Service & Security Data Sheet

Updated March 7, 2022 (Revision Summary)

Table of Contents

iManage Cloud Overview

The iManage Cloud is a comprehensive cloud service (SaaS) for delivery of iManage's best-in-class professional work product management solution.

Since 1995, thousands of professional organizations have licensed and benefited from iManage's industry-leading suite of products for work product management. Now, as these organizations look to the cloud to help them eliminate complicated on-premises deployments of enterprise software, streamline operations, and improve ROI, they can subscribe to the iManage Cloud. Here they will have access to the powerful and familiar iManage solutions without the need for in-house implementation of back-office infrastructure. They find that their subscription to iManage Cloud provides a level of service that would have been cost prohibitive to implement on their own, with increased security, disaster recovery and performance.

The iManage Cloud makes the iManage work product management solution available to new customers as well. These are customers of all sizes for whom an on-premises software deployment was not possible. With a subscription to the iManage Cloud they reap the benefits of the industry leading solution for work product management, with the security, scalability, and performance typically available only to large organizations with big IT departments.

Our cloud service is a scalable multi-tenant solution built on a secure, high-availability, modern platform. A shared infrastructure provides core services like metadata storage and management, file services, preview, and OCR while the application architecture provides logical separation of data.

Access to the iManage Cloud is available via an HTTPS connection using a lightweight HTML5 web application, with optional desktop and mobile apps that provide for integration with key desktop productivity applications for Windows and iOS such as Microsoft Office. The mobile application can be further secured with mobile device management solutions (MDM).

This data sheet provides details about the architecture of the iManage Cloud and is intended to assure you that data stored in the iManage Cloud is highly secured and in compliance with modern industry security standards.

Service Offerings

The iManage Cloud offers a suite of services centered around our core work product management platform iManage Work. The security details provided in this data sheet are based primarily on this core platform.

iManage Cloud add-on services may provide an additional level of application security or utilize different architecture, but all products are implemented to meet the security levels defined within this data sheet.

Add-on services include, but is not limited to:

- **iManage Security Policy Manager**: An iManage Cloud Service which allows for the creation of ethical walls which can be applied to the iManage Work repository.
- **iManage Threat Manager**: An iManage Cloud Service which uses machine learning to detect and alert administrators to suspicious activity within the iManage Work repository which may suggest a data breech or theft.
- **iManage Share**: An iManage Cloud Service for collaborative sharing of content which originates in the iManage Work repository. A security data sheet for content stored within iManage Share is available upon request.
- **iManage Records Manager**: An iManage Cloud Service for governing both paper records and electronic content stored with the iManage Work Repository.

Data Centers

The iManage Cloud is available in eight regions across the globe. Each regional implementation consists of a primary and secondary data center.

Region	Primary Data Center	Secondary Data Center	Data Center Owner
United States	US Central (Illinois)	South Central US (Texas)	Microsoft Azure
Canada	Canada Central (Toronto)	Canada East (Quebec City)	Microsoft Azure
Brazil	Brazil South (Sao Paulo State)	South Central US (Texas)	Microsoft Azure
Continental Europe	West Europe (Netherlands)	North Europe (Ireland)	Microsoft Azure
United Kingdom	UK South (London)	UK West (Cardiff)	Microsoft Azure
Australia	Australia East (New South Wales)	Australia Southeast (Victoria)	Microsoft Azure
Asia Pacific	Southeast Asia (Singapore)	East Asia (Hong Kong)	Microsoft Azure
Japan	Japan East (Tokyo, Saitama)	Japan West (Osaka)	Microsoft Azure

All Microsoft Azure data centers are provisioned in Azure regions supporting Azure Availability Zones. Availability Zones are physically separate locations within an Azure region that provide discrete power, networking, cooling and are tolerant to local failures such as fire floods or earthquakes and support provide low-latency communication between zones. All infrastructure is managed and deployed via code on based upon a container orchestration platform. All iManage cloud services are distributed across Availability Zones to ensure that iManage can continue to provide service even if up to two zones are compromised. Microsoft itself does not have access to the iManage Cloud nor to the customer data in the iManage Cloud.

All facilities and cloud services have been thoroughly vetted by iManage Operations and Security Personnel to ensure they meet necessary security and redundancy standards.

Data Domicile

The data associated with a specific customer account will be hosted within one of these regional implementations, ensuring that data domicile is clear. The customer account and its associated data (including backups) will remain within the regional implementation defined within the agreement unless the customer requests a change of venue. Customer contain is automatically and asynchronously replicated to a paired Azure region via Azure's Geo-Zone Redundant Storage (GZRS) service.

Disaster Recovery

Each Azure region offers a region pair within the same geography (such as Europe or Asia). In the unlikely event of a catastrophic disaster sufficient to render all three Availability Zones in the primary region inoperable, iManage would programmatically redeploy all cloud services to the paired regional center and would resume services within the contractual RTO. Customer data is asynchronously replicated between regional pairs and iManage is able to restore access to customer data within the contractual RPO.

Certification and Compliance

All iManage Cloud data centers are validated against the SOC 2 criteria and ISO 27001 controls.

Audits are conducted annually to ensure continued compliance with these standards. Each audit includes assessment of the control objectives and activities set forth by these standards, including controls over information technology and related processes.

Data Center Certification documents can be provided for the data centers of interest. You can request these documents from your account representative if they have not already been provided to you.

Regional Data Center	Available Certification Documents
United States	Azure SOC 2 Type II Report Microsoft Azure ISO 22301 Certificate Microsoft Azure ISO 27017 Certificate Microsoft Azure ISO 27018 Certificate Microsoft Azure ISO 27701 Certificate CSA STAR Certificate
Canada	
Brazil	
Continental Europe	
United Kingdom	
Australia	
Asia Pacific	

Japan	

Annual ISO 27001 audits are conducted for the iManage Cloud in the first quarter of each calendar year. This certification covers the management, operation, and maintenance of the information assets and information systems that support the iManage Cloud, providing for confidentiality, availability, privacy, security, and integrity of iManage customer data during storage, processing, and delivery.

ISO 27001
Information Security Management System
CERTIFIED

SOC 2 Type II
Service Organizations Controls
REPORT

Our annual SOC 2/SOC 2+/SOC 3 audits are also conducted in the first quarter of each calendar year. Such third-party certification confirms that iManage Cloud has the controls and safeguards in place to securely host and process customer data.

The iManage security and compliance program is certified and independently audited to the following standards and frameworks.

- ISO 27001
- ISO 27701
- ISO 27017
- ISO 27018
- ISO 22301
- SOC 2 Type 2 (All Trust Principles: Security, Availability, Confidentiality, Integrity & Privacy)
- SOC 2+ (includes select NIST 800-171 controls)
- SOC 3
- CSA STAR Level 2

Refer to http://imanage.com/security for the most current list of certifications.

Network Security

Application Access

Access to the iManage Cloud Services is provided via a secure HTTPS connection. Data is protected in transit using the TLS 1.2 protocol for authenticated and encrypted communication. The encrypted communications utilize an RSA-2048 key-exchange.

Industry standard best practices are implemented to restrict access to backend components and ensure that public facing web servers maintain the highest security ratings. These practices include, but are not limited to:

- Implementation of zero-trust network architecture principles
- Implementation of firewalls and proxies with monitoring to detect hostile activity
- Internal segmentation utilizing common application security methodology
- Separation between production, development, and testing environments
- Full segregation between iManage Cloud and iManage Corporate networks

In addition to regular internal monitoring, iManage conducts annual penetration tests through an independent third party.

Testing is conducted in the first quarter of each calendar year, testing is based on NIST SP 800-115 and NIST 800-53 standards. An executive summary of the scope and the results of this test can be provided on request.

System Network Access

The iManage Cloud services are delivered on a dedicated, independent network that is isolated from all other networks including those used for development, testing and iManage internal IT networks. Access to the production network for each regional implementation requires VPN authentication with 2-factor authentication and a valid digital machine certificate.

Access to the production iManage Cloud network is restricted to individuals who are tasked with operation and deployment of the production services. Authentication with a unique user ID is required. Once authenticated, access to the services is determined based on user role and provided on a "need to know" basis.

Security Information and Event Management (SIEM)

The iManage Cloud utilizes Splunk Enterprise for unified log management and archiving for 1 year. Host system event logs (e.g., system event log, non-iManage application logs and network logs) are ingested and analyzed to detect potential threats.

Dynamic Application Security Testing (DAST)

The iManage Cloud performs continuous dynamic application security testing (DAST) using a high-quality industry standard DAST provider. The DAST provider connects to the iManage Cloud and conducts fuzzy testing and deep application scanning to identify potential vulnerabilities that could result in data loss. Test algorithms are continually updated to test against newly discovered vulnerabilities.

Data Ownership

With the iManage Cloud, the customer retains sole and exclusive ownership of their data. The iManage Cloud Services Agreement (a sample is available here), specifies the terms governing the ownership and handling of confidential data, unless superseded by an alternative agreement between iManage and the Customer. The customer managed encryption key (CMEK) service discussed in the Data Encryption section below allows additional control of ownership by allowing the customer to control the encryption keys used to encrypt their data.

Data Encryption

The iManage Cloud encrypts all iManage Work documents at rest using AES 256-bit encryption. At rest encryption is mandatory for all data storage, including storage volumes supporting operating systems, backup, and recovery systems.

All customer content in the iManage Cloud is encrypted by default. At minimum, data at rest is encrypted via volume-level encryption. Content stored in iManage Work provides higher levels of encryption ensuring that every version of every file stored in Work is ***individually*** encrypted at rest with a randomly generated encryption key, and that each encryption key is securely wrapped with a higher-level key, thereby providing a highly granular encryption model for added data security. iManage Work additionally provides an add-on option that enables the customer to assume ownership of the primary encryption key ("CMEK") used to encrypt their content. It also provides the customer with the ability to revoke the CMEK, thereby ensuring that data stored in the iManage Cloud cannot be decrypted.

With CMEK the customer has complete and exclusive control of the primary key. The key is setup by the customer in a third-party key management service. iManage never receives or stores a copy of the customers encryption key. Currently, the supported third-party service provider is Microsoft Azure Key Premium Vault which supports HSM-backed keys and is

FIPS 140-2 Level 2 compliant. The customer will configure their iManage Cloud environment to connect to this third-party service provider using their company-specific private credentials. A data sheet on CMEK is available for customers who are interested in learning more about this option. Please inquire with your Account Representative.

Data Segregation

iManage Cloud Services are delivered by a shared infrastructure, but customer data is logically separated by various access controls and validation mechanisms:

- Logical content segregation via unique per-customer encryption key hierarchy in accordance with NIST best practices
- Logical metadata segregation by customer ID for metadata storage
- Independent tenant administrative functions
- Containment Security Model
  - Highly granular security model with independent security access down to the document version level
  - Ability to require filing of documents and emails to a container
  - Refiling service to ensure document and email access aligns to the container where required
  - Users outside of the schema/library with access to content are easily recognized and can be blocked
  - Integration with iManage Security Policy Manger to govern access by client or matter/engagement
  - Integration with iManage Share to provide a clear distinction with content shared with external collaborators and that which is visible to internal collaborators.

Data Safeguarding Practices

User accounts used to access the iManage Cloud contain only the following information about the user:

- User First Name
- User Last Name
- User Email Address (required)
- Location (optional)

No other Personally Identifiable Information (PII) is necessary for access to the iManage Cloud

iManage Cloud can support your obligations required by HIPAA at the product, platform, and organization level in a variety of ways including, but not limited to:

- Strict employee security policies and procedures in alignment with ISO 27001 requirements
- Restricted physical access to production servers
- Formally defined breach notification policy
- Encryption of data in transit
- Encryption of data at rest
- Built-in application access controls like account lockout
- Ability to grant/deny access to documents
- Multiple optional folder access rights to provide granular user access to folders
- Audit trail of account activities on both users and content
- Restricted employee access to customer data files
- Defined disaster recovery procedures

- Company (account) level limitations for who within the account can create and manage user accounts.
- The ability for company (account) level administrators to revoke user accounts.
- User account level limitations for who can grant the ability to access, modify, and delete content
- User synchronization from an LDAP repository to ensure timely revocation of user accounts.
- Group synchronization from an LDAP repository to alignment of access to content to job function
- Support for SAML 2.0 Single Sign-on and OpenID Connect to ensure user identity and enforce central administration of users.
- Built-in functionality to provide reasonable assurance that confidential user content is not compromised including but not limited to refile services, multi-tier encryption key management, and role restrictions

Personnel Access Controls

iManage controls ensure that all employees involved in the processing of customer data through the iManage Cloud Services are authorized personnel with a need to access the system resources and data, are bound by appropriate confidentiality obligations and have undergone appropriate training on an annual basis regarding the protection of personal data. Personnel are subject to background checks.

Should any affiliate or third-party subcontractor become involved in the processing of customer data through the iManage Cloud Services, iManage will ensure that the third party enters into a written agreement with iManage by which they are subject to these same obligations. As of the publication of this document, there are no such third-party processors.

Access Authorization Management

All iManage personnel who are engaged in the delivery of iManage Cloud Services are subject to iManage standards for secure user identification and authentication protocols which require use of unique access IDs. This applies to both system access and application access.

System Logs

Access to system and network logs is provided on a need-to-know basis for operating and supporting the iManage Cloud Services. Only iManage personnel who are engaged in the delivery of iManage Cloud Services can access the production network where the logs reside, and access is restricted based on the job function of each user (e.g., DBA has access to database logs, web administrator to web server logs, system administrator to system event logs, etc.)

System Logs are secured so that they cannot be edited and are maintained for a minimum of 1 year.

Application Access Controls

SAML 2.0 Single Sign-on

The most common user authentication method for iManage Cloud is via a SAML 2.0 compliant identity provider (IDP). This provides the highest level of security and convenience for both users and administrators with centralized user management. It also enables enhanced account and password restrictions and additional security capabilities such as multi-factor authentication. iManage Cloud is certified with ADFS, PingFederate and Azure ADFS identify providers. However, it has been configured with a wide variety of other providers which are also SAML 2.0 compliant. When it is configured, users initiate a login to an iManage Cloud endpoint, which redirects the user to the identity provider (IDP) configured in their iManage Cloud company account. When the user's identity is confirmed via authentication to the IDP, a SAML token is sent back to the iManage Cloud endpoint to allow entry to the iManage Cloud as the associated user. When using Single Sign-on, user administration (creation and suspension) is done via the Identity Provider.

Enabling the Single Sign-On option will require all users in the company library to be authenticated against the specified IDP to gain access to the iManage Cloud. Since a SAML 2.0 IDP may not be an option for all customers, particularly those who are in the process of on-boarding, the following additional authentication options are supported.

OpenID Connect (OIDC)

Customers are increasingly choosing to adopt SSO authentication via OpenID Connect, a modern authentication standard based upon OAuth 2.0. OIDC is generally easier to configure and support than SAML 2.0. It can be configured with the exchange of two URLs and requires no certificates to manage and no complex metadata files to exchange. OIDC is supported by all commonly used IDP vendors including Microsoft (ADFS, Azure AD), Okta and PingFederate.

Directory Synchronization

The iManage Cloud subscription includes access to a utility which will synchronize users and groups from the company's LDAP directory to the iManage Cloud user directory. The Directory Services Sync Utility (DSSync) can be downloaded and installed on any server within the company's domain where it will run as a Microsoft Windows service. It will communicate to the iManage Cloud over a secure connection and will be subject to the authentication requirements setup by the company administrator for the service account.

A configuration interface is included with the utility which allows the company administrator to configure the connection, the user accounts, and users and groups to be synchronized. Extensive filtering options allows for a subset of the users in the LDAP directory to synchronized to the iManage Cloud, including filtering by OU, group, or user attribute.

The DSSYNC utility also allows for synchronization of groups and group membership to the iManage Cloud directory which allows group management to be done within the LDAP directory services. This lightweight utility can be run continuously to provide near real time alignment of users and groups.

Administrative Access Controls

A role-based security model allows granular control of the administrative capabilities, such that helpdesk agents who need to manage users can be limited. Higher-level administrative accounts can have access to run company reports or setup integration policies (for example, mobile integration). Finally, these role assignments can be specified at the library level, such that you can choose separate administrators for each library (e.g., your organization has merged with another)

Data Access Levels

Access to the content uploaded to the iManage Cloud is governed by access control lists assigned to the specific object, the object being a version of a document or email. Access can be granted to a user or a group of users with the following access levels:

- No Access
- Read Only
- Read/Write
- Full Access (includes the ability to modify the access control list)

Security can be defaulted based on the container to which the object is filed. An optional refile service will ensure that all filed objects adhere to the security set at the container to which it is filed.

Optional Client and Project/Matter based access levels

The iManage Security Policy Manager is an optional service available within the iManage Cloud which allows for access to objects and content based on the client or project/matter to which the content pertains. Frequently referred to as an ethical wall, the governance rules defined by iManage Security Policy manager will ensure that only users who are explicitly allowed access to a client-related or project-related content will be able to access the content. It also allows for explicit denial of access to any content pertaining to a client or project/matter and it applies to both existing content and any content created in the future.

Application Logs

The iManage Cloud Services maintain audit trail logs for the following activities:

- User login/access
- Document Activity

Only persons with access to the content can view the document activity. Each document activity entry captures IP Address, date/time, User ID, the object being accessed, and the action taken or result.

Document Activity logs are maintained for the life of the subscription and are only deleted when the customer library is deleted).

Activity log entries are retained for objects (i.e., users, documents) even after these objects have been deleted from the company library.

Business Continuity and Disaster Recovery

iManage performs annual disaster recovery tests. The primary focus for iManage is to ensure reliability and availability of the iManage Cloud services. However, there may be incidents and events outside iManage control, and iManage has invested in the resources and defined processes to ensure business continuity and a timely recovery of the services in the event of a disaster.

Disaster Recovery is included in the iManage Cloud services. The iManage Cloud Disaster Recovery services include replication of customer data, in encrypted form, to a secondary Azure region which is maintained in the event of a disaster. Secondary Azure regions are located far enough away from the primary region to avoid the impact from a large-scale regional disaster. A global network of iManage support and operations resources ensures that in the event of a disaster, communications are maintained, and the technical resources required to recover are available.

iManage maintains a Business Continuity Policy, which is compliant with and certified against the ISO 22301 standard to guide the development, implementation, and management of business continuity in the event of a disaster impacting iManage business operations. The iManage Business Continuity Policy is documented and part of the iManage Information Security Management System. The iManage Head of Information Security is responsible for maintenance of the Business Continuity Program with oversight from the iManage Governance Board, a board consisting of iManage executive management. The iManage Business Continuity Policy is reviewed, at minimum, annually. Employees directly involved in the implementation of the business continuity program are trained through participation in table-top exercises and review of the appropriate procedure and process documentation.

Data Retention

iManage Cloud documents and emails that are deleted are retained in the company trash. From here they can be restored or removed from trash by an administrator with the required access level using the iManage Control Center.

JOURNALING

Each time a document object is modified in the system, a copy of the original document is written to a journal. This provides a complete history of every revision to a document. Any user with access to the document can view and recover one of the prior revisions maintained in the journal. Documents written to the journal are retained indefinitely, or until explicitly purged, to allow customers to recover replaced or overwritten documents. Additional details on journaling and how it can be used to recover documents can be found in the *Document Recovery Data Sheet for iManage Cloud Customers*.

BACKUP

iManage maintains the ability to recover all modified or deleted data objects for a period up to 90-days. This capability is intended for system recovery purposes only. Customers who require recovery of individual documents may recover documents from the Journal as noted above.

RETENTION AFTER TERMINATION/DELETION

If a company terminates their iManage Cloud subscription, arrangements can be made to obtain a copy of the company documents from the iManage Cloud. Following the end of a customer's subscription, customers are given a period time to remove their data from the iManage cloud after which point the account and data will be deleted.

After deletion of the company account, customer data may continue to exist on system recovery backups in an encrypted state. With current backup schedules, all traces of the encrypted customer data on the system recovery backups will be removed after 90 days.

Revision Summary

Revision Date	Revision Description
Mar 2018	• Revised the designation of the Australian Data Centers. Previously reported as Primary in Sydney and Secondary in Melbourne. This was incorrect and has been corrected with this revision.
May 2018	• Reflected name change of co-lo provider for iManage owned data centers from CenturyLink to Cxytera. • Updated to reflect move of Australian data centers from Microsoft Azure to iManage owned and operated data centers within a Cxytera co-lo. • Updated terminology regarding data encryption to reflect storage of CMEK in third-party service provider. • Updated to reflect most recent ISO audit certification results.
Nov 2018	• Simplified section on CMEK and provided reference to the CMEK data sheet • Added information on desktop encryption • Added section on application architecture • Added references and appendix of additional available references
Jan 2020	• Corrected Data Retention section to remove text which indicated trash was automatically purged after 90 days. It is not. • Updated technologies in use to reflect new services • Removed appendix of additional available references and incorporated references into body of the document. • Updated to reflect move of data centers in Germany • Section on iDrive data encryption has been removed. Application specifics will be provided in product documentation.
April 2020	• Updated branding • Corrected UK Data Centers primary and secondary locations
Nov 2020	• Added plans for Japan Data Center • Removed references to retired Germany Data Center location • Removed references to requests for reports
Mar 2021	• Added availability of Japan data center • Added plans for additional Azure data centers
Sep 2021	• Added availability of new Azure data centers in 2021 • Added Azure regional names to data center locations • Corrected data center owner name and city where applicable
Dec 2021	• Updated availability of new Azure data centers in US, UK, and Australia
March 2022	• Updated to better reflect the capabilities of iManage Azure data centers

Return to Top