Iress Information Security

Iress is the Australian technology company that provides the Xplan financial planning software, CommPay remuneration system and a linked client portal. Centrepoint Alliance licensees utilise Xplan/CommPay as a CRM and financial planning tool. Iress is globally certified to ISO/IEC 27001:2013, an international standard to manage information security.

Where is client data stored?

Client data in Xplan for Australian clients is stored on Australian Amazon Web Services (AWS) servers. Iress may have staff from overseas locations accessing the data, but the data itself is retained on Australian servers. Iress has an Information Security Management System (ISMS) which preserves the confidentiality, integrity, and availability of information. AWS, as the underlying technology platform, has numerous global certifications and compliance programs.

How is the data kept secure within the system?

- Data at rest is encrypted through AWS S3 encryption.
- Data in transit is encrypted through TLS/ HTTPS.
- Client data transmitted within the internal network in the Iress Cloud Platform is also encrypted in transit.

How is data backed up?

The Xplan software utilises an automated backup and retention capability. Backup frequency and retention period are below:

- Daily - retain for 35 days
- Monthly - retain for 12 months
- Bi-Annually – retain for 7 Years

Clients that are soft deleted from Xplan are automatically hard deleted (irretrievable) from the system 90 days after the soft deletion date.

What happens if there is a disaster that impacts client's data?

Re-creation of the system from source code and recovery of the backed-up data is possible, in the event of a disaster, such as the loss of underlying physical infrastructure or accidental/malicious deletion of the virtual infrastructure. AWS Servers are in multiple locations and if one is impacted there are additional servers available to be utilised.

What happens if there is a security incident?

Iress maintains an Information Security Incident Management Policy and an Information Security Incident Management Procedure. In the event of a security breach, all security incidents are managed by their global Information security team.

Iress will, as soon as possible (and where reasonably practicable within 72 hours after becoming aware) notify a customer of a security incident or a security control weakness and will provide all relevant information within its possession. Iress will remedy any security control weakness as soon as reasonably practicable and will provide timely updates until the security control weakness is remedied.

Centrepoint would at the point of notification of a security breach notify our Cyber Insurer and work with them and Iress on the Cyber Incident response plan.

What happens if there is a data breach?

Data breaches are incidents which involve the exposure of personally identifiable information and/or confidential data. Iress maintains a Legal, Regulatory and Compliance Policy to ensure that Iress is maintaining the privacy and security of its staff and clients by complying with applicable regional laws, regulatory requirements and other commitments such as GDPR, POPIA or the Australian Mandatory Data Breach Notification Scheme. In the event of a data breach, Iress will respond by complying with such relevant laws and regulatory requirements. Centrepoint would also notify the relevant authorities of the breach.

What ongoing checks does Centrepoint Alliance (CPAL) undertake with Iress?

On an annual basis we obtain information from Iress covering the following:

- Information regarding governance, compliance and risk framework, BCP, DRP, Data security Policy, IT Security Policy
- Results of external IT audit to identify any security vulnerabilities of Xplan, CommPay and client portal
- Results of annual BCP/DRP test
- If there have been any incidents in the past 12 months where physical or IT security controls were breached.

The result of this annual assessment is reviewed by the Cyber Security Committee, CPAL IT Infrastructure and Technology Delivery and Architecture teams.

What indemnities do CPAL have for security and data incidents?

Under the current Agreement with Iress executed in 2022, where Iress has failed to implement and maintain technical and organisational measures against unauthorised or unlawful processing of personal information, Iress will indemnify CPAL for that breach and may be liable for up to $1M for loss suffered. In addition, Iress is also responsible for remedying its breach under contract, which supplements Iress' obligation to comply with privacy laws.

Your obligations

Iress is a cloud based system that is accessed via password and log on with Multi Factor Authentication. Passwords are stored as SHA256 encryption. Enforcement of minimum password strength is set in the system, along with temporary account lockout to protect against brute force password guessing attacks.

Whilst accessing the system through the cloud is convenient, it means that good password hygiene and security is of utmost importance. Practices are required to:

- Notify when staff members/users leave to remove access
- Ensure that passwords are sufficient complex and kept securely
- Change passwords immediately or remove access if an incident occurs

CP_0048 08/2023