Keyfort Cloud Services (KCS)

Data Location, Security & Privacy

1. Executive Summary

The purposes of this document is to provide a common understanding of the data location, security, privacy, resiliency and disaster recovery aspects of KCS.

2. Corporate Security Policy

Keyfort's security policy defines and facilitates the secure operation of the KCS systems, data therein and its supporting organization.

For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

For Keyfort, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as encryption, firewalls, intrusion detection and physical security.

3. Organizational Security

Keyfort:

- Reviews security plans for Keyfort's networks, systems, and services using multi layered processes.
- Conducts security design and implementation level reviews.
- Provides ongoing consultation on security risks associated with a given project.

- Monitors for suspicious activity on Keyfort's networks, systems and applications, and follows formal incident response processes to recognize, analyse, and remedy information security threats.

- Drives compliance with established policies through security evaluations and internal audits.

- Develops and delivers training for employees on complying with Keyfort security policy, including in the areas of data security and secure development.

- Runs a vulnerability management program to help discover problem areas on Keyfort's networks, and participates in remedying known issues within expected time-lines. Keyfort also works with the security community outside of Keyfort.

- Works with physical security teams dedicated to the physical security of Keyfort's data centres. These security officers are qualified with training to protect high security enterprises with mission-critical infrastructures.

4. Data Asset Management

Data assets comprise customer and Keyfort data.

Operation of KCS includes the use of virtual machines running across multiple physical machines. This provides for processing, memory, data storage and network bandwidth on demand in an automatic, dynamic and scalable environment. As a result in the event of physical hardware failure the virtual machines are automatically redistributed to other hardware without service interruption. Likewise additional hardware can be added and taken out for maintenance without loss of service.

The virtual machines, each with its encapsulated customer services, are automatically backed up complete with operating system, application software, data and configuration enabling rapid restoration of service in the event of disruption.

The data is stored across multiple data storage devices complete with RAID10 mirroring and auto backup. Thereby avoiding disruption in the event of hardware failure and also past data versions can be restored as required.

Dual system monitoring complete with alerts and logging is implemented throughout KCS.

Automatic data replication from customer site(s) to KCS is available for disaster recovery purposes.

Automatic data replication from KCS and any linked cloud services such as Google Apps for Work or Microsoft Office 365 to the customer site using a Keyfort data storage device, provided for the purpose and located on the customer's site, is available. This ensures that the customer always has a copy of all their data which can be used for disaster recovery and independence of Cloud purposes.

All data is held in country of origin unless requested otherwise by the customer. Keeping data in country simplifies legal jurisdiction and reduces security risk.

Keyfort can supply, as appropriate, a Written Statement of Assertion in accordance with the International Standard on Assurance Engagements ISAE 3402 standard if so required by the customer.

5. Access Control

Keyfort employs a number of authentication and authorization controls that are designed to protect against unauthorized access.

Authentication Controls

Keyfort requires the use of a unique user ID for each employee. This account is used to identify each person's activity on Keyfort's network, including any access to employee or customer data. This unique account is used for every system at Keyfort. When an employee commences work with Keyfort they are assigned a user ID and granted a default set of privileges. At the end of a person's employment, their account's access to Keyfort's network is disabled and passwords reset.

Keyfort's password policies include as appropriate password expiration, restrictions on password reuse, sufficient password strength, two-factor authentication, certificates and one-time password generators.

Authorization Controls

Access rights and levels are based on an employee's job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Keyfort employees are only granted a limited set of default permissions to access company resources, such as their email, and Keyfort's internal portal. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Keyfort's security policies. An employee's authorization settings are used to control access to all resources, including data and systems for Keyfort's cloud technologies and products.

Accounting

Keyfort's policy is to log administrative access to every Keyfort production system and all data. These logs are reviewable by Keyfort on an as-needed basis.

6. Personnel Security

Keyfort employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Upon employment, Keyfort will verify an individual's education and previous employment, and perform internal and external reference checks. Where appropriate and statutory regulations permit, Keyfort may also conduct criminal, credit, immigration, and security checks. The extent of background checks is dependent on the desired position. Upon acceptance of employment at Keyfort, all employees are required to execute a confidentiality agreement as part of their employment contract.

7. Physical & Environmental Security

KCS includes power feeds (A&B), uninterruptible power supply (N+1), generator backup (N+1), air conditioning (N+1) and fire suppression systems to ensure its server environment is resilient.

KCS features.

- Direct connection to services via encrypted data links from your designated office(s) and roving staff. Ensuring that your data is available in part or full only as you designate for staff and selected partners if any.

- Secure resilient 100Mbps high performance Internet connection. Greater bandwidth speed is available on request.

- 24x7 security and support.

- In the event of a power failure your services are automatically protected through an uninterruptible power supply (large mains batteries) with further protection via generators with many hours of fuel.
- All servers are above flood level.
- Security personnel ensure that only authorised members of staff are permitted access.

8. Infrastructure Security

KCS includes a series of threat prevention and management services.

- Automatically updated malware prevention
- Automatically updated intrusion prevention.
- Automatically updated anti virus.
- Firewall protocol, application, access and bandwidth control.
- Encrypted network links.
- White lists.
- Black lists.
- Dual monitoring with auto alerts.
- Traffic and activity logging.
- Change management to provide a centralized mechanism for registering, approving, and tracking changes.
- Operating systems and application services are 'patched' and upgraded as an when required on a proactive basis.

9. Systems & Software Development & Maintenance

Security is a key component of our design and development process. Keyfort's engineering organization does not require development teams to follow a specific software development process; rather, teams choose and implement processes that fit the project's needs. As such, a variety of software development processes are in use at Keyfort, from Agile Software

Development methodologies to more traditional, phased processes. Keyfort's security review processes are adapted to work within the chosen framework. Engineering management has defined requirements for project development processes:

- Peer reviewed design documentation.
- Adherence to coding style guidelines.
- Peer code review.
- Multi-layered security testing.

The above mandates embody Keyfort's software engineering culture, where key objectives include software quality, robustness, and maintainability. While the primary goal of these mandates is to foster the creation of software artifacts that excel in all aspects of software quality, Keyfort's experience also suggests that they can reduce the incidence of security flaws and defects in software design and implementation.

- The existence of adequately detailed design documentation is a prerequisite of the security design review process, since in early project stages it is generally the only available artifact on which to base security evaluations.
- Many classes of implementation-level security vulnerabilities are fundamentally no different from low-risk, common functional defects. Many implementation-level vulnerabilities are caused by fairly straightforward oversights on the developer's part.
- Given developers and code reviewers who are educated with respect to applicable vulnerability patterns and their avoidance, a peer review-based development culture that emphasizes the creation of high-quality code supports a secure code base.

10. Disaster Recovery & Business Continuity

The objective is to minimise service interruption due to hardware failure, natural disaster, or other catastrophe. Keyfort implements a disaster recovery program at all of its data centres. This program includes multiple components to minimize the risk of any single point of failure, including the following:

- Data replication and backup. Application data is replicated to multiple systems within a data centre and in some cases also replicated to multiple sites.

- Keyfort operates a geographically distributed set of data centres/customer sites that are designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between these centres help to support swift failover. Management of these centres is also distributed to provide location-independent, around-the-clock coverage, and system administration. Keyfort conducts regular testing of its disaster recovery plans. For example a disaster in a centre is simulated by taking IT systems and business and operational processes in that location off-line, and allowing such systems and processes to transfer to fail-over services designated by the disaster recovery (DR) plan. During the course of the test, it is verified that business and operations functions can operate during fail-over and hidden/unknown dependencies on the off-line location are identified and logged for later remediation.

11. Summary

KCS provides a resilient, secure and cost effective environment for customer services and data. From initial porting of the data and services to the cloud to its subsequent use, data privacy is respected as the right of the customer and limited in accordance with the customer's requirements. All data is transmitted over encrypted links and is stored in country of origin unless otherwise requested by the customer. Keyfort also provides an option for keeping a synchronized updated copy of the data held within KCS on the customer premises with a data storage unit supplied for the purposes thereof.