iManage

Making knowledge work

# SECURITY CERTIFICATION AND SYSTEM SECURITY

iManage offers a comprehensive approach to security, adopting the best practices from the security and cloud industries to provide a secure global platform for professional services firms. Our platform is independently verified by auditors, large commercial financial institutions and significant players in the defense space.

## Application Security

We build secure software by providing enhanced annual security training for our developers, conducting peer reviews on all code, and continuously testing our code via Dynamic Application Security Testing (DAST).

### Developer Training

- iManage requires all software engineers to take security training annually

- iManage engineers are required to participate in written and practical exercises (Capture the flag events) to ensure they understand security concepts and standards

- Once above are done, all engineers have to sign an assertion confirming their commitment to understanding and following software security standards

### Developer Led Assurance

- All changes are peer reviewed prior to being committed

- Dev team uses industry leading tools to test their own code prior to QA and external testing

### Dynamic App Testing

- All cloud applications are tested using externally managed continuous dynamic application security testing (DAST) service (with support from iManage QA and iManage Security)

- Any defects found are escalated according to internal software defect process and remediated

### Static App Testing

- All code is reviewed using static application security testing (SAST) tool, and defects are remediated as part of development process

### Penetration Testing Detail

- All cloud products are independently tested at least annually

## Compliance Certification

iManage security practices exceed industry standards, as shown by the continued expansion of our security compliance certification and achievements.

To help validate its compliance status, iManage maintains:

- ISO 27001 certification, including the additional controls from ISO 27017, ISO 27018, and ISO 27701

- CSA STAR Level 2 certification

- ISO 22301 certification

- An annual Type 2 SOC 2 report that includes:

  - All the Trust Services Criteria; Security, Availability, Con identiality, Integrity and Privacy and additional SOC2+ criteria; NIST 800-171 and Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0.1

- A current Privacy Shield certification

## Disaster Recovery and Availability

iManage leads the industry in service availability. Our policy is to replicate your data across datacenters (in-region) and maintain four copies.

- In addition to offering the best availability when it comes to cloud DMS providers, iManage offers contractual service level commitments for availability

- Every iManage production data center has a corresponding spare site in-geography to allow for immediate recovery

- iManage maintains multi-gigabyte connectivity to ensure timely replication to ensure we can meet your recovery point requirements

- Our DR process is seamless to our users. In the event of a disaster, no host or DNS changes are required by our customers

- Our DR plan is tested regularly

## Privacy

iManage can help ease your regulatory burden with our products that support privacy objectives.

- iManage is compliant with GDPR regulations
- Customer retains ownership of the Customer Data
- iManage will cooperate with Customer in meeting the obligations of Article 28 and other related articles

iManage includes an addendum to our Cloud Services Agreement that defines our obligations.

## Best Practices

Maintaining your own iManage stack? Go to help.imanage.com to download detailed security best practices (for end users and server administrators) and stay current on software updates.

## Data Center and Network Security

You can rely on the confidentiality, integrity and availability of your data in our best-in-class (Tier III) data centers with protections from blast walls to at-rest encryption.

### Facility
- iManage datacenters are located in tier III (or better), SSAE18, PCI, ISO compliant facilities
- Power is supplied by redundant systems and multiple UPS/backup generators

### Physical Security
- Blast walls, gates, steel-reinforced concrete exterior walls, reinforced and alarmed doors
- Biometric authentication, 24/7 security officers, fixed and rotating cameras, video recorded

### Employees
- Annual training of all employees
- Background checks of all employees
- Segregation of duties enforced

### Encryption and Segregation
- All data is encrypted using standards compliant systems
- All data in transit is encrypted via https/TLS

### Logging, Monitoring and Incident Response
- iManage uses industry leading SIEM to monitor and alert on anomalous events
- 24 x 7 monitoring and escalation of security events
- iManage conducts internal training on incident response

### DDOS
- iManage mitigates the threat of Denial of Service via multiple tools to balance traffic and prevent loss of service to customers
- iManage purchases additional services to provide additional DDOS protection

### Vulnerability and Patch Management
- Internal and external network tested via automated tools at least monthly
- Monthly patching of all systems

### Network Segmentation
- Limited number of iManage employees have access to dedicated customer environment (access granted for maintenance purposes)
- Customer environment requires 2-factor authentication to access

## Integration

We provide ease of use and security features for your organization by providing support for SAML and IP filtering.

- iManage offers many ways to integrate your identity provider into our solution including SAML2 compliant identity providers and ADFS
- All our traffic is encrypted via TLS (encryption in transit) using an independent cert, however we can support any additional security requirements you may have such as IP Filtering for your profile
  - iManage has published a comprehensive, secure REST api SDK

---

**About iManage™**

iManage transforms how professionals get work done by combining artificial intelligence, security, and risk mitigation with market-leading document and email management. iManage automates routine cognitive tasks, provides powerful insights and streamlines how professionals work, while maintaining the highest level of security and governance over critical client and corporate data. Over one million professionals at over 3,000 organizations in over 65 countries – including more than 2,000 law firms and 500 corporate legal departments – rely on iManage to deliver great client work – securely.

iManage
Making knowledge work

Blog: imanage.com/blog