iManage Govern
Security Policy Manager

Manage global security policies at scale

KEY FEATURES:

- Protection of content in iManage and non-iManage repositories
- Intuitive, role based UI design runs on any browser and any device
- Cloud or on-premises deployment options
- Advanced notifications, timeline and audit capability
- Role based dashboards for administrators/owners and end users

KEY BENEFITS:

- Implement need-to-know security enforcement at scale
- Reduce system load with no performance overhead when security policies are created and no re-indexing of iManage Work content when security policies are created, adjusted or removed
- Improve productivity and increase scalability with delegation of access management
- Improve client security with client-centric design
- Better respond to client audits with client-centricity and client dashboards
- Manage and review policies from anywhere with responsive design

IMANAGE WORK PRODUCT MANAGEMENT

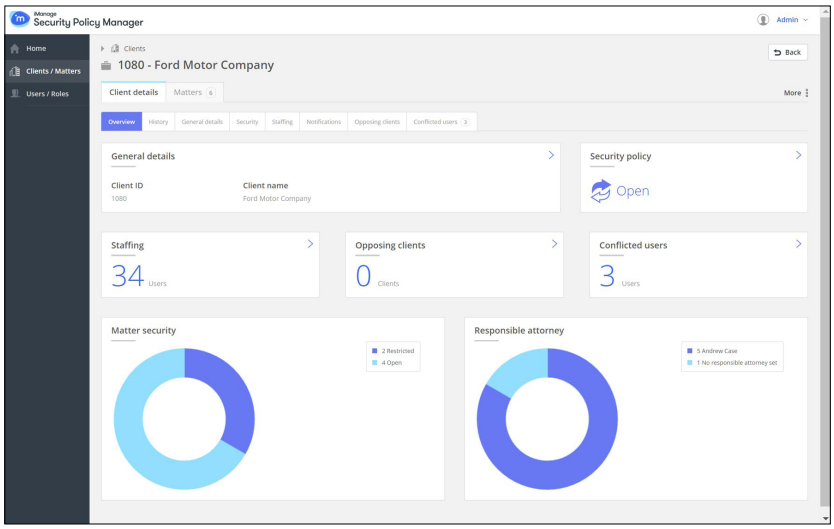
- **iManage Work:** Secure document and email management
- **iManage Share:** Secure governed file sharing and collaboration
- **iManage Insight:** Enterprise content search and analysis
- **iManage Govern:** Archiving, Records, Threat detection and Security Policy Management

In today's world of relentless cyberattacks on law firms and other professional service firms, clients are demanding that more care is taken with their confidential materials. Even with regular user training in spear phishing tricks and other steps taken to secure the perimeter, the likelihood of a breach remains high.

Securing sensitive content on a need-to-know basis and segmenting other content appropriately within the firm are critical parts of any strategy to limit the exposure and reputational damage that a breach can bring. A new approach to data security is needed and with it software that can handle the volume and complexity of security policies is required.

iManage Security Policy Manager

iManage Security Policy Manager meets modern security challenges with no impact to firm productivity. Security Policy Manager allows you to manage your global security policies, including ethical walls and barriers, at scale to meet today's increasing client demands. Security Policy Manager delivers data protection without inconveniencing professionals by getting in the way of how they want to work.



iManage Security Policy Matter dashboards provide easy-to-use top-level views of security settings, by client or matter

Instant protection with no-refiling or re-indexing of Work content

A tight and unique integration with iManage Work ensures that security policies can be instantly established, adjusted and ultimately removed, all without costly access control cascades, document re-files or content re-indexing of the

IMANAGE GOVERN MODULES

- **Records Manager:** Electronic and physical records circulation, retention and disposition management
- **Disposition Workflow:** Automated disposition processing workflow
- **Archive Manager:** Email and document archival and access management
- **Threat Manager:** Detection of internal and external threats
- **Security Policy Manager:** Global, scalable security policy management including ethical walls

SUPPORTED SYSTEMS:

- iManage Work
- iManage Records Manager
- Network file shares
- Time entry systems
- Agent framework is available for third party integrators

iManage Work workspace. This ensures there is no performance impact to Work end users or delays in new documents appearing in search results, even for the largest of workspaces.

Secure sensitive data to those who need-to-know

Clients are increasingly demanding that access to their matters is restricted to the team that is working on them. With Security Policy Manager, it is easy to enforce this, through assignment of policy to the client or to individual matters.

Responsibility for maintaining access can be left with the IT service desk or handed to the client or matter owner or their delegates.

A range of options allow the required level of self-service access to be provided, including automatic time limited to ensure urgent requests can be resolved out of hours and access-after-approval by existing team members or the responsible attorney when access must be tightly controlled. All changes are fully audited.

Segment data in multiple ways

Segmenting data helps to minimize the impact of a cyber breach by limiting the exposure to the set of documents accessible by the victim whose credentials have been compromised. Security Policy Manager allows policies to be applied based on practice group, matter type and any other metadata value.

Modern intuitive user experience

A modern responsive user interface ensures that security policies can be managed and inspected on computers, tablets and phones.

Security policies are clearly indicated in iManage Work and Records Manager client screens, making it easy to see who does and who does not have access.

Role-based dashboards enable administrators, client owners and users to view information that is pertinent to them.

Multiple security policy types

Policy types include restricted (need-to-know) access, opposing client/matter segregation and conflicted user exclusions.

https://imanage.com

@imanageinc
www.linkedin.com/company/imanage

iManage

About iManage™

iManage is the leading provider of work product management solutions for legal, accounting and financial services firms and the corporate departments they serve worldwide. Every day, iManage helps professionals streamline the creation, sharing, governance and security of their work product. Over 3,000 organizations around the world—including more than 2,000 law firms—rely on iManage to help them deliver great client work. Headquartered in Chicago, IL, iManage is a management-owned company. For more information, please visit https://imanage.com.