Consultation Manager Systems Security Document

Mysite Design Pty Ltd

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

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

CONSULTATION MANAGER

Contents

Application Security

Application Overview

Consultation Manager is a secure web-based application hosted on Microsoft's Azure Cloud platform. Utilising industry-leading technologies, we deliver an enterprise class application which is 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 with the option for Federated Authentication including Single sign-on.

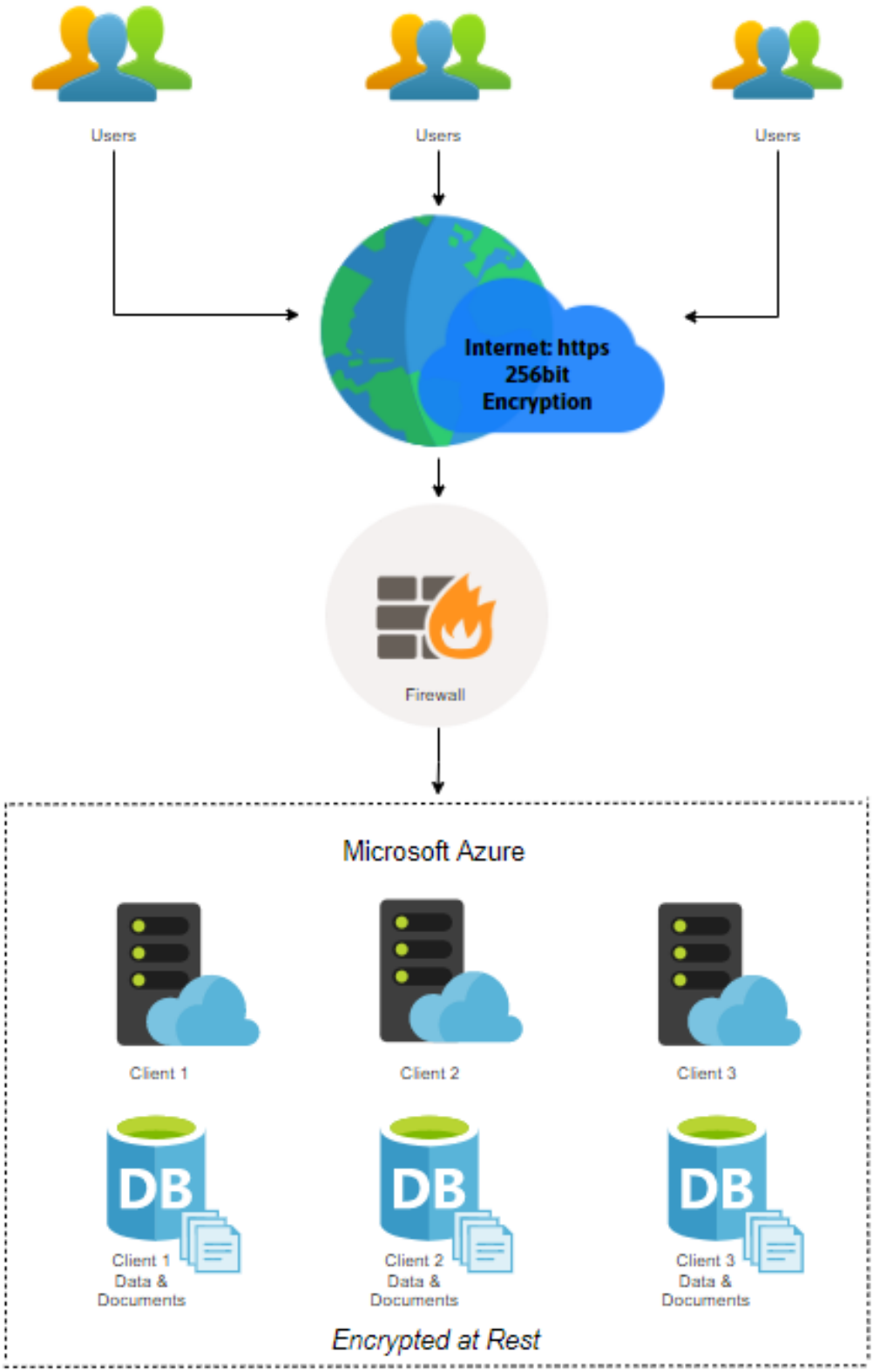
All project data is stored in isolated storage areas unique to your Enterprise and this information is backed up on a regular schedule. Database files, documents, application and system files are backed up in an encrypted state to mitigate major disasters, including complete loss of a server facility.

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

Location: Servers and Data Centre

Consultation Manager is hosted on Microsoft Azure Cloud infrastructure. Our servers are hosted on a Tier 4 data centre located in the Australia East region. Anonymised telemetry information is stored in Loggly. We deploy in a multi-instance configuration to provide fault tolerance and high availability.

Architecture Diagram



Data Centers Security

Physical access to servers is restricted to registered technical staff with two-factor biometric identification. Further information can be found here: https://docs.microsoft.com/en-us/azure/security/azure-physical-security. Thoroughly vetted Consultation Manager Senior Developer staff are the only personnel who have virtual access to the servers.

Firewalls

Consultation Manager uses Microsoft Azure's provided firewall infrastructure. Access lists are tightly controlled – only port 443 (https) is publicly accessible.

HTTPS Encryption

All Consultation Manager applications are encrypted using 256-bit SSL.

Email Encryption

Email traffic originating from Consultation Manager is transmitted securely using TLS / SSL connections.

Password Rules

At the application level, password rules are defined as:

- 10 characters minimum
- At least one upper case character
- At least one lower case character
- At least one number or symbol character

Data Ownership

Your organisation always owns the data that you store in Consultation Manager. If you ever wish to obtain a Project backup, please contact your account manager or our Customer Success team, and we will work with you to provide this.

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 Injections 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.

Cross Site Request Forgery

JWT Bearer tokens are used for user access controls along with appropriate Cross Origin Resource Sharing (CORS) and Access-Control HTTP headers.

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 JWT bearer token authentication transmitted over 256-bit TLS encryption.

Insecure Cryptographic Storage

Data is encrypted at rest and in transit using cryptographic encryption mechanisms. These include Service-managed transparent data encryption for data at rest and TLS using 256-bit certificates for data in transit.

Insecure Communications

- All client-server http traffic is encrypted with 256-bit SSL.
- All email traffic sent via CM is encrypted via TLS/SSL.
- All internal network traffic is via the Microsoft Azure network infrastructure.

Failure to Restrict URL Access

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

Disaster Recovery Plan

Consultation Manager uses Microsoft Azure Site Recovery facilities to protect against data loss and ongoing service interruption. In the event of full data centre loss, the Consultation Manager platform can be restored from a recovery vault to restore system access. For further information, please visit the following link: https://azure.microsoft.com/en-au/services/site-recovery/

Backup Procedures

Data Backups

CM does support point-in-time restore (PITR) by automatically creating full backup, differential backups, and transaction log backups. Full database backups are created weekly, differential database backups are created every 12 hours, and transaction log backups are generally created every 5-10 minutes, with the frequency based on the amount of database activity.

Document Backups

Documents, Reports and Import data are backed up daily. All backups are retained for a 52-week period and stored in the Disaster Recovery Vault within Azure, which is stored in multiple locations.

Identity Management

User Roles

Users are granted pre-defined permission roles according to the tasks they need to perform in the platform. Permissions are provided by the Enterprise Administrators of the system. All users will need to have a user capability and a team permission to access data in the system.

User Capability	Enterprise Administrator	Standard User
Import Data	✓	
Batch Update Data	✓	
Manage Projects	✓	
Create Users	✓	
Manage Users	✓	
Manage Classifications	✓	
Report Creation	✓	✓
Report Generation	✓	✓

Team Permissions	Team Leader	Editor	Contributor	Viewer
Manage Team	✓			
Restore	✓			
Delete	✓	✓		
Relate	✓	✓	✓	
Unrelate	✓	✓	✓	
Modify	✓	✓	✓	
Create	✓	✓	✓	
View	✓	✓	✓	✓

Audit and Accountability

Audits of user access and roles can be performed by the Enterprise Administrator of the system. It is the responsibility of the Enterprise Administrator to revoke access to users who have left the organisation or no longer require it. Consultation Manager will not grant or revoke access to users unless explicitly expressed in writing by our Key Contact of the Enterprise.

Privacy

We are acutely aware of the sensitive nature of your data. All Consultation Manager staff sign a Confidentiality statement and have police checks performed upon commencing employment. To ensure we provide the best support we can, Consultation Manager has a user profile to access each Database. CM 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

Accreditation

ISO Accreditation

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

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

System Security Controls

Risk Assessment

We review our risk assessment and risk management plan annually in line with ISO requirements to systematically identify the liabilities and opportunities which would impact our business and infrastructure. This risk assessment encompasses all departments to ensure optimal improvement and pre-emptive risk mitigation across the entire company.

Incident Response

All Incident Rectification Targets quoted are based on a target that faults will be rectified, or services restored within the defined time in 95% of all incidents of that type. Regardless of the target, all work to rectify faults and restore services will be done as fast as reasonably possible. Modifications, upgrades, development and configuration of the Consultation Management software will occur continually. However, the work to restore and fix the application will have priority at all times.

Severity	Definition	Example
Critical	An incident that impacts on the ability of the organization to conduct business. The problem if unresolved will continue to have an adverse effect on production/operations and/or safety.	Application unavailable
High	An incident that has the potential to impact the ability of the organization to conduct business.	Critical feature or function not working
Low	An incident that has an effect on operations but does not halt the ability for the organization to conduct business.	Minor feature or function not working at all
Minor	An incident that does not impact operations or halt the ability for the organization to conduct business.	Minor feature or function not working optimally

Incident Class	Target Fix Time
Critical	4 hours
High	1 day
Low	1 fortnight
Minor	1 month

All security incidents are logged in CM's internal incident register and reviewed yearly to formulate process improvement. All security breaches must be reported to the Customer Success team at Consultation Manager immediately to ensure a prompt response. In the unlikely event that a verified security breach has occurred CM will follow the steps provisioned in the Australian Privacy Act 1988 as well as the Privacy Amendment (Notifiable Data Breaches) ACT 2017.

Remote Monitoring

MySite continuously monitors application and platform health. Application, system and security notifications are sent to monitoring staff based on preconfigured severity levels.

Vulnerability Testing

Consultation Manager perform annual Vulnerability testing to proactively mitigate the potential for security breaches. All vulnerabilities raised from these tests are rectified within a 30-90-day period depending on a level of priority.

System Maintenance

All system maintenance and feature upgrades are performed out of office hours to ensure no user is affected. Critical hot fixes of the system will be performed when needed, however should not affect users due to the multi-instance configuration.

Awareness and Training

All Consultation Manager staff are subject to Police checks and are trained in security awareness which encompasses all aspects such as security policies, data classification, workspace security, data communication security, social engineering awareness and incident response procedures. This training is held at the induction of all staff members and refreshed yearly.

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.