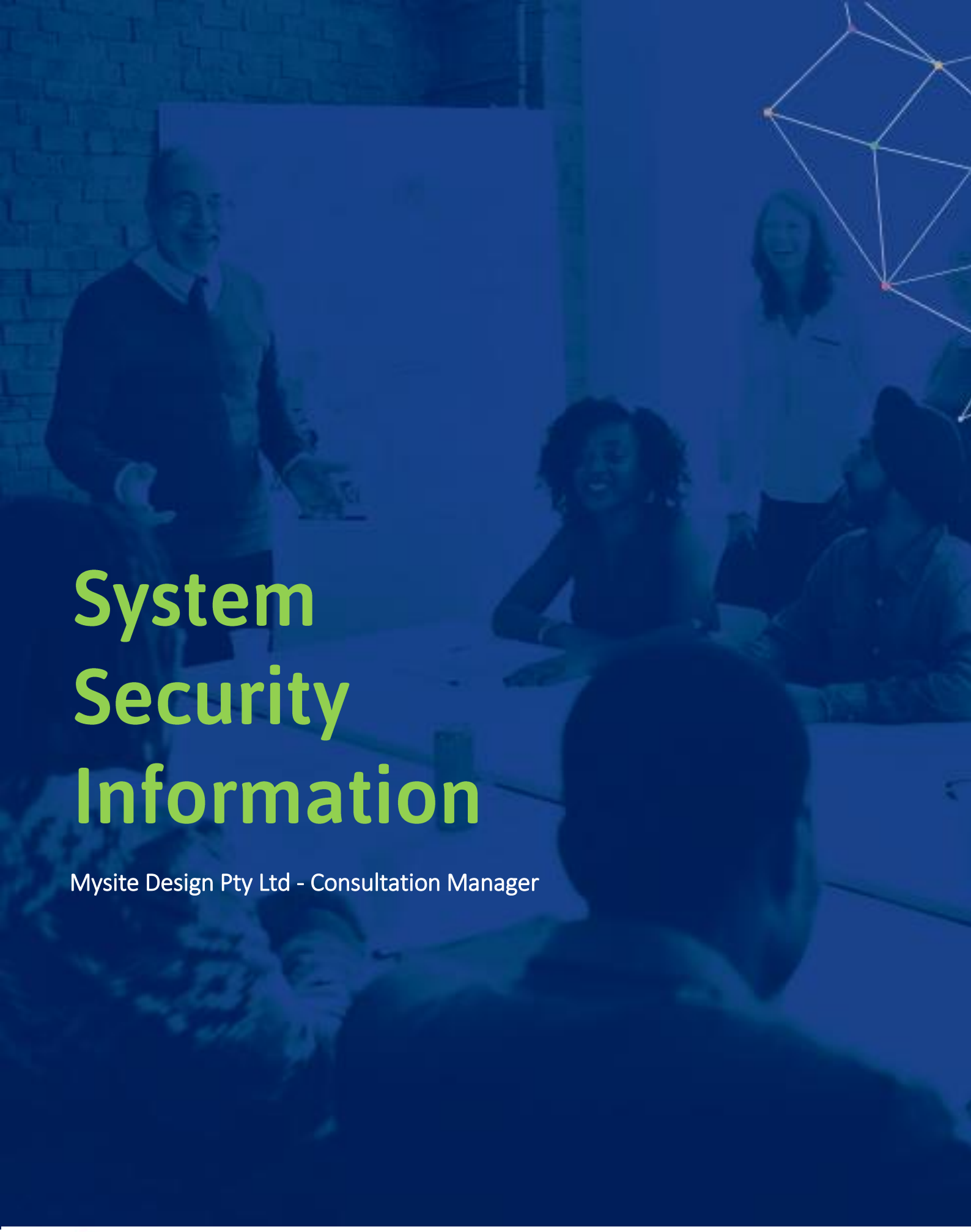


System Security Information

Mysite Design Pty Ltd - Consultation Manager

Consultation Manager
P 1300 850 058
E enquiries@consultationmanager.com

PO Box 1217
New Farm, QLD, 4005
W consultationmanager.com

CONSULTATION MANAGER

Contents

Overview and System Architecture

Consultation Manager is a secure web-based application that runs on 64 bit Microsoft Windows Server 2008 R2 and 64 bit Microsoft SQL Server 2008 R2. These technologies are industry-leading, Enterprise class applications and are capable of handling very high volumes of data quickly and securely.

All access to Consultation Manager is conducted via 256 bit Secure Sockets Layer (SSL) security, ensuring all data is encrypted in transit. Users access the system via unique username and password combinations.

MySite's servers are stored in a secure, climate-controlled facility and can only be accessed by authorised technical staff with photo identification. MySite's servers are firewalled and port access is tightly controlled by IP Address access lists.

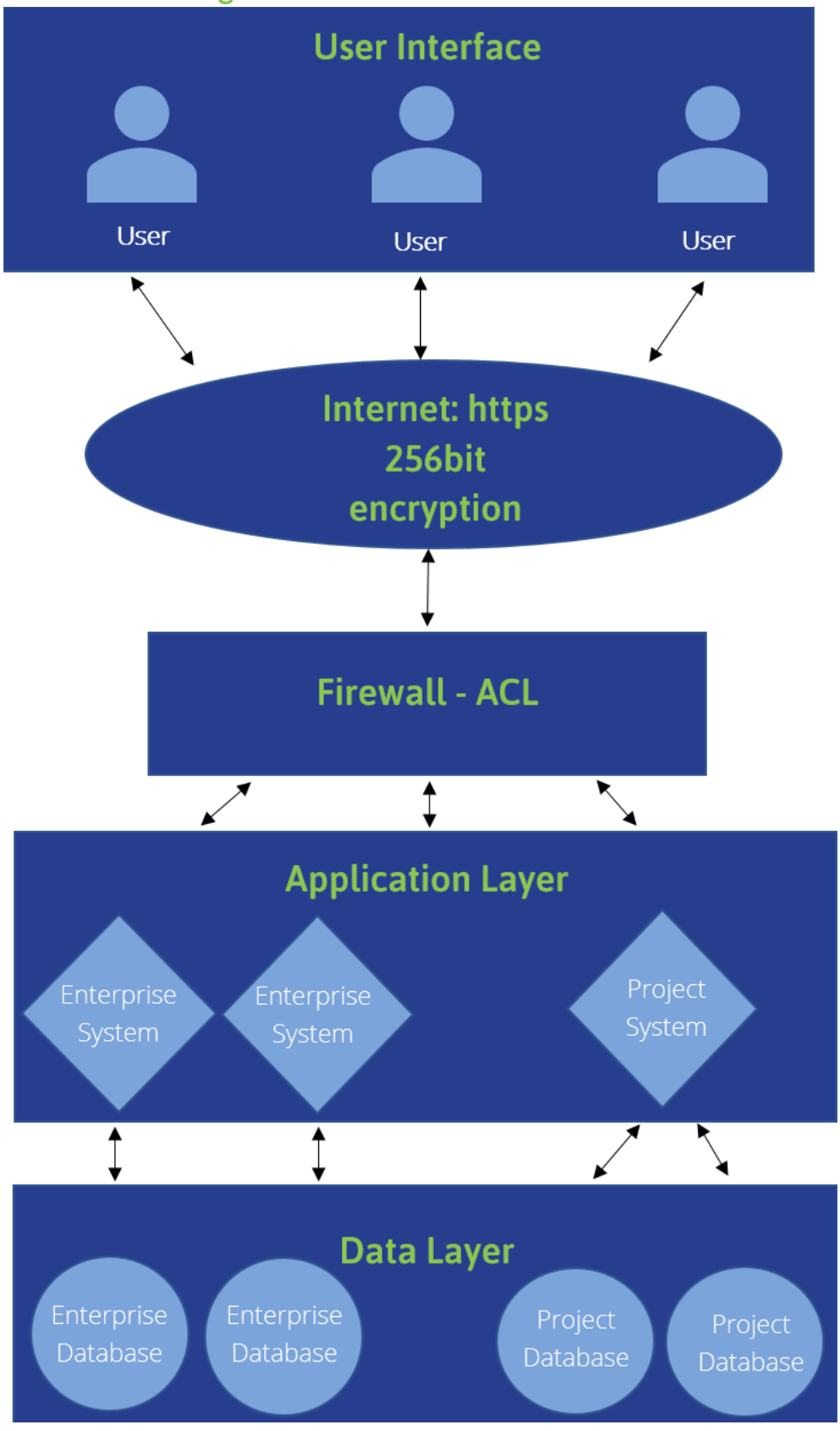
All project data is stored in a database file unique to your Enterprise and this database file is backed up to disk every hour. Database files, documents, application and system files are backed up in an encrypted state via SSL connections to offsite facilities to guard against major disasters, including complete loss of a server facility. MySite also runs daily backups of all data via tape. Tape backups are stored on-site for up to 7 days and offsite for one year.

MySite's servers rely on a robust, completely virtualized and high availability hardware environment. They are connected to the internet via high speed links ensuring rapid application response. MySite's servers have a high level of redundancy including redundant Fibre Channel SAN, high availability, VMware virtualization hardware clustering including redundant power supplies, supplied by discrete feeds.

Wherever possible, data is exchanged using AJAX (Asynchronous JavaScript and XML) technology and sophisticated caching routines, which act to minimise the volume of data being transferred over the web, significantly enhancing performance of the system.

Consultation Manager's availability is continually monitored locally and remotely giving you the added assurance that your application will be performing at its peak at all times.

Architecture Diagram



Servers

Consultation Manager applications are hosted on VMWare ESX 5.1 virtual infrastructure with dynamically scalable processor and RAM capability. They are configured to run well within hardware limitations (capacity planning is proactively monitored).

Data Centre

Consultation Manager's Australian Servers are located in Global Switch IDC, Pyrmont Sydney. GS IDC is a Tier 3 facility.

Global Switch Sydney infrastructure details:
http://www.globalswitch.com/en/infrastructure

Network Connectivity

In addition to active SAN and VMware redundant infrastructure, MySite provides a business continuity plan via replication of data to a geographically diverse offsite facility. MySite believes this level of risk is more than adequate to comply with industry risk standards with respect to availability and business continuity.

- Dual Fibre Feeds with Redundant Fabrics
- Access to Most Tier 1 and IX Providers
- Carrier Neutral
- Shared Burstable Network
- Dual Load Balanced Cisco ASR1K Routers and Cisco Switches
- Data Transit: Optus, Verizon, Asia Netcomm, Pacific Internet, Uecomm, Pipe Networks

System Security and Availability

Data Centres

Access to servers is restricted to registered technical staff with photo identification. Access is controlled using proximity card readers and monitored via CCTV cameras.

Firewalls

MySite uses redundant hardware firewalls. Access lists are tightly controlled – only ports 25 (smtp), 53 (dns), 80 (http), 443 (https) and 465 (secure smtp) have unrestricted access. A minimal set of ports are made available for administrative and network access purposes and such access is permitted only to a short list of IP addresses.

HTTPS Encryption

All Consultation Manager applications are encrypted using 256 bit SSL (required).

Email Encryption

All Email traffic emanating from Consultation Manager attempts TLS / SSL connections if available at the receiving server.

Password Rules

At the application level, password rules can be set on a client by client basis as follows:

- Minimum characters
- Name and username disallowed
- Password expiry days
- Must change password on first login
- Can't use previous (x) passwords (default is 3)
- Custom regular expressions to require non-alphanumeric characters, at least one capital letter, etc are available
- Access to the application is suspended following 3 unsuccessful password attempts.

In the event of an account lockout, access can be re-enabled by users with Team Leader permission or by successfully using the 'forgot password' feature in the application which requires a username / email combination.

User Roles

Users are granted roles in the application according to the tasks they need to perform in the application. The standard role definitions are:

Role	Team Member	Data Viewer	Data Entry	Data Editor	Team Leader	Enterprise Admin
View Data, Reports and Documents	•	✓	✓	✓	✓	✓
Edit and add data	•	•	✓	✓	✓	✓
Delete data	•	•	•	✓	✓	✓
Manage team and manage lists	•	•	•	•	✓	✓
Create groups lists	•	•	•	•	•	✓
Create or change Projects	•	•	•	•	•	✓
Make Entities private	•	•	•	•	•	✓
Add new Team Members	•	•	•	•	•	✓

Remote Monitoring

MySite continuously monitors server and application health including infrastructure health and application health. Application, system and security warnings and notifications are sent to development staff, depending on severity.

Application Security: OWASP TOP Ten Response

Cross Site Scripting

- All input data to Consultation Manager is explicitly filtered according to expected data type.
- All output data is appropriately encoded and encoding type is explicitly specified.

Injection Flaws

All GET and POST input to Consultation Manager is explicitly filtered according to expected data type to mitigate against SQL Injection and to prevent scripting errors.

Malicious File Execution

- Folders used for document upload have no execute, script or read permissions.
- Uploaded files have their extensions stripped and filenames obfuscated.
- Uploaded documents can only be streamed to client browsers and not opened or executed.

Insecure Direct Object Reference

- Database keys are used as object identifiers however all database queries are verified to ensure the user has permission to access the object in question.
- Unauthenticated users cannot access any application URLs or documents except for login points and documents that are explicitly marked public.
- Filenames (but not paths) are used as object identifiers however files cannot be directly accessed – rather they are streamed via script.

Cross Site Request Forgery

- IIS7 forms authentication used
- Encrypted Session Cookies (256 bit)

Information Leakage and Improper Error Handling

No application configuration information or error data is available to client browsers, except for sanitised errors generated by the application.

Broken Authentication and Session Management

Consultation Manager uses forms authentication with 256 bit SSL encryption.

Insecure Cryptographic Storage

Stored data is not encrypted however all traffic and all backup transport is encrypted.

Insecure Communications

- All client-server http traffic is encrypted with 256 bit SSL.
- Email traffic is encrypted via TLS / SSL where supported by the receiving server.
- All internal network traffic is via IPSec VPN tunnels.

Failure to Restrict URL Access

- All URL access is restricted to properly authenticated and authorised users.
- All URL access is logged.

Disaster Recovery Plan

Hardware

EVENT	SYSTEM DOWN?	SEVERITY	DATA LOSS	LIKELY DOWNTIME	RESPONSE
FAN FAILURE	No	Low	No	None	*Redundant fans are replaced in hot swap environment by Virtualisation vendor (Server is VMotioned if required)*
POWER SUPPLY FAILURE	No	Low	No	None	*Redundant power supplies are replaced in hot swap environment by Virtualisation vendor (Server is VMotioned if required)*
DISK DRIVE FAILURE	No	Low	No	None	*Redundant FC SAN isolates faulty disk and allows hot swap FC disk replacement*
RAM FAILURE	No	Low	No	Reboot	*RAM is replaced by Virtualisation vendor (Server is VMotioned off affected host)*
NETWORK CARD FAILURE	No	Low	No	Reboot	*Network Card is replaced by Virtualisation vendor (Server is VMotioned off affected host) All hosts feature dual, discrete Network Interfaces.*
FIREWALL FAILURE – CONFIGURATION	Yes	Moderate	No	None	1. Contact managed firewall vendor and

					restore previous working configuration. Firewalls are redundant N+1 throughout the physical environment. 2. Test all applications. 3. Restore access to all applications
FIREWALL FAILURE – HARDWARE	No	Low	No	None	*High Availability firewall to take over and primary hardware is fixed and restored to working state*
MOTHERBOARD/CPU FAILURE	No	Low	No	Reboot	*Motherboard/CPU is replaced by Virtualisation vendor (Server is VMotioned off affected host)*

Software / Data

EVENT	SYSTEM DOWN?	SEVERITY	DATA LOSS	LIKELY DOWNTIME	RESPONSE
OS FAILURE	Yes	Moderate	No	8 Hours	1.New server is provisioned and backups recovered. 2.Test all applications 3.Restore access to all applications
DATABASE CORRUPTION OR LOSS OF DATA	Yes	Moderate	Yes	1+ Hour	1.Take full SQL backups daily and transaction log backups hourly 2.Suspend access to affected application 3.Restore database from last known good state using point-in-time restore in SQL Backup. Row by row restoration of data is also possible. 4.Test in conjunction with client representative to verify data integrity 5.Restore access to application

Data Centre

EVENT	SYSTEM DOWN?	SEVERITY	DATA LOSS	LIKELY DOWNTIME	RESPONSE
LOSS OF POWER TO DATA CENTRE	No	Low	No	None	1.If GS IDC has a power failure of both feeds then the IDC will seamlessly switch to generator power and can operate indefinitely from diesel DRUPS. See GS IDC technical specification information.
LOSS OF NETWORK CONNECTIVITY	No	Low	No	Up to 30sec (BGP convergence	Multi-homed upstream providers provide BGP routing redundancy
COMPLETE LOSS OF SERVER	No	Low	Yes (1 hour max)	24 hours	1.New server is provisioned and backups recovered. 2.Test all applications externally 3.Restore access to application
LOSS OF DATA CENTRES	No	Low	Yes	48 hours	1.In the event of complete loss of both Data Centres, servers can be rebuilt from geographically isolated backup facility. 2.Sites will be tested and confirmed with customers. 3.Roll back after outage will be coordinated with customer

Backup Procedures

Database Backups

MySite runs daily full database backups (to disk) and hourly transaction log backups (to disk) on all Consultation Manager databases. Backups are facilitated using RedGate SQL Backup (www.red-gate.com) which is considered superior to native SQL Server backup both in terms of performance and compression – allowing more frequent backups without a noticeable loss of application performance. SQL Backup also allows very fast, point-in-time restores.

Disk Backups

MySite runs daily backups of all data via tape. Tape backups are stored on-site for up to 7 days and at offsite for one year.

DR Backups

Databases, applications and client documents are replicated to a remote facility through an encrypted channel on a daily basis to guard against loss of both primary facilities.

Escrow

MySite does not currently have escrow arrangements in place as this has not been requested by clients in the past. We are open to working out such arrangements at the clients' expense.

Administrative Access

Administrative access is only available on a permanent basis to senior developers. All administrative access is IP address specific.

Penetration Testing

Consultation Manager proactively mitigates the potential for security breaches with annual penetration testing. MySite are willing to work with clients to facilitate additional penetration testing at the client's expense where requested.

ISO Accreditation

CM has 2 ISO accreditations. ISO 2001:2013 (Information Security) and ISO 9001:2015 (Quality Management). Both are international security standards specifying management best practice. To become certified to these standards, and to continue to keep our certifications, we must:

- systematically evaluate our security risks.
- demonstrate how our information security controls address these risks.
- continuously review our practices to ensure that our information security controls continue to address these risks.
- have our information security practices audited annually and verified by an independent auditor.

Data Sovereignty

All data is stored and processed in Australia.

Privacy

We are acutely aware of the sensitive nature of your data. Our staff do not access your data unless explicitly instructed by you in the context of user training or support. Our Privacy Policy is available at consultationmanager.com