IRIS Financials

Information Security Assurance Statement

Document control	
Version number:	1.0
Owner:	Drew Willson
Date of last update:	20-March-2024
Document type:	Information Security Assurance Statement
Replaces:	Information Security Assurance Statement v0.5
Approved by:	Claire Treadwell
Approval date:	20-March-2024
Data protection impact screening: No PIA required	
Date of next formal review: 1-Dec-2024	

Contents

Information security assurance statement 2

Objective of this document 2

Description of the data processing carried out by **IRIS Financials** 2

Statement of assurance 2

IRIS Financials Organisational Security 3

IRIS Financials human resource security 6

IRIS Financials Access Control 7

Encryption (cryptology) 7

IRIS Financials physical and environmental security 9

Equipment ..... **Error! Bookmark not defined.**

Media handling 10

Operations security 11

Communications security 12

System acquisition, development and maintenance 13

Security in development and support processes 14

Test data 14

Processing locations and international data transfers 15

Supplier relationships 15

Summary of sub-processors ..... **Error! Bookmark not defined.**

Information security incident management 16

Business continuity – Information security aspects 17

Compliance 18

Data Protection – quick reference 18

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS Financials by IRIS with transparency as to the security and personal data compliance of this product from all threats, whether internal or external, deliberate or accidental. This document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS Financials as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS Financials

IRIS Financials is a Financial Management enabling organisations to track spend and budgets. IRIS financials does provide API connectors to other sites such as the Department of Education & HMRC to enable the transmission of accounting data.

- IRIS Financials is an integrated financial management suite that allows our clients accurately record, analyse and report their financial data.
- IRIS Financials software can be hosted on the client's own IT infrastructure in which case financial data is held and processed by the client. If required, the software and Data can be hosted on the PS Cloud hosting in which case software, data and processing is at the specified hosting service.
- Personal data may be shared by clients from time to time with the IRIS Financials Support team/service or Professional services team for software application support and product implementation.
- IRIS Financials integrates with payroll and HR solutions and will typically integrate with software and services are designed to support customers in running payroll services for themselves or their clients and to fulfil their obligations as a UK Employer.
- All data is hosted in UK data centres
- IRIS Financials holds financial accounting data. Which mainly consists of company data
- In some circumstances companies can choose add personal data to the system. For example, the processing of expenses or the creation of a pupil ledger or staff expenses
- Personal data can be held in IRIS Financials sufficient for the purposes of recording expenses and salaries paid to staff members. This may include name, email address, banking information, salary and are processed in accordance with HMRC requirements. In this circumstance personal data may be held in the system. This is likely to include the following:

Employee information	
Surname	Bank Details
Forename	
Date of Birth	
National Insurance Number	
Payroll/ Pupil ID	
Post Code	
Job Title	

Statement of assurance

IRIS Financials will ensure that:

1 We will put in place measures to protect customer information from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
2 We will meet our regulatory and legislative requirements.
3 We will produce, maintain and test Business continuity plans.
4 We will provide information security training to all our staff
5 We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
6 We will monitor compliance with our Information Security Policy.

IRIS ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, passwords-authentication, communication and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

IRIS Financials Organisational Security

Statement of Assurance

IRIS Financials will ensure that:

1 We will put in place measures to protect customer information from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
2 We will meet our regulatory and legislative requirements.
3 We will produce, maintain, and test business continuity plans.
4 We will provide information security training to all our staff.
5 We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
6 We will monitor compliance with our Information Security Policy.

IRIS ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, password-authentication, communication, and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

Organisational security at IRIS Group level

Data protection and information security at IRIS Software Group is controlled by the *IRIS Privacy, Security and Compliance Steering Group*. This group meets at least quarterly and includes:

- Members of the Executive Committee
- The Chief information Officer (CIO)
- IRIS Group IT Director
- IRIS Group Data Protection Officer
- IRIS Group Compliance Manager
- Other key security leads within the company

The Privacy, Security and Compliance Steering Group approves IRIS Group level policies relating to information security and data protection, which IRIS products must comply with. There are three Group

policies and a detailed Information Security Management System (ISMS). The three Group level policies are:

- IRIS Group Data Protection Policy – this sets out the roles and responsibilities for data protection compliance within the IRIS Group. It also sets out the requirement for risk assessment and data protection assessment for all projects and proposals that will change or impact on the handling or use of personal data.

- Information Security and Acceptable Use Policy Summary – this sets out the basic information security and acceptable use standards that all staff within the IRIS Group are required to adhere to.

- IRIS Personal data incident reporting and investigation procedure – this indicates the reporting and investigation procedure for all security incidents that become known or are reported to anyone within the IRIS Software Group.

The above policies are communicated to all staff and relevant external staff within the IRIS Group at least annually, using a dedicated training and policy management platform. Managers responsible for delivering IRIS products and services are required to ensure local arrangements are in place to comply with those policies and to evidence this.

- IRIS ISMS – This is the default security system for IRIS Software Group. All IRIS products must meet or be working towards meeting the standards of the IRIS ISMS except for those which already have their own certification under ISO27001 or any other standard relating to information security and data protection.

Organisational security for IRIS Financials

At IRIS Financials the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering the product to ensure IRIS Financials complies with the IRIS Group policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

For IRIS Financials the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- IRIS Financials Senior Product Manager – Drew Willson
- IRIS Financials Product Owner –Graham Fain
- IRIS Financials Development Manager – Paul Finn
- IRIS Financials Support Services – Tracey O'Brien

The IRIS Financials team keep your data secure by ensuring that appropriate measures are implemented to protect your data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to your data while being stored, transmitted or otherwise processed by or on behalf of IRIS Financials.

Measures are "appropriate" if they have been identified through risk assessment.
Date of last IRIS Financials risk assessment review: 8th February 2024

The IRIS Financials team will ensure adequate records are created and maintained to support compliance verification and inspections and incident response (subject to any limitations set out in our Terms and Conditions).

The IRIS Group Data Protection officer is responsible for providing advice and guidance to the IRIS Financials team and for monitoring our compliance on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner's Office.

Group Operations are responsible for the operation and integrity of IRIS Financials IT systems and for keeping systems reasonably up to date. IRIS Financials are managed in by BlackBox Hosting: https://www.blackboxhosting.net/about-us/certifications/

IRIS Financials' Development systems are managed by IRIS Group IT, supported by the IRIS Financials development team.

The IRIS Cloud Operations team and our hosting provider BlackBox are responsible for the operation and integrity of IRIS Financials' Cloud deployed systems and for keeping systems reasonably up to date.

Asset register: IRIS Group IT records and maintains a register of all assets, relevant to IRIS Financials (including acquired software licences) in a fixed assets system.

Client defined classifications: Client information and materials processed, stored or transmitted by IRIS Financials shall be handled strictly in line with the customer's prior advised classification policies and standards, subject only to legal compliance

IRIS Financials human resource security

IRIS Financials may, under controlled circumstances, have access to your or your customer's data. This is to assist customers with the investigation of support issues and during implementation or services engagements. Access to production data is controlled, monitored and audited by the Cloud Operations team.

Prior to employment

- Staff and contractors are subject to background checks and verifiable references to ensure suitability for any given job role.

- All staff are required to accept our Group Data Protection Policy, Incident Reporting Procedure and Information Security & Acceptable Use Policy.

During employment

- Corporate policies, procedures and training are administered via the IRIS training and compliance monitoring tools (Knowbe4). Compliance with mandatory training courses and acknowledgement of policies is regularly tracked through these tools.

- A formal and communicated disciplinary process is implemented for situations where an employee may have committed a security breach. This process is owned by HR.

Termination and change of employment

- Upon instruction from HR of a person leaving IRIS Financials, that person's access to confidential areas shall be restricted immediately, culminating in:
    - Full removal of access to any part of the corporate network prior to departure.
    - All corporate assets in that person's possession having been returned and or been collected by the relevant Department manager or the Information asset Owner as appropriate.
- In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

IRIS Financials Access Control

Users are granted access to systems and information therein on a need-to-know basis by role and department. This is managed as per the Organisational Security section in conjunction with the Group IT Manager and Information Asset Owner and in accordance with the IRIS Group Access Control Policy.

Access is granted on the least privileged rule basis consistent with an individual's job/role responsibilities. For IRIS Financials, system enforced Password complexity rules ensure that strong passwords are used and Users are responsible for keeping them confidential. Systems and information should be secured whenever left unattended. All administrators have their own accounts, separate from their normal user accounts and all use 2 factor authentication.

- Users can be authenticated using 2 Duo factor authentication if the customer chooses.
- IRIS users cannot access the systems within the hosted environment externally. They must VPN into the IRIS network before they can connect. All of these connections are audited and have 2 factor authentication. The same applies to contractors and vendors.
- The hosted environment is separated from the IRIS network via VLAN.

All static user equipment must be kept in good order and used responsibly; all laptops shall be subject to the IRIS Group Laptop and Tablet policy. Passwords must not be disclosed to colleagues or any third parties. As set out in IRIS Payroll Professional's standard HR Policies all personnel must maintain full conformance with company undertakings in respect of confidentiality.

Access to cloud-based administration consoles for privileged IRIS Financials and IRIS users is mandated with multi-factor authentication. Access is only available though a 'jump box' and not directly from the users systems to the customer system.

Server Operating System Access Control along with change and patch management shall at all times adhere to Microsoft's best practice and shall be administered by the Group IT team in conjunction with the Development managers in respect of their individual department's development and support environments.

All administration systems are monitored and audit trails produced together with email notification to the System Manager of any unauthorised attempts to access the corporate network.

All IRIS personnel involved in the delivery, installation and implementation of IRIS Financials software or product for a client must comply with the Client's security policy and access control mechanisms. In all cases Microsoft's best practices should be followed.

Remote access to a Client's network shall always be subject to Client's prior written (or otherwise validated) consent or request; and must be controlled either by using Client provided VPN and or remote assistance software which utilises SSL and provides a full audit trail.

For the avoidance of doubt, IRIS Financials warrants to Clients that it will not seek to circumvent, compromise or change the Client's security controls, and IRIS Financials will not change the Client's software configurations (without proper authorisation); and no 'back door' password or other method of remote access into IRIS Financials's software shall exist.

Encryption (cryptology)

- All data within the hosted environment is encrypted at rest and in transit.
- All data at rest is held on drives under BitLocker.
- All data transmitted is encrypted using TLS 1.2 or 1.3.

- The customer databases can be encrypted at rest (also know as TDE – transparent data encryption) upon customer request.

IRIS Financials physical and environmental security

IRIS does not maintain physical servers or other infrastructure for IRIS Financials. All infrastructure is hosted by BlackBox Hosting, and as such, IRIS Financials inherits the physical and environmental controls implemented by them. BlackBox Hosting are committed to meeting and exceeding industry standards for IT business security, safety and continuity. BlackBox have various business certifications and have independent third-party assessments that review the company practices, the technology BlackBox provides and also the people behind these services at their data centres. BlackBox Hosting hold the following certifications:

- CSA STAR Level 2 - the CSA STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix. Certification certificates follow normal ISO/IEC 27001 protocol and expire after three years unless updated.

- ISO 27001 - BlackBox Hosting is fully ISO 27001 certified. The ISO 27001 standards help organisations to keep information assets such as financial information, intellectual property, employee details and third-party information, secure. It guarantees that ample controls and other forms of risk treatment are in place to prevent and defend against potential vulnerabilities.

- ISO 20000-1 - BlackBox Hosting maintains a Service Management Service (SMS) that is certified to ISO 20000-1 standards.

- ISO 22301 - ISO 22301 allows BlackBox Hosting to demonstrate their commitment to achieving the highest available international standard for business continuity management. BlackBox Hosting is ISO 22301 certified, which demonstrates the required systems in place to support our customers, and for the provision of SaaS (Software as a service).

- ISO 9001 - BlackBox Hosting has a Quality Management System (QMS) in place to ensure they we supply products and services that meet both regulatory requirements and the expectations of their clients. Their QMS is certified to the ISO 9001 standard. It is also reviewed and updated on a regular basis to help ensure that they continue to meet and exceed expectations.

- ISO 14001 - ISO 14001:2015 specifies the requirements for an environmental management system that an organization can use to enhance its environmental performance. ISO 14001:2015 is intended for use by an organization seeking to manage its environmental responsibilities in a systematic manner that contributes to the environmental pillar of sustainability.

- G-Cloud 12 - BlackBox Hosting is a government approved cloud service supplier through the G-Cloud 12 framework. For public sector departments, procuring services through the G-Cloud framework is more efficient.

- Cyber Essentials + - Cyber Essentials is a government-backed scheme that helps to protect organisations and their customers, against a whole range of the most common cyber-attacks. BlackBox Hosting is Cyber Essentials Plus certified. The ‘Plus’ scheme requires companies to pass a more hands-on technical verification process to be awarded the certification.

Media handling

IRIS Financials staff may only use prior authorised removable media supplied by Group IT. Such media will typically comprise encrypted external drives and memory sticks, all of which are password protected and their use duly monitored by Security software. Unauthorised media handling devices will not work. Individual Client security requirements may from time to time necessitate specific authorisations being prior arranged with Group IT.

Operations security

Change management – The IRIS Financials hosted environment is subject to change control and all changes are subject to approval from the central Change Board.

Capacity management – The current hosting model is to provide dedicated infrastructure per customer. We size a customer infrastructure to the expected workload based on the number of licensed users. Capacity monitoring is performed by the Cloud Operations team and capacity issues are raised with Customer support and the IRIS Financials development team who then investigate and resolve.

Separation of development, testing and operational environments – The production environment is owned and operated by BlackBox Hosting and is physically separated from the development and test environments. Members of the IRIS Financials team must access the production environment using separate credentials from their IRIS account. All access is subject to 2 factor authentication and is audited.

Protection from malware - IRIS Financials utilises MS Endpoint protection with real time scanning enabled. Definitions are downloaded every 4 hours so emerging threats will be detected as soon as possible. If a virus is detected, an alert will be generated by SCCM which will be handled by the central monitoring team. On connection/reconnection to the network all machines are automatically updated. SendGrid is used for email transport and emails are scanned for viruses. Firewalls are employed throughout the IRIS Financials infrastructure and FortiGuard Intrusion Detection is used for URL filtering, anti virus and deep packet inspection.

Back-ups: Backups are the responsibility of BlackBox Hosting. The entire environment is replicated every 15 minutes to a separate data centre. Recovery can be down to transaction level if necessary or point-in-time per customer requirement. Business Continuity and Disaster Recovery tests are scheduled and happen regularly. A 3 2 1 backup strategy is employed: *Three* copies of data – the original and 2 copies. *Two* different types of media and *One* offsite copy. If a customer decides to terminate their IRIS Cloud contract, all backups will be removed 30 days after contract termination.

Event logging - user activities, exceptions, faults and information security events are recorded in the server event logs, which can be examined by administrators.

Protection of log information – Logs and audit trails are subject to normal windows system controls and are accessible by authorised administrators only. All access is logged and audited. Logs are retained for 6 years.

Administrator and operator logs – All system administrator and system operator activities are logged, and the logs protected and regularly reviewed

Clock synchronisation – IRIS Financials customer servers have their clocks synchronised with the IRIS Financials to domain controllers. These are synchronised to external NTP servers.

Control of operational software – All access for the implementation of software is subject must be done with credentials separate from IRIS Financials users normal accounts. All accesses are audited and logged.

Management of technical vulnerabilities – Penetration testing is undertaken in partnership with a 3rd party. Penetration tests are performed at least every 12 months. Results are then examined, prioritised, fixed and retested. Identified Critical or High severities are acted upon immediately and implemented as soon as possible. Critical security patches are implemented within 3 days. Critical vulnerabilities are escalated immediately to board level.

Restrictions on software installations – users are not allowed to install software.

Communications security

Network controls – The IRIS Financials hosted environment is owned and Operated by BlackBox Hosting. All access to the network is tightly controlled, logged and audited. Only authorised access is allowed from authorised locations.

Security of network services – Access is limited to IRIS employees only and the auditing is contained within BlackBox Hosting.

Segregation of networks – The IRIS Financials hosted environment is owned and operated by BlackBox Hosting. All customer infrastructures are isolated from each other and no lateral movement is possible. The IRIS network and the hosted environment are physically separated.

Electronic messaging - IRIS Financials staff must comply with the IRIS group IT Acceptable use policy. The IRIS Financials support team procedures & this security policy mandate that any PII must be sent via encrypted (Egress) email.

Confidentiality or non-disclosure agreements - As required, IRIS Financials uses NDAs and maintains signed agreements to protect confidentiality.

How we transmit confidential information to customers

- No confidential information is sent between IRIS and the customer during onboarding as users register directly on the system.

Training is carried out on-site or virtually and no confidential data is shared

Information transfer policies and procedures – where information needs to be transferred securely between IRIS Financials and our customers, the files section in the customer support portal will be used.

Agreements on information transfer – Occasionally, IRIS Financials will need to take a copy of customer data for fault resolution. This is always done with the explicit written consent of the customer. Data is anonymised before use and all data will be destroyed once investigations are completed.

System acquisition, development and maintenance

IRIS Group IT are responsible for the implementation and management of VPN access, Firewalls and the use of encryption and other security measures to ensure the protection of IRIS Financials systems and connected services when new systems are implemented or changed. The IRIS secure development lifecycle ensures that security is considered at all stages of the development process, from requirements, development, testing, implementation and operations.

Within the IRIS Financials hosted environment BlackBox Hosting are responsible for implementing new hardware, with IRIS Financials Cloud Operations responsible for implementation of operating system, network services and security.

The IRIS Cloud Operations team are responsible for ensuring that appropriate security mechanisms and segregation is in place, together with appropriate service levels for cloud hosted services.

All access to the IRIS Financials applications across public networks is secured and encrypted using the latest industry accepted standards.

Security in development and support processes

IRIS Financials staff specialise in the development and support of software systems and are privy to confidential information and potentially personal data which is subject to the General Data Protection Regulations. We ensure that our software and services are designed with robust information security at their core. This includes coding for security for both desktop and cloud services and in particular with reference to OWASP security guidelines. The IRIS secure development lifecycle ensures that security is considered at all stages of the development process, from requirements, development, testing, implementation and operations. Security scanning tools are used at various stages of the development lifecycle and identified issues are captured, analysed, prioritised and remediated as part of normal development activities.

The IRIS Financials cloud service is subject to annual 3rd party security penetration testing, performed by NCC Group, and vulnerability scanning to ensure it remains secure. Results are then examined, prioritised, fixed and retested. Identified Critical or High severities are acted upon immediately and implemented as soon as possible. Critical security patches are implemented within 3 days.

All IRIS Financials developed software must incorporate appropriate controls and audit trails or activity logs.

All source code for Iris Financials products must be treated as highly confidential and all personnel with authorised access must strictly adhere to the use of the appropriate IRIS development tooling for the purposes of checking code in and out.

All versions due for release to any client must have prior undergone IRIS Financials QA and release management process to ensure that changes to issued software are controlled, have been thoroughly tested and are to a high quality. Test plans are stored as part of the development process. Automated tests are built to help ensure future changes do not impact the application.

Changes to Cloud production systems must have been well documented and tested and have been approved by a central change board. All changes to production systems are only via approved routes, either manually via a secure jump box where access and administrator actions are logged and audited or by automated deployment mechanisms.

Test data is based on sample test data as a rule. Occasionally, production derived data may be used but its use is carefully protected and controlled and any such data is destroyed once testing is completed.

Clients must always be advised to maintain suitable facilities for testing and training purposes separately from their live environment. System changes must be reviewed and tested as agreed between IRIS Financials and the Client.

IRIS Financials cloud servers and all other equipment containing confidential information, personal data or source code must be ring fenced. All source code must be stored in central repositories to which physical and logical access is closely monitored. All desktops and laptops, whether static or mobile, shall be fully encrypted using BitLocker and only authorised encrypted media handling devices can be used.

All major changes are subject to internal acceptance testing and customer facing pilot programmes before being rolled out to the customer base.

Test data

All test data used for system testing is internally generated. On rare occasions, customer data sets may be used. This is only with the express prior approval of the customers involved and will be anonymised before use. This data will be destroyed once testing is completed.

Processing locations and international data transfers

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & vulnerability management. In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it. All relevant security requirements have been addressed and further information is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

Supplementary measures for personal data processed in India

IRIS and its engineers in India adhere to the standards of ISO 27001 and uses privileged access management controls to audit activity of engineers. VPNs and Bastions are used where appropriate and all communications are over encrypted channels. IRIS has an international data transfer agreement in place with all sub-processors used that are based in India. This requires them to comply with IRIS data protection and security policies and standards, particularly in relation to handling requests from official sources.

Data processing for IRIS Invoice Matcher (IIM) is carried out in the Microsoft Azure North Europe-Ireland data centre in Dublin, Ireland. Kofax (now called Tungsten Automation), are subject to the same data protection arrangements as IRIS.

Supplier relationships

Partner	Primary Contact	Primary Contact Title	Primary Contact Email	Core Functionality / Markets	Software	Services	Support	Data processor
Calumo	**Michael Sullivan**	**CEO**	Michael.Sullivan@insightsoftware.com	Business Intelligence	Yes	No	No	No
Kofax	**Tim Frazer**	**Sr. Sales Account Executive**	tim.frazer@kofax.com	Account Payable Automation	Yes	No	No	Yes
SBS	**Leyla Tovey**	**Director**	ltovey@schoolbusinessservices.co.uk	School Financial Planning and Budgeting	Yes	Yes	Yes	Yes
Juniper Education	**Gavin Freed**	**Chairman**	gavin.freed@junipereducation.org	HR & Payroll for Education	Yes	Yes	Yes	Yes
Solution 7	**Simon Miles**	**Managing Director**	simon.miles@solution7.co.uk	Excel add in that integrates with IRIS Financials	Yes	No	No	No
Amazon Business	**Vivek Agarwal**	**Senior Partner Manager**	agaviv@amazon.co.uk	Purchasing integration with Amazon Business	No	Yes	No	Yes

Confidentiality or non-disclosure agreements – as required, IRIS Financials uses NDAs and maintains signed agreements to protect confidentiality.

Agreements on information transfer – The IRIS Financials standard terms of business and EULA contain agreements on information transfer between IRIS and the customer and the parties' roles/responsibilities under data protection legislation. Additional data processing agreements with sub processors are maintained to ensure compliance with regulations.

As part of IRIS Software Group, IRIS Financials abides by the group supplier data protection assessment policy. This policy ensures that suppliers who may have access to customer data are properly & regularly assessed, published to those customers whose data may be involved and engaged under a data protection compliant contract.

BlackBox hosting own and operate the servers and infrastructure for the PS Cloud service. Please see the section on **Error! Reference source not found.** for more information. The services provided by BlackBox hosting are monitored to ensure that adequate performance is maintained.

Information security incident management

In the event of an information security incident IRIS Financials follows the IRIS Group incident management policy.

Personal data incidents are investigated by the IRIS Financials team and in accordance with the IRIS group Incident Reporting and investigation procedure.

In the event of any critical incident that threatens or may reasonably be construed as threatening the information security of a client or the continuity the IRIS Financials service to any set of clients, such critical incident must be immediately reported to the Critical Incident Manager and or the Information Asset Owner.

Business continuity – Information security aspects

The IRIS Financials cloud hosted environment is owned and operated by BlackBox Hosting therefore disaster recovery, hardware fail-over and information security continuity are managed by them.

BlackBox Hosting have designed a resilient infrastructure with the following features:

- All servers are Virtual Machines, the host servers are all over-specified and if any single host fails, the remaining are all capable of running the load.
- There are 12 Remote Desktop Protocol (RDP) gateways all load balancing and any two of which could maintain the average daily load.
- There are 3 Domain controllers each hosting AD services, as well as the internal Domain Name System (DNS).
- Any customer with more than 20 contracted RDP accounts has multiple RDS Servers allocated, designed to handle the load if any server is missing from a group of servers.
- All disks in the primary data centre are Solid State Devices, all configured with 3PAR redundancy.
- The primary data centre has its own Uninterrupted Power Supply (UPS), backed up with on-site diesel generators and 5 day's supply of diesel. The secondary data centre is serviced to the same standard and located 40 miles away. Each data centre is serviced by 6 internet providers, any two of which are active at any point in time.
- If any virtual server is detected as having failed, it is automatically restarted. All virtual servers are replicated to our secondary data centre on an hourly basis. All transient data is replicated to the secondary data centre on an hourly basis.
- In the event of a catastrophic disaster (Explosion, Flood etc.) at the primary site, the whole infrastructure will continue to be delivered from the secondary site, the latest data backups are applied and the externally facing non-geographical IP addresses are repointed. This process may take up to 48 hours to complete from a completely cold start, but there will be no changes required from a customer perspective.

Compliance

As a developer and implementer of Software and provider of Support Services and, as part the IRIS software group, IRIS Financials will have access to personal data and or other confidential information. This may be held on Clients' systems or transmitted or otherwise made available to IRIS Financials from time to time.

IRIS Financials and IRIS Group comply with industry, legal and contract requirements and maintain and protect information records compliant with Companies House, HMRC and IRIS group document retention policy.

Personal data is at the heart of the General Data Protection Regulation ("GDPR").

Article 5 of the GDPR sets out six key principles. These specify that personal data must be:

1 Processed lawfully, fairly and transparently in relation to the data subjects.
2 Obtained for specified and lawful purposes.
3 Adequate, relevant and not excessive.
4 Accurate and up to date.
5 Not kept any longer than necessary.
6 Processed securely, with integrity and confidentiality.

Principles 2, 5 and 6 especially apply in respect of IRIS Financials access to personal data which shall be for the sole purposes of implementation, support and maintenance of Software supplied to Clients ("IRIS Payroll Professional's Services").

Where IRIS Financials is in possession of information about, held by or belonging to a Client that is by its nature confidential, or is designated as such by the Client (whether in writing or orally), IRIS Financials is obliged to:

(i) keep it confidential
(ii) use it only in connection with IRIS Financials Services; and
(iii) not disclose it to any other person without the Client's prior written consent.

IRIS Financials warrants to its clients that their use of IRIS Financials software will not infringe any copyright, patent or trademark right, or any other proprietary right, or constitute a misappropriation of any trade secret, of any third party. IRIS Financials also warrants that its software will be free of any harmful code. Encryption is used to ensure security of PII in all public data transmissions Egress and https plus VPN for access to networks. Cryptographic keys are maintained securely throughout the lifecycle in accordance with the IRIS encryption policy.

Information security reviews

ISO27001 certification is audited annually by an external assessor. Internal compliance with Group ISMS is also annually reviewed. Annual external 3rd Party Penetration testing is carried out for IRIS Financials hosted services with regular vulnerability scanning.

Data Protection – quick reference

IRIS Group Data Protection Officer – Vincenzo Ardilio – dataprotection@iris.co.uk

Data protection owner for IRIS Financials – Drew Willson – drew.willson@iris.co.uk

The following categories of personal data may be processed as part of the IRIS Financials product/service provision:

Customer Clients – Contact Details: addresses, email addresses, Phone numbers

Customer Clients – Financial information: Bank account information, Bank account number(s), Financials transactions

Customer Employees – Browsing Information: Cookies

Customer Employees – Contact Information: Address, Email address, Phone numbers

Customer Employees – Financial: Bank account information, Bank account number

Customer Employees – Personal Identification: First name, Surname

Customer Employees – Travel & Expense: Expense details, Travel history, Car information

Customer Employees – User Account Information: Account password

The above data is processed as part of the normal operation of IRIS Financials for payment of suppliers, staff expenses and salaries, login to IRIS Financials and related products

Additionally, the following data may be processed for the operation of eProcurement integration with 3rd party suppliers:

Date/time of transaction, Partner name, Customer code, Iris order reference, 3rd party order reference, Gross order value, Net order value

Location of personal data processing, hosting and access by IRIS agents

IRIS Invoice Matcher data is processed and stored in the MS Azure in Dublin, Ireland. All other IRIS Financials data is stored and processed within the UK.

IRIS Financials data pertaining to IRIS Analytics or IRIS Financials reporting will occasionally be accessed by IRIS KPO in India for resolution of support tickets. All access is via a secure online portal and is logged and regularly audited.

Retention of data

- Data is retained as long as the customer has a valid service agreement for IRIS Financials.
- If a customer cancels their agreement for IRIS Financials Cloud Services, they have 30 days to request copies of all their data, after which time their customer setup for software and databases, including all backups, is deleted from the IRIS Financials Cloud system, ensuring all personal data is removed.
- If a customer is running IRIS Financials as a local 'on premise' installation and cancels their agreement with IRIS Financials, the Customer is asked to remove all related software from their systems.
- No paper copies of customer data are held at any time by IRIS Financials. Access is solely via our secure systems for the purposes of guaranteeing Project Partners' full and comprehensive use of the system and to realise our aim of effective, first class customer service.
- In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may disclose personal data to respond to court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. We may also share such information with relevant law enforcement agencies or public authorities if we believe same to be necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms and Conditions, or as otherwise required by law.
- Data can normally be deleted by the customer, but if there are any data that cannot be deleted, it can be requested by raising a ticket with IRIS Financials customer support.
- Backup data is normally held for 3 months (1 month of daily backups, and 2 extra monthly backups). Data older than 3 months is automatically deleted by an aging out process.

Data subject rights

All data subject access requests should be referred to our online terms and conditions and data processing terms on the IRIS website:

http://www.iris.co.uk/assets/Terms/IRIS-General-Terms-Conditions.pdf

http://www.iris.co.uk/assets/Terms/IRIS-Customer-Data-Processing-Terms.pdf

In general, if a customer needs to deal with an access rights requests e.g. where someone wants access to all the data held by IRIS Financials, this can be done in-product. If it is not possible, a ticket can be raised with IRIS Financials customer support and the relevant data will made available/deleted etc. This will normally be done within 5 working days.