waste is placed in locked confidential waste boxes and then shredded (with destruction certified) in accordance with Good Industry Practice by a competent independent third party.
- 3.12 Decommissioning.** On termination of the Services, Keyloop will work with its customers and suppliers to communicate the arrangements. The operational practicalities of this will depend upon the products and services provided. Information which needs to be retained for legal reasons will be retained securely, and not in active use, until it is no longer required.

Access Control

- 3.13 General Principles.** Keyloop shall establish an Access Control Policy based on our operational requirements. Users shall only be provided with access to the Keyloop networks and services required in order to perform the responsibilities of their roles and which they have been authorised to use. Access will be reviewed at regular intervals. Access to program source code is restricted.
- 3.14 User Access Management.** A formal process exists to register and de-register users to enable assignment of access rights. Once assigned, access may also be revoked or re-assigned if the user's responsibilities change. Access is revoked when a user leaves the business and will be suspended when a user is inactive for lengthy periods of time.
- 3.15 Privileged Access Management** Privileged access is granted to a restricted number of users and additional controls exist to manage privileged users' access. Administration accounts must be used when performing operations requiring additional levels of security (such as installing applications which require authority). Production and non-production Systems will have separate and unique
-

accounts.

3.16 User Responsibilities. Users will be allocated unique user ID which is not shared with others. All users must follow Keyloop's Information Security Policies. Users must ensure that they use authentication information (e.g. passwords) which are secret and not revealed to any other user. Such passwords must follow the Keyloop system-enforced password policies and procedures, which include;

3.16.1 changing the password on first entry;

3.16.2 always keeping the password secure and not writing it down in clear text;

3.16.3 minimum password length;

3.16.4 requiring alpha and numeric, lower and upper case, special characters etc.;

3.16.5 being locked out if password is entered incorrectly after a maximum number of tries;

3.16.6 regular system-enforced change of password.

Where available, multi-factor authentication tools must also be used by the user. Users will be required to re-authenticate prior to permitting them to re-access a System after a period of inactivity.

Cryptography

3.17 Keyloop ensures encryption is considered when deploying Privacy by Design and Security by Design principles and aims to adopt industry-standard protections to confidential and secret Information Assets.

3.18 Key management procedures are also in place to ensure the secure generation, storage, distribution, backup and destruction of the cryptographic keys.

Physical & Environmental Security

3.19 Keyloop ensures that the following security measures are in place in all buildings and equipment (where applicable) that are controlled by Keyloop:

3.19.1 physical security measures to prevent unauthorised persons from gaining access;

3.19.2 protection against environmental risks to the premises, such as water ingress, severe weather, fire threats, pest infestations, earthquakes and similar occurrences;

3.19.3 entry access control systems to the premises which record entry and exit;

3.19.4 a visitors process which must be followed, including visitor logs, escorted visits and temporary visitor passes;

3.19.5 CCTV in place where appropriate and properly controlled and logged in compliance with Applicable Laws;

3.19.6 data centre security procedures in place;

3.19.7 unique ID passes for Keyloop personnel;

3.19.8 liaison with third parties to cover out of hours periods to ensure prompt response to security issues;

3.19.9 equipment protected securely to ensure unauthorised logical or physical access;

3.19.10 protection for power and telecommunications cabling to guard against interference, interception or damage;

3.19.11 maintenance schedules to ensure continued availability and integrity;

- 3.19.12 guidance and training available to personnel for the correct handling of equipment and safety precautions in premises;
- 3.19.13 fire detection, power protection, air conditioning, humidity control and other environmental detection systems provided and operated in accordance with manufacturer's guidelines and in compliance with health & safety regulations;
- 3.19.14 suitable procedures in place to ensure appropriate authorisation for removal of equipment.
- 3.19.15 processes in place to report lost or stolen equipment to Keyloop as soon as possible.

3.20 Where Keyloop works with third parties who provide services impacting Customer Personal Data and does not control the physical and environmental security measures, Keyloop ensures that the measures in place with its supply chain require similar standards (which are based on the standards set out in the ISO27000 series).

Operations Security

3.21 *Operating Procedures.* Keyloop has in place operational procedures to ensure that all personnel who need to use them have them available for reference, including system configurations, maintenance and backup, information handling, communication and escalation contacts, Security Incident handling, logging and monitoring.

3.22 *Change Management.* Changes to Keyloop's organisational measures, business processes, facilities and Systems are controlled with change management procedures which track the changes required, relevant dates, test results (where applicable), appropriate approvals, status of change and audit trails.

3.23 *Capacity Management.* Keyloop manages its resources to monitor, tune and project future capacity requirements to ensure system performance in line with any service levels appropriate to its products.

3.24 *Separation of Environments.* Separate production and non-production environments are implemented to reduce the risk of unauthorised access or changes in a production environment. Testing should not take place in production environments unless in exceptional circumstances. Access to the separate environments is strictly controlled. Production data containing personal data should not be copied to non-production environments unless the equivalent controls are provided and it is approved by members of the Keyloop Leadership Team and the Data Protection Officer.

3.25 *Protection from Malware.* Anti-malware is in place on Systems in accordance with Good Industry Practice. Controls are in place to detect and block attempted malware. Scans for malicious code take place periodically. Controls exist to prevent or detect use of unauthorised software, use of known or suspected malicious websites and procedures are in place to handle suspected or confirmed malware.

3.26 *Back-ups.* Keyloop operates a back-up policy which confirms the intervals for back-up, validation of the back-ups, the back-up retention periods, testing schedule and support. Back-ups will be encrypted in transit and at rest.

3.27 *Logging & Monitoring.* Event logs exist to record user activities, exceptions, faults, key operational and security related events to support threat detection and investigations into Security Incidents. Access to such logs is restricted to only those who need to know for operational purposes and unauthorised modification or deletion is not permitted. Logs are maintained for a minimum of 7 years.

3.28 *Control of Software.* Procedures are implemented to control the installation of software on operational Systems.

3.29 *Vulnerability Management.* Keyloop has a vulnerability management procedure which is aligned with ISO27001 and Good Industry Practice. Where vulnerabilities are detected, security patches, fixes or workarounds are implemented in order to address the vulnerabilities within reasonable timeframes. Penetration testing is scheduled to take place periodically by a competent independent third party and upon material changes to core Keyloop Systems. It is our policy not to allow third parties we work with (such as customers or suppliers) to conduct their own penetration tests.

Communications Security

3.30 Networks forming part of Systems are designed, managed and controlled to protect information systems and applications according to Good Industry Practice. This includes the following factors:

- 3.30.1** network boundaries in place to prevent unauthorised access to the Systems, allow only authorised and authenticated access and to deny unauthorised outbound traffic;
- 3.30.2** firewall rules are configured based on least privilege principle and ensure secure network services are used (such as SFTP, HTTPS, SSH);
- 3.30.3** firewalls are reviewed periodically (usually every 3 to 6 months);
- 3.30.4** devices which are not Keyloop-owned or approved are not permitted to join the corporate network;
- 3.30.5** suitable protection of wireless networks within Keyloop's own premises and logically separated from all networks that form part of Keyloop's core Systems.

3.31 Information transfers take place securely and in accordance with Keyloop policies and procedures. Where information needs to be transferred to third parties, appropriate agreements are put in place to govern such transfers including appropriate non-disclosure of confidential information provisions.

System Acquisition, Development & Maintenance

3.32 Keyloop maintains software development, acquisition and maintenance processes which are defined and regularly maintained in accordance with Good Industry Practice.

3.33 Privacy by Design and Security by Design principles are implemented when designing and implementing Keyloop software.

3.34 Change management processes exist and are detailed and reviewed in accordance with Good Industry Practice.

- 3.35 When development work and code changes take place, testing and reviews take place to ensure there is no adverse impact on organisational operations or security.
- 3.36 Outsourced development work is supervised and monitored to ensure compliance with Keyloop's requirements and all Applicable Laws.
- 3.37 Acceptance testing regimes are in place to ensure new information systems, upgrades or version changes are properly verified and tested before launch.
- 3.38 Keyloop retains and maintains its source code in secure repositories which are only accessible to those who have an approved 'need to know' purpose for accessing them.
- 3.39 Third party code used (such as open source) is appropriately licensed and authorised for use.

Supplier Relationship Management

- 3.40 Keyloop ensures that it documents in contractual agreements with Sub-Processors provisions to address information security and the protection of Customer Personal Data.
- 3.41 Key risks involved in using suppliers are communicated and discussed regularly, including supplier performance and service delivery.
- 3.42 Changes to the provision of services are recorded with appropriate change control and contract variation mechanisms.
- 3.43 Any supplier security standards which are available publicly for review are reviewed and verified by the KSO.
- 3.44 Third parties that Keyloop contract with will naturally determine their own technical and organisational measures appropriate to their business operations and their assessment of risks. Keyloop confirms that it procures, within its contractual relationships with its Sub-processors, that Sub-processors process any Customer Personal Data with measures that are compliant with applicable Data Protection Legislation and at least similar to the controls in these Measures.
- 3.45 Suppliers providing core or critical information services to Keyloop are risk assessed in accordance with Keyloop's standard risk matrix. If risks are required to be mitigated they will be captured on the functional risk register and treatment plan.
- 3.46 Keyloop is unable to procure a blanket condition that all Sub-Processors are bound to a requirement to be audited by third parties (such as Keyloop customers wishing to audit them directly) but it ensures that appropriate steps are in place to enable Keyloop to confirm Sub-Processor's compliance with the terms of the applicable contract.
- ~~3.47 Contractual agreements with suppliers also contain appropriate provisions allowing for the~~

remediation of issues and non-compliance within reasonable timeframes agreed with Keyloop and, where these are not adhered to, a notice of termination of the contract for material breach may be necessary.

Information Security Incident Management

- 3.48 Keyloop operates an incident management policy to ensure a quick, effective and orderly response to Security Incidents.
- 3.49 Security Incidents are reportable through a variety of channels, including external email addresses available to use if the Security Incident is discovered by third parties.
- 3.50 Keyloop personnel are expected to remain vigilant to Security Incidents and are required to report suspected or observed Security Incidents, or weaknesses, in Systems or services that Keyloop operates or uses.
- 3.51 Security Incidents are investigated promptly and responded to in accordance with our procedures. This includes analysing and reporting on the root cause of the Security Incident.
- 3.52 Third parties Keyloop needs to inform (including Customers in the event of a personal data breach regarding their Customer Personal Data) are informed within legally prescribed timeframes.
- 3.53 Lessons which can be learned from Security Incidents are recorded and acted upon.

Information Security Aspects of Business Continuity Management

- 3.54 Keyloop holds appropriate business continuity plans to support its availability levels in its contractual arrangements, taking into account the size, scale and nature of the Keyloop organisation and the products we offer.
- 3.55 Reviews and verification of the procedures in place within relevant departments are conducted at regular intervals and actions arising from such tests are reviewed and acted upon appropriately.

Compliance Management & Reviews

- 3.56 Independent reviews of Keyloop's information security measures take place at planned intervals or when significant changes to the scope of any audit or certifications occur.
- 3.57 Management reviews of the information security system and protection of data mechanisms take place in forums and committee meetings that take place regularly throughout each financial year, with high risk or serious matters being escalated to the Board of Directors and/or Audit Committee as necessary.
- 3.58 Where Keyloop receives external validation or certification it shall make a copy of the certificate available to third parties upon request.

4.0 Administration

This document will be administered and managed in line with the governance and approval structure in Keyloop. This shall ensure that Keyloop remain conscious of the need to ensure that the minimum service and control levels so that they do not drop below the standards set out within our Risk and Control Framework. Keyloop control functions, including the Keyloop Security Office and Data Protection Office, have the authority to create further guidelines to aid Keyloop employees in meeting the requirements of this document. Any guidelines produced shall also be regularly reviewed, at least annually, and may be amended to better serve the needs of employees and objectives of this document.

5.0 Further Information

If you have any questions about the content of this document, please contact your Keyloop Account Manager.

6.0 Version Control

Creation Date: June 2023
Last Reviewed: June 2023
Next Planned Review: June 2024
Document Owner: Keyloop Data Protection Officer

Version	Date	Comments
V1.0	June 2023	Final version approved for launch

APPENDIX 1: Definitions

Term	Description
Good Industry Practice	means the exercise by Keyloop of that degree of skill, diligence, prudence, foresight and operating practice which would reasonably and ordinarily be expected from a skilled and experienced provider of the Services or comparable Services.
Security Incident	means any actual and unauthorized breach of Keyloop's Systems which could have a direct impact on the confidentiality, integrity or availability of Customer Data.
Systems	mean the information and communications technology systems used by Keyloop in performing the Services including any software (including cloud software), middleware, hardware, applications, infrastructure, network, devices and peripherals which are used to process Customer Data.