Client Due Diligence Information Pack

Private and confidential

Version 4
January 2024

1. Company Information

Iress is a global technology business providing software to the financial services industry.

Iress Limited is our ultimate parent company, it was incorporated in Australia in June 1993 and is listed on the Australian Securities Exchange.

“Iress” is a trading name used by the companies within our Group. Details of our trading/ contracting entities are set out below.

Country	Contracting entity within Iress	Company Registration Number	Registered Address	VAT number
Australia	IRESS Limited	060 313 359	Level 16, 385 Bourke Street, MELBOURNE VIC 3000	
United Kingdom	IRESS FS Limited	02958430	Honeybourne Place, Jessop Avenue, Cheltenham, GL50 3SH	100 1056 02
	IRESS Portal Limited	02596452	Honeybourne Place, Jessop Avenue, Cheltenham, GL50 3SH	100 1056 02
	Proquote Limited	03851830	Honeybourne Place, Jessop Avenue, Cheltenham, GL50 3SH	100 1056 02
	O&M Life & Pensions Limited	02717535	Honeybourne Place, Jessop Avenue, Cheltenham, GL50 3SH	623 1714 70
France	Iress SAS	449 703 248	86 Boulevard Haussmann, 75008, Paris, France	
South Africa	IRESS MD RSA (Pty) Limited	1965/002808/07	BUILDING 3, 2929 ON NICOL, 2929 WINNIE MANDELA DRIVE,	

			BRYANSTON SANDTON, GAUTENG, 2191	
Canada	IRESS Market Technology Canada LP	1 4041 2008 (Ontario) 1114 1041 (Alberta) XP37 3761 (British Columbia) 33 6435 5506 (Quebec) 62 9500 (New Brunswick)	5300 Commerce Court West, 199 Bay Street, Toronto, Ontario M5L 1B9	
Singapore	IRESS Market Technology (Singapore) Pte Ltd	200923761E	18 Robinson Road, #19-01, Singapore 048547	
New Zealand	IRESS (NZ) Limited	9 429 039 268 846	c/o Bell Gully Solicitors, Level 21, 171 Featherston Street, Wellington, 6011, NEW ZEALAND	

2. Regulation and Membership of Industry Bodies

2.1 Is Iress a regulated entity?

Certain Australian subsidiaries in the Iress Group are holders of an Australian Financial Services Licence, and are subject to the relevant licence conditions and associated regulation.

In those regions in which we operate outside of Australia, Iress' business activities are not regulated.

2.2 Accreditations and Membership of Industry Bodies

Iress is globally certified by BSI to ISO/IEC ISO 27001:2013. Our Certificate Number is IS 615380.

Note: There are certain areas of the Iress business which are not currently covered by the ISO accreditation (as noted in the certificate which is available on the Iress Community) as these business areas have to date not been included in the scope of the BSI audit. We intend to include these business areas in the next applicable regional audit. In the meantime, these areas of the business are subject to the information security controls applicable to Iress' global business, as described in section 8 below.

A list of our partnerships and memberships can be found in our ESG report - available here: https://www.iress.com/about/investors/results-and-reports/.

3. Financial Information

Details of Iress' latest results and reports - including our latest Annual Report - can be found here: https://www.iress.com/about/investors/results-and-reports/

4. Environmental, Social and Governance (ESG)

Iress has a well defined environmental, social and governance strategy. We have made significant strides in our ESG approach and we continue to focus on specific areas we can support, where it makes sense for us to do so. We are committed to effectively managing risks across our operations, including cyber security, modern slavery and climate change. In 2022, we continued to roll out our 2021–2023 information security strategy to strengthen our security culture and systems, in addition to developing a 2023–2024 modern slavery roadmap to improve transparency in our supply chain. We also developed our initial response to the recommendations from the Task Force on Climate Related Disclosures, conducting climate risk and opportunity assessments and establishing a 2022–2024 climate-related risk and opportunity roadmap to improve our disclosure overtime.

Through Iress Impact, we are committed to making a visible, reliable, and meaningful contribution to partner charities that align with the United Nations Sustainable Development (SDG) goals of quality education (SDG 4), decent work (SDG 8), and partnership for the goals (SDG 17). Since Iress Impact was established in 2017, it has contributed over $1m to our local communities.

A strong environmental, social and governance proposition drives value creation. Accordingly, ESG responsibilities to oversee strategy, policies, processes and performance are included in both the Iress Board and Audit & Risk Committee Charters ensuring effective governance.

Details regarding Iress' approach to ESG can be found here: https://www.iress.com/about/our-approach-to-environment-social-governance-esg/

Our ESG strategy can be found here: https://www.iress.com/about/our-approach-to-environment-social-governance-esg/2025-strategy/)

Our ESG Statement can be found here: https://www.iress.com/media/documents/Environmental_Social_and_Governance_Statement-_March_2021.pdf

Environmental

Our Environmental Policy can be found here: https://www.iress.com/media/documents/Enviromental_Policy_-_March_2021.pdf

Our Sustainable Procurement Policy can be found here: https://www.iress.com/media/documents/Sustainable_Procurement_Policy_-_March_2021.pdf

Emissions data is included within our annual ESG Report. Our latest ESG Report can be found here: https://www.iress.com/about/investors/results-and-reports/

With the known impacts of climate change and greater visibility of environmental considerations across the supply chain, taking action on environmental issues is critical. To align with best practice we have established a near term science-based emission reduction target and are in the process of validation with the Science Based Targets initiative (due to be completed December 2023).

Social

Modern Slavery

Iress' zero tolerance for modern slavery is communicated to all suppliers, contractors, and business partners at the outset of those business relationships, and reinforced thereafter. Iress has a Supplier Code of Ethics which requires suppliers to ensure they comply with the terms of the Acts - see: https://www.iress.com/trust/corporate-governance/governance-documents/supplier-code-of-ethics/

Our Modern Slavery statement can be found here: https://www.iress.com/trust/corporate-governance/governance-documents/modern-slavery-act-statement/.

Diversity and Inclusion

At Iress, our people are our greatest asset and we recognise and respect that each person is unique. We also acknowledge that diversity makes us stronger. By promoting a breadth of ideas, experience, and talent, we can create a successful, stimulating and innovative workplace.

Throughout 2022, we've worked to ensure the technology we build is accessible and meets the needs of as many people as possible, including those who live with disabilities. Our Iress Design System (IDS) is continuing to evolve and mature, as we build more user interface components across our products. IDS is fully accessible, which ensures that teams who adopt it are also getting the benefits of accessible user interface components and standards.

Iress' Diversity Policy can be found here: https://www.iress.com/trust/corporate-governance/governance-documents/diversity-policy/

Our Gender Diversity Policy can be found here: https://www.iress.com/trust/corporate-governance/governance-documents/gender-diversity/

Governance

Iress operates under a set of well-established corporate governance policies and processes. The inclusion of ESG matters in our Audit & Risk Committee Charter formalises Board oversight of this area. Our Charter can be found here: https://www.iress.com/trust/corporate-governance/governance-documents/audit-risk-committee-charter/. See also section 5 below for further governance information.

5. General Policies & Governance

Given the number of clients Iress has across the globe, and Iress' desire to operate as a 'one-to-many' service provider, it is not feasible for Iress to commit to compliance with specific client policies. We understand the importance of having certain policies and procedures in place, and we have an area of our website dedicated to corporate governance where various policies can be found - https://www.iress.com/trust/corporate-governance/governance-documents/.

This includes:

Anti-bribery and Corruption Policy

Iress' policy can be found here: https://www.iress.com/trust/corporate-governance/governance-documents/anti-bribery-corruption-policy/

Note: this policy includes sections on Iress' approach to hospitality, entertainment, gifts and expenses, and to training.

Conflict of Interests Policy

https://www.iress.com/trust/corporate-governance/governance-documents/conflict-interests-policy/

Whistleblowing Policy

https://www.iress.com/trust/corporate-governance/governance-documents/whistleblowing-policy/

Anti-fraud and fraud awareness policy

https://www.iress.com/trust/corporate-governance/governance-documents/anti-fraud-and-fraud-awareness-policy/

6. Staff background checks and vetting

Our approach is set out below:

Region	Checks
APAC	● Proof of eligibility to work - passport / visa is obtained. ● Proof of address check completed to confirm residency ● National Police History check ● Bankruptcy checks ● Employment verification ● Qualification verification - Highest level checked ● Resume assessment ● Banned Persons Check ● International Watch Lists Check
North America	● Social insurance number check ● Criminal check ● Credit check ● 5 years employment referencing ● Highest Education Verification
Africa	● Copy of ID or passport with Work VISA ● ID validation

	● Verification check ● Criminal check ● ITC check that confirms past employment ● A full credit record ● Two reference checks for confirmation of employment ● Qualification verification and copies of certificates saved ● Directorship checks to verify if an individual has ownership of or directorship in other organisations
UK and Europe	● Proof of Eligibility to Work in the applicable country - either a Passport or Full Birth Certificate ● Proof of National Insurance Number ● Basic Criminal Record Check ● Credit Check ● Electoral Roll ● Risk and Compliance checks ● 5 years employment referencing ● Highest Education Verification ● CV check for accuracy - aligned to pre-employment screening entry data

Our contracts of employment include comprehensive provisions requiring the protection of confidential information and the protection of personal data.

7. Data Protection

7.1 Collection of personal data

Where Iress collects personal data, it will do so in accordance with its Privacy Notice, a link to the Privacy Notice applicable to each region in which we operate can be found at the bottom of our website page (for the United Kingdom) and in the 'Legal' section of our website for other regions.

7.2 Processing of personal data

Iress' Global Data Protection Policy can be found on this page: https://www.iress.com/resources/legal/data-protection/ . This applies across all of the jurisdictions in which Iress operates, and sets out the principles with which Iress complies when collecting and processing personal data.

7.3 Training

All employees and contractors engaged to supplement Iress teams are required to comply with our Global Data Protection Policy. They are also required to carry out privacy and information security training on joining Iress, and annually thereafter.

7.4 Data Protection Officer

Iress has not appointed a Data Protection Officer in any of its locations. The role and responsibilities that would typically be assumed by a Data Protection Officer are spread across our legal, information security, compliance and risk functions within Iress. Iress' Chief Legal Officer has ultimate responsibility for privacy compliance.

Queries in relation to Iress' specific processing operations should be directed to compliance@iress.com.

7.5 Transfer of personal data outside of the country in which the client is based

Iress is a global organisation and as such Iress employees and contractors based in locations outside of that in which the client resides may have access to certain personal data relating to our clients, or their customers. In addition, Iress may engage certain third party suppliers to assist in the provision of services. Any transfer of personal data to a third party outside of the country in which the client is based will be carried out in accordance with our contractual terms and the laws in which the Iress entity providing the services is based.

For clients based in the UK, we will obtain your prior consent before transferring personal data to a third party via a general authorisation. In order to obtain general authorisation, we maintain a list of sub-processors on our website (this list is accessible here: https://www.iress.com/resources/legal/data-protection/ under the heading 'Authorised Processors'). The mechanics by which clients are deemed to have approved transfers of personal data to Authorised Processors will be set out in our contract with you.

7.6 Data Retention

Iress' approach to data retention is documented in our Global Data Protection Policy.

Please note that where clients are licensing software products from Iress, then unless there is a specific data retention period built into the product, the Customer (as the party responsible for the collection of data from its clients, and the manner in which that data is used) will be responsible for determining data retention periods applicable to the data it stores within the product. (For example, if a client of an Iress Customer no longer receives financial advice from that Customer, then it will be up to the Customer to decide how long it will retain that end clients' records in the applicable Iress product in accordance with the agreement that Customer has in place with the end client.)

Where Iress provides Xplan to Customers as a managed service, data will be retained on the multi-site for a period of two years following termination of the services by the Customer, following which it will be deleted.

Where the product/ service is hosted by Iress and the Customer deletes data, this data will be retained in back-up for a period of 7 years, following which it will be securely deleted.

For clients based in the UK, we have a separate data retention policy which can be found here: https://www.iress.com/resources/legal/data-protection/.

7.7 Technical and organisational and security measures

Details of Iress information security controls are set out here: https://www.iress.com/resources/legal/data-protection/ and Iress' Information Security Policy is available here: https://www.iress.com/resources/legal/iress-information-security-policy/

Please also see the Information Security section below.

Iress understands the importance of privacy by design. Our supplier engagement process requires that a data protection impact assessment (DPIA) is considered when Iress is onboarding a new supplier and that supplier has access to personal information controlled or processed by Iress. In addition, new projects are required to consider whether a DPIA is necessary - for example where there is new processing activity involving personal data, or a change in current processing activity. The requirement to complete a full DPIA for suppliers or new projects will be dependent on the data risk classification; all suppliers engaged in activity which meets the status of high risk processing, as determined by the relevant data protection regulator, will be subject to a DPIA. A DPIA considers the scope of the processing activity and the personal information that is involved in order to form a view on the risk posed to data subjects. This helps Iress identify mitigation activity to limit the risks identified and is an effective way to comply with its data protection obligations.

7.8 Data Breach Management

Iress maintains an Information Security Incident Management Policy (contained within the Iress Information Security Policy) and an Information Security Incident Management Procedure, as well as a specific Data Breach Policy. In the event of a security or data breach, incidents are reported to the global Information Security team and then managed by the legal and compliance team or the information security team, depending on the nature of the breach.
Security incidents involving unauthorised access to sensitive data are escalated to the CISO. This formal security incident process is based on good practice. It includes the following procedures:

1. Identification and reporting of security vulnerabilities and incidents
2. Recording and classification of information security incidents
3. Incident prioritisation / escalation
4. Incident containment
5. Incident treatment / resolution
6. Process, technology and/or data recovery
7. Collection of evidence for root-cause analysis
8. Post-incident review to identify how to reduce risk of recurrence

7.9 Accountability

To ensure there is accountability for data privacy across Iress we have a suite of policies, processes and procedures to support the correct handling of personal data. We review our compliance against guidance from the privacy regulators within jurisdictions in which Iress operates and in support of Iress' privacy programme.

8. Data Ethics and Artificial Intelligence

Iress is committed to ensuring that data is used in an ethical manner.   We have a Data Ethics Policy which applies to anyone in our business who is working with data. The policy sets out the principles by which we operate in key areas (lawfulness, accountability, impact, transparency, fairness, security, retention and access, and data sharing).

The responsible use of AI forms part of our data ethics considerations, and we have a specific policy covering the use of AI which includes clear guidelines which must be followed when AI tools are used within our business, and the process to be followed when AI tools are adopted.

Iress has established a Data Governance Council (DGC) with representatives from various parts of the global business, including Legal, Compliance, Information Security and Business Intelligence. This group is responsible for overseeing the manner in which Iress handles data and to establish guidance for the business around the use of data.

9. Information Security

Iress has an Information Security Management System (ISMS) in place which is implemented, monitored and maintained in order to preserve the confidentiality, integrity, and availability of information. It covers integrated software and managed services across managed environments. The ISMS is aligned and complies with the international security standard ISO/IEC 27001:2013.

Iress' Information Security Policy (please see the high level control areas that it covers via this link https://www.iress.com/resources/legal/iress-information-security-policy/) defines Iress' fundamental information security goals and expectations for the organisation. Iress translates these goals into specific objectives and controls (and assigns roles and responsibilities to achieve them). In setting these goals, Iress is committed to protecting the information for which it is responsible in line with customer, industry and statutory expectations to minimise any security risks accordingly.

The ISMS is formally documented and approved by senior management; all policies within the ISMS are reviewed and published on an annual basis. BSI audits Iress' ISMS as part of its annual global ISO27001 audit.

Iress' Information Security policy is underpinned by it's ISO27001 certification and global statement of applicability defines the policy documentation that is implemented within the organisation, policy documentation covers areas such as:

- Acceptable Use
- People Security
- Identity and Access Management
- Asset Management
- Data Security and Cryptography
- Incident Management
- BCP
- Supplier Management
- IT Systems and Maintenance
- Physical and Environmental

We have the following Information Security specific collateral which is available on the Iress Community and provides an in depth overview of the information security controls Iress implements across the organisation:

- Iress Shared Responsibility Model:
  ○ Iress Shared Responsibility Model - Governance Layer
  ○ Iress Shared Responsibility Model - Platform Layer
  ○ Iress Shared Responsibility Model - Physical and Environmental Layer
- Iress ISO 27001 Certificate
- Iress Global Statement of Applicability

10. Supplier Engagement

Prior to the engagement of a new supplier, the proposal is discussed at the Supplier Council, a group of representatives from relevant business units, with input from legal, ESG and procurement. Any new supplier must be approved by the Supplier Council before being contracted.

In addition to Supplier Council approval, Iress undertakes initial due diligence before engaging a supplier, this comprises checks regarding financial stability and sanctions exposure, detailed information security due diligence together with other details as appropriate (based upon a risk assessment of the supplier which takes account of country and/or industry specific risk).

All non-governmental suppliers are also subject to ongoing monitoring using a real time data tool - which triggers alerts to flag issues in certain risk areas - including financial, environmental, product, regulatory, social (workforce), sanctions and political exposure.

In addition, Iress carries out an annual review of its key suppliers - this involves revisiting many of our initial due diligence enquiries and checks (including information security where relevant), and in certain cases can involve Iress visiting supplier sites and interviews with supplier management teams. This review, its criteria and output are the subject of annual external assurance reviews.

The Iress Information Security Policy contains a Supplier Management Policy to ensure that Iress applies all relevant security controls in its arrangements with third parties engaged by the organisation, and ensures that Iress:

1. Puts in place legally binding contracts with third party suppliers;
2. Conducts supplier due diligence on all new third party suppliers that are on-boarded and considers the need for a DPIA;
3. Keeps a record of and tracks third party suppliers;

4. subjects critical third party suppliers to ongoing monitoring to ensure the effectiveness of their information security controls. (Iress uses a web based security monitoring system to track suppliers on an ongoing basis).

Where Iress deems appropriate (as determined by the nature of the services being provided), provisions will be included in our contracts with suppliers to ensure that supplier personnel are subject to appropriate background checks, will comply with certain Iress policies (including certain information security and compliance related policies) and will (where required) carry out certain training in these areas.

Iress' supplier engagements are governed by a variety of policy controls. Our policies regarding outsourcing, sustainable procurement and external collaborator policies will be in scope depending on the specific nature of the procurement.

11. Risk

At Iress, our purpose, mission and goals articulate who we are and what we want to achieve. As a global technology company and licensed financial services business, risk (positive or negative) is inevitable in order for Iress to achieve success. Therefore, our risk management culture is one that proactively identifies, manages, and mitigates risk so we can learn from risk events and continuously anticipate emerging risks and opportunities.

Iress has a strong organisational culture where the Leadership Team demonstrates and sets the standards by role-modelling values and behavioural expectations for risk management, which are anchored in the Code of Conduct and Risk Management Framework. Whilst we do not make our Risk Management Framework available for confidentiality reasons, we can confirm that it describes our commitment to managing risk and establishes our risk management principles, responsibilities and processes that support the integration of risk management activities across Iress. Our Framework, underpinned by the principles outlined in *ISO 31000: 2018 – Risk Management Guidelines*, aims to foster risk management capabilities and culture at all levels throughout Iress that allows us to identify early warning signals, escalate information and fully appreciate the risks impacting our organisation. Importantly, the benefits associated with a robust Framework include fewer surprises, reduced loss (and increased reward), more efficient decision making and sound governance.

Our Risk Governance structure provides oversight for the effective operation of our Framework through the following bodies:

- The Iress Board, which has ultimate accountability to stakeholders for organisation risk oversight along with overall responsibility for ensuring that an effective risk management framework is established. The Iress Board set clear direction for Iress and provide appropriate risk oversight, having regards for the foundations for good governance in the ASX CGPR.
- The Audit and Risk Committee (ARC) is appointed and authorised by the Board to assist in carrying out its obligations as they relate, inter alia, to risk management at Iress. The ARC reviews material enterprise risks in light of the risk appetite set by the Board to monitor deliverables for ongoing alignment with Iress' strategic priorities.
- The Executive Risk Committee (ERC) supports the Board and ARC and has responsibility for the application of the framework across the organisation.

All employees hold responsibility for incorporating risk management into their day-to-day practices coupled with our operational design that provides clear role responsibilities and position accountabilities. This structure (commonly referred to as the Three Lines Model) enables sound decision making, drives effective risk management collaboration and underpins strong engagement across all roles, ultimately for the achievement of Iress' broader strategic objectives.

12. Insurance

Save in respect of Employer's Liability Insurance, all Iress entities are covered under the Iress group insurance policies. Iress has appropriate levels of cover in respect of these policies.

Type of cover
Crime
IT Liability (Professional Indemnity)/Financial Institutions (Professional Indemnity) Australia only.
Cyber Liability
Public & Products Liability
Business Travel
Voluntary Workers
Employers Liability
Industrial Special Risks (covering material damage and business interruption)

13. Business Continuity

Iress operates in accordance with a business continuity framework which sets out the key principles we follow in order to manage business continuity and mitigate the risk of business interruptions that may arise as a result of unexpected disasters or system failures.

The key objectives of our approach are to:

- minimise the risks associated with business disruption through advance planning, preparation and testing;
- reduce Iress' recovery time when a disruption occurs;
- ensure the safety and wellbeing of Iress' people and clients in the event of a business disruption event; and
- increase Iress' overall operational resilience in response to business disruptions.

We have identified certain key business units which we believe are essential to ensuring business continuity for our clients, and we require each of these units to develop and maintain their own BCPs, detailing the specific procedures they will follow in the event of a business disruption together with recovery strategies and protocols. These key business continuity units are also required to regularly review and test their BCPs, and make necessary changes based on the outcome of such tests.

For confidentiality reasons we do not make BCPs available to clients.

14. Hosting and Disaster Recovery

If the product you are purchasing is hosted on the Iress Cloud Platform, then further details of this service can be found in our 'Iress Cloud Platform - Technical Reference Guide' which is available on the Iress Community.

We also have certain product specific Technical Reference Guides which are available on the Iress Community and include information relating to disaster recovery and backup management (as well as other useful information) relating to specific products.

For copies of all available technical documentation please see:
https://community.iress.com/t5/Technical-Documentation/tkb-p/TechnicalDocumentation