Security
White Paper

FYI Docs

Contents

Summary

Securing more time and reliability

It's true. When it comes to cloud-based document management, the right solution will save you vital time. But nothing is more critical than the security of the data it contains.

We know that for enterprise accounting practices, conducting processes manually is not only inefficient, but it can expose you to risks through the rekeying of data. That's why FYI created an online document management and automation engine, purpose-built for accountants.

Nothing is more critical than the security of your data

In this white paper, you'll discover FYI's broad-based approach to information security, and the safeguards you can depend on to ensure the reliability of our platform and your data.

> ❝ Having a secure space that clients can drop documents into is fantastic and far more secure than email, so it provides clients with peace of mind. ❞

ABBY ACUTT, CLIENT SERVICES MANAGER - GJ WALSH & CO

Results

At FYI, business continuity is our business.

Trusted by 1000+ practices and 15,000+ users with 400 million+ documents hosted on the platform, FYI is a robust system with uptime that exceeds industry best-practice.

Since our November 2018 launch, FYI has achieved:

- 99.99% availability
- Zero security incidents

Data Security

Peace of mind with enterprise-grade data security

Protecting your information is paramount. That's why FYI is committed to providing practices with the highest level of data encryption.

FYI safeguards your data with:

✅ **Encryption both in transit and at rest**
Our two-way encryption keeps your information safe while sitting idle on servers or being accessed in transit via the FYI application, so it's doubly secure.

✅ **Unique encryption keys**
Just for you. FYI allocates separate AES-256 encryption keys to each subscription, meaning each accounting practice has their own layer of protection from unauthorised access.

✅ **Private data migration**
We keep it confidential by moving data over SSL and encrypting with a 2048-bit strength certificate to secure you against interception.

✅ **Independent penetration testing**
When it comes to security, we don't like weakness. That's why FYI engages external consultants to perform annual assessments including penetration tests.

✅ **Controlled data access**
We're strict on this. Only users who need to access production data for customer support or problem resolution retain access, and we'll securely delete a customer's data on request.

✅ **Manage user permissions easily**
With a tap in the app, you can set user permissions to control what data a user can access, and what company-wide actions and settings can be controlled.

✅ **You own your data**
Your practice always retains full ownership of the content you upload to FYI. And if you end your subscription, you can export your documents to a Windows Explorer directory structure.

✓ **Data deletion upon agreement**
All parties agreed? Your practice can delete your data from FYI once processing is complete, and legally binding retention requirements are met.

✓ **Cookie compliance**
At FYI, our cookie policy is to ensure consent is gained, and they're treated as personal identifiable information (PII) when required.

Authentication

Secure access with one-step verification

No extra layers of complexity. FYI makes verifying users logging into the platform simple and secure.

To ensure secure access, we utilise:

Microsoft Windows authentication

Forget creating an authentication layer requiring yet another username and password. FYI leverages the trusted Microsoft Windows user authentication to identify users.

It's easy. To log in to FYI, a user only needs their Microsoft 365 username and password. The authentication enabled for Microsoft 365 applies to FYI.

Multi-factor authentication

Like to take it a step further? FYI supports multi-factor authentication (MFA) when implemented as part of Microsoft 365.

Your practice administrator can choose whether to apply it to FYI.

Architecture

Designed for confidence in the cloud

Secure AWS infrastructure

By utilising the Amazon Web Services (AWS) Well-Architected Framework and regular feature releases, FYI guarantees high-availability, data redundancy and government-grade security.

Regular Load Testing

As part of the regular software development life-cycle, FYI is routinely load tested to guarantee it can scale to host the (yes) billions of documents that might be required

24/7 Protection

FYI continually works with AWS to apply the latest monitoring and defences against interceptions, including 'denial of service' attacks, so we're always on guard for any alerts.

Hosting

Safe storage only you have access to

With FYI, your data is securely hosted in AWS data centres and disaster recovery sites, and only you have the keys.

Local Storage

For Australian and New Zealand clients, data is stored in AWS data centres in Sydney, while for our UK clients, data is hosted in AWS's London data centres.

Robust backup

AWS is ISO27001 compliant and offers the security of inbuilt offsite backups, replication to multiple data centres, rapid disaster recovery and more.

Your own data store

With your practice documents stored in your own discreet store within AWS, you can lock up your data from unauthorised access with a unique set of encrypted keys.

Backup

Dynamic backup, fully restorable

With FYI, every document and version you create can be completely restored. Now that's comforting.

Automatic

Your practice data is dynamically backed up by AWS as part of their core service for total peace of mind.

Comprehensive

One solution, broad defence. AWS provides inbuilt offsite backups, disaster recovery, and multiple sites synchronisation.

Local

For greater security control, we also give you the ability to back up your own data locally.

Disaster Recovery

Rapid response and resolution

A disaster recovery event doesn't have to be a disaster.

Using FYI, your data is replicated to multiple data centres and backed up to ensure full protection.

Priority Incident Managment

Our process ensures a rapid response to security events that affect the integrity or availability of the platform or data, with customer-affecting events given the highest priority.

Effective Incident Response

Our procedures ensure potential security events are identified and reported to appropriate personnel, that defined protocols are followed for resolution, and that results are documented and reviewed by the InfoSec Team regularly.

But we don't stop there. We're also working to update these processes to include breach notification if a security incident involves the loss or unauthorised use of personal identifiable information (PII).

Fast Service Recovery

Time is money. That's why we store your files on servers that are made available in a high-availability failover cluster, and backed up to the disaster recovery service (DRS), which is tested on a quarterly basis.

In the case of a disaster recovery event:
- The maximum period of modified data that could be lost is 5 minutes
- The maximum time expected to restore data and service is 30 minutes

FYI has a fully operational DRS to maximise availability including:
- Failover clustering of websites
- Continuous data replication from the primary site to the DRS
- Standby server for database recovery located at DRS
- Recovery point objective (RPO) of 30 minutes
- Recovery time objective (RTO) of 30 minutes
- Goal of a fully operational service within 30 minutes of elevating the DRS

In the case of a disaster recovery event the maximum period of modified data that could be lost is 5 minutes.

The maximum time expected to restore data and service is 30 minutes

Certifications

Certified security to global standards

At FYI, we understand how critical compliance is to your business which is why we provide certification at the highest international standards, right from the start.

ISO 27001:2019 Certified

Your data is backed by the international standard for information security management.

OWASP Grade Compliant

Enjoy full confidence in the cloud with the international standard for web application security.

### ATO Digital Services provider

This means FYI meets all requirements for authentication, encryption, certification, data hosting, personnel security and security monitoring practices.

GDPR Compliant

We're committed to protecting the personal data and privacy of FYI users in EU and EEA countries by ensuring General Data Protection Regulation (GDPR) compliance.

FYI is also compliant with:

- SOC 2 Type I
- HIPAA
- The U.S. ESIGN act of 2000
- The Uniform Electronic Transactions Act (EUTA) of 1999
- The eIDAS regulation for the EU of 2016 (EU Regulation 910/2014)
- Privacy Shield
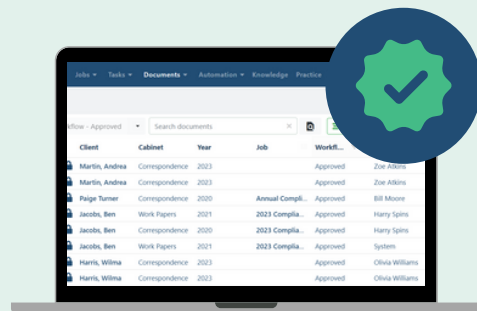
Privacy

Publicly committed to your privacy

Confidential data should remain just that, so we comply with privacy laws in Australia, New Zealand and the UK to prevent unauthorised access to and disclosure of customer information.

Data mapping and privacy impact assessment

To verify our privacy practices are appropriate, FYI conducted data mapping and a Privacy Impact Assessment (PIA) to assess how we collect, process and store personal data, and determine potential privacy impacts. You can be sure your data is in good hands.

Training and Privacy Awareness

Security from platform to people. All FYI employees receive GDPR training (upon hire and repeated annually) overseen by our on-site compliance team.

Information security policies

For added peace of mind, FYI's informational security and data protection policies govern when employees and contractors can access data stores containing your data.

Data transfer compliance

FYI complies with both the EU-US and Swiss-U.S. Privacy Shield Frameworks for all onward transfers of personal data and liability provisions from the EU and Switzerland.
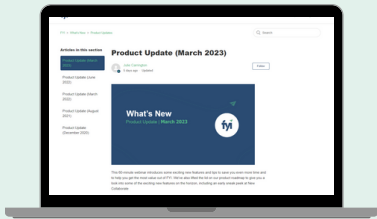
Under each Privacy Shield Framework, FYI is responsible for the processing of personal data it receives, and transfers data to a third party acting as an agent on its behalf.

Read our Privacy Policy

Platform Updates

Easy access to enhancements

At FYI, our in-house developers continually deliver enhancements to ensure the highest level of security for your data.

You'll always find up-to-date announcements on platform updates, features and fixes online on our What's New page.

View Latest Updates

Service Status

Our service, at your service

You can get a full overview of updates on scheduled maintenance, service interruptions and incident resolutions online, anytime.

Plus, subscribe to receive status updates by email, Microsoft Teams or Slack on our Service status page.

View Service Status

Licence Agreement

A license with flexibility

FYI is licensed via a Software as a Service (SaaS) agreement which renews monthly, giving you flexibility to exit if ever required at short notice.

Your licence agreement clearly states:

You retain ownership of your data

In the unlikely event of FYI's receivership, you have the guaranteed right to export your documents, including the associated metadata.

You retain ownership of the content you upload

Should you wish to leave FYI, anyone with an administrator role can download all documents in a logical folder hierarchy of client and related metadata.

Conclusion

A secure return on investment

With FYI, security isn't something you're just entitled to, it's a prerequisite of everything we do.

With 99.99% uptime, 24/7 protection and completely restorable files, you can trust us because we know the importance of getting it right. And it's what makes FYI a truly secure return on investment.

Discover how your business can put enterprise-grade security into practice. Get started with a live demo or see FYI in action with a free, no-obligation 30-day trial.

Book a demo or start a free 30-day trial at

www.fyidocs.com