SELECT
CHALETS & HOTELS

Select Chalets & Hotels IT Security Policy

1. Governance

Under Select Chalets & Hotels data security policies, all of IT operations undergo risk, compliance and business continuity reviews. This is documented in our Select assessment of our IT infrastructure and it updated as and when a formal software 'update' takes place.

2. Data Access

2.1 Audits

Information security documents, procedures, policies and training materials are annually updated, reviewed and audited. Audits are performed by our data protection officer on representative sample sets to ensure reasonable coverage by staff across the aforementioned materials.

2.2 Access and authorization

All accounts on our systems have role-based privileges. An accompanying audit trail with active/disabled status uniquely identifies user accounts, notes access can also be sourced. Segregation of duties/profile is an underlying principle when using our internal software CRM or reservation software or Sage programmes.

All 'user' accounts that can access sensitive data are managed by automated systems that follow basic password compliant password standards

(a) Each person has an individual account that authenticates the individual's access.

(b) Any staff that are no longer working for Select have their access revoked as standard HR exit procedures

2.3 Data storage location

Cloud based applications that have encrypted import/export capabilities

2.4 Physical data

Select does not keep any data in physical form

2.5 Training

Training is devised to the immediate team based on information flow or updates reflecting our audit tests and legislation updates.

3. Change Management

3.1 Methodology

The methodology for how Select manages change, ensures data integrity, data protection and asset security is then documented and reported on annual basis.

This is then socialised as part of staff on-boarding as well as subsequent operational updates and regular update compliance training.

4. Operations

4.1 Software systems

Monitoring our systems takes place on a daily basis with the use of our third party supplies.

4.2 Data backup and retention

Data backup and retention schedules are documented in line with requirements of Select business operation requirements. Security event logs and application audit trails are kept in manual form. Periodic checks are performed to ensure backup integrity and procedure completeness.

4.3 Transmission and encryption

All data transfers with external parties are done over industry standard encryption channels. When sensitive data at rest it is encrypted by industry standard encryption.

4.4 Breach and security incidents

Dedicated incident (breach and non breach) management documents are reviewed, audited and socialised on a periodic basis at least annually in accordance with SiteMinder's Data Security Breach Policy.

All security incidents are initially prioritised as critical, and then adjusted as the incident progresses and is assessed. Priority is given to containment. While active, all security incidents have dedicated resources applied until resolution of the incident is achieved. Following resolution, a post-event analysis is performed and all reasonably practicable steps are taken to implement measures to avoid recurrence and improve security for both direct and indirect related risks. All security incidents as well as known operational risks are recorded and managed from a central risk register.

Select will advise all relevant third parties of any security or data breach in accordance with applicable legal requirements. Select may share a high-level summary of the incident timeline, data impact and resolution taken once confidence has formed around scope, impact and resolution.

4.5 Network, host and endpoint security.

All production networks holding sensitive data has deployed dedicated firewall (AWS security groups), intrusion detection/prevention (IDS), file integrity management systems, systems hardening (CIS), and other network security technology in the operation of systems and facilities. Workstations will have anti-malware software deployed, updated from the point of purchase.

5. PII and PAN

Personally Identifiable Information (PII) are protected to industry compliance levels and/or legislative compliance levels in the regions whe re Select operates.

Dedicated systems and procedures include but are not limited to:

- industry level encryption in transit and at rest where appropriate
- network intrusion detection
- network segmentation
- file integrity management
- key, password management
- application level firewall restrictions
- limited role based access
- events monitoring and detection
- security breach and incident management