Super Concepts

Information Security and Privacy

Fact Sheet

Contents

1. Information Security

The three main objectives of information security are at SuperConcepts are;

- **Confidentiality**: Information must be accessible only to those authorised to view it;
- **Integrity**: Information must be accurate and complete to utilise it or make business decisions based on it;
- **Availability**: Information must be available when the business or client requires it.

At SuperConcepts we operate and manage our own IT Infrastructure on private servers in Australian Data Centres where it remains under our control. We do not outsource the management of our infrastructure or services to third parties, and we only use Public Cloud based facilities that retain information within Australia.

1.1 Security Controls Overview

SuperConcepts use an Information Security Management System as part of our ISO 27001 responsibilities which comprises of many Information Security controls to protect your data from unauthorised access.

On request we are happy to discuss these in more detail with you if you have specific queries around the controls.

- CREST certified Penetration Testing.
- Intrusion Detection and Prevention Systems
- Network segregation and Firewalling
- Staff security awareness training and education
- Encryption in transit and at rest of all confidential information.
- Data Loss prevention and protection
- System High Availability and Data Centre failover
- A defense in depth approach using multiple global vendor security solutions.
- Properly tested and audited disaster recovery
- Threat hunting and vulnerability monitoring and detection on all critical systems
- Least privilege access to all production systems.
- System monitoring, alerting and remediation on all system metrics 24/7

We are continually updating our security practices based on industry best practice and emerging threat knowledge. SuperConcepts participates in a number of industry events to help keep abreast of the latest trends, and we adjust our Information Security Objectives annually to stay ahead of threats and the latest tools and controls.

1.2 ISO 27001 and SOCII certifications

SuperConcepts has been awarded ISO 27001 certification – an international standard defining best practices on how companies should implement, maintain, and improve information security practices.

This accreditation applies to our SuperMate software environment as well as core information technology controls across the wider SuperConcepts. ISO 27001 is now mandated by the ATO to connect directly to their systems, something only a small number of providers have achieved in the Administration market.

SuperConcepts has been audited against the Trust Service Criteria defined by the American Institute of Certified Public Accountants, and now more widely adopted internationally. Our SOC 2 covers the SuperMate hosting environment including our data feed environment, testing the controls that underpin the security, availability and process integrity of our systems and data.

1.3 Privacy

We take the privacy of you and your client's information extremely seriously at SuperConcepts. We have several staff who are dedicated to the security and privacy of your information including:

- An IT and Security Manager responsible for our networks and infrastructure security
- A Risk and Compliance Manager responsible for our risk frameworks, regulatory compliance and
- An Operation Risk and Compliance Committee
- An Information Security Management Committee
- An Incident and Breach committee

Our Privacy Policy is available on the Internet and can be found here: https://www.superconcepts.com.au/container/privacy. The policy is based on the relevant provisions of the Privacy Act and the Australian Privacy Principles.

1.4 Third Party Security Assurance

Vendors in respect of the provision of IT services are managed via our Information Security Management System including annual audits of vendors and management of any remediation activities to uplift their security processes in-line with best practice.

SuperConcepts operates an ISMS committee that has oversight of vendor due diligence conducted for IT service providers and approves the risk rating applied for each vendor due diligence presented to the committee

1.5 Information Security Awareness

SuperConcepts has various awareness activities aimed to educate staff and to make sure staff are informed on their responsibilities and obligations.

All staff reaccredited yearly on the following modules:

- Privacy and Data protection.
- Privacy and Information Security Awareness.
- Code of Conduct and consequence management
- Incident, issue, and Breach management.
- Preventing Financial Crime.
- Conflicts of Interest training.

On top of this various Phishing Simulation tests are carried out over the course of the year to test our staff's ability to spot and report malicious email.

2. Data Handling and Management

Your personal Information is one of your most important assets and at SuperConcepts we treat your data security as our most important Information Security objective.

2.1 Data Sovereignty

Your data is only ever stored on Australian shores and within SuperConcepts owned Infrastructure. Our Supermate software uses SuperConcepts owned and operated systems that are housed in the state of the art iSEEK data centre facilities in Sydney and Brisbane.

2.2 Who has access to my data?

SuperConcepts is the sole custodian of your data on you and your client's behalf. Only SuperConcepts staff and in some occasions contractors who have been through a rigorous background checking, contract and Non-Disclosure process have access to your personal information. We do not pass your data to 3rd party marketing or statistical analysis companies and we always know exactly where your data is. Whilst your data is stored by us, it is covered by our Privacy Policy which adheres to the Australian Privacy Principles.

2.3 Data loss protection

SuperConcepts backs up all data to encrypted disk, SAN and tape systems on a nightly basis and has the ability to roll back to these backups quickly if required. Additionally, we take high availability snapshots of the data every two hours to facilitate a rapid on-site recovery if needed. These snapshots are stored locally within the primary Data Centre.For rapid Disaster Recovery, we replicate your data in near real-time between our two Data Centres, geographically separated (Brisbane and Sydney). We keep one local replication in the primary Data Centre to facilitate rapid recovery from hardware loss, and a remote replica in our secondary Data Centre to cover a loss of connectivity to the primary Data Centre.

We regularly test disaster recovery processes and the ability to recover your data in the event of a serious hardware or system failure.

Backups are encrypted to tape and stored in a secure storage facility and managed by Iron Mountain Pty Ltd. Iron Mountain specialise in the secure transport and storage of backup data. We do not store any backup data remotely on public Cloud systems.

3. System and Data Availability

Data must be available to both clients and to the business to properly function and make up to date business decisions based on it. To this length SuperConcepts has a layered system availability model that means your data will always be available to you when you need it.

3.1 System Resiliency

SuperConcepts uses a combination of technologies to provide the absolute best uptime on our server, switch and router systems.

- Our state of the art SANs (storage area networks) can survive multiple disk failures and hardware failures within itself and continue to operate with no performance hit. We snap shot data locally on the SAN to allow rapid recovery or restore as required.

- Dual network path servers provide redundancy against core switch failure and network card failure. The system has dual paths to the internet and internal networks and can continue to function if one fails.

- SuperConcepts uses High availability firewalls at all locations. These provide protection against a core router failure with no downtime or performance degradation. They also support patching without interruption of traffic flow.

- Virtual Server VMotion technology means in the case of a full server host failure our servers will move automatically to another available host instantly. This ensures little to no downtime for hardware failures.

3.2 Data Centre Resiliency

The iSEEK data centres are state of the art hosting facilities which offer controlled video and guard monitored entry points, formal induction procedures and 24/7 environment monitoring amongst other benefits.

SuperConcepts uses these facilities in Sydney (Gore Hill) and in Brisbane (Brisbane Airport Precinct) and these data centres are connected for us by a private high-speed network link. This allows us to do critical data replication from one site to the other giving us resiliency in the case of a full data centre closure or disaster.

3.3 Network Resiliency

Our upstream provider iSEEK has a managed multi-path redundant network to the internet meaning that a core internet failure at any level can be rectified by moving to another providers link. iSeek supports routing traffic via multiple Tier 1 telecommunications providers.

3.4 Monitoring and Response

SuperConcepts uses multiple monitoring systems to monitor system metrics, uptime and performance on all our systems. Alarms are triggered and available visibly via a monitoring dashboard, delivered by email to the network ops team and for critical issues via SMS to our senior engineers. Alarms are triggered if a metric falls outside the baseline set for it or if it becomes unavailable or degraded in any way.

In addition to core system monitoring we also do security incident and event monitoring and threat hunting on all systems within our networks.

SuperConcepts continually monitors the load on our servers and takes proactive actions to ensure our operations are running efficiently.

3.5 Our Operations Team

SuperConcepts has a dedicated IT Security and Operations team that is responsible for the operation of our systems and the security of your data. Our core staff include:

- A dedicated IT and Security Manager with complete oversight and responsibility for IT Management
- A dedicated Operations Team who monitor and manage our systems
- A Network Administration Team who build and maintain our network and hosting facilities
- A dedicated Support Team who are the primary point of contact for our clients
- An internal Support Programming team who focus on rectification of issues as they arise

Further information

CALL
1300 023 170

EMAIL
enquiries@superconcepts.com.au

VISIT
superconcepts.com.au

Subscribe to SMSF news & insights: superconcepts.com.au/subscribe

SCFS-ISP-20210804