IRIS KashFlow

Information Security Assurance Statement

Document control
Version number: 7.0
Owner: Masih Ahmed
Date of last update: 09/05/2024
Document type: Information Security Assurance Statement
Replaces: Not applicable
Approved by: Paul Onions
Approval date: 26 Mar 2024
Data protection impact screening: No PIA required
Date of next formal review: February 2025

Contents

Contents

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of KashFlow 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. Also this document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS Software Group as a thoroughly secure software and service provider.

Description of the data processing carried out by **IRIS KashFlow**

- IRIS KashFlow is a SaaS web application, hosted with Rackspace servers.
- The product is designed to allow end user businesses to run their business in the cloud such as managing Customers i.e. sending them quotes and invoices – and collecting payment for these invoices using a payment solution as well as their Suppliers i.e. sending them Purchase Orders and Purchase Invoices.
- Personal data stored and processed by IRIS KashFlow is sufficient for the purposes of facilitating effective bookkeeping.
- The subjects of the information being processed is limited to end user businesses (employees in a business) and where appropriate their bookkeepers and their accountant (staff members).
- Personal data for end user businesses stored includes company name, first name, last name, email address, mobile or landline numbers. For clients it could be the client email, postal address and contact information.
- Personal data may be included within the files being exchanged between accountancy customers and their clients. The customer is in full control of the data shared unless the accountant has not provided the end user business with KashFlow access i.e. they provide a full bureau service

Statement of assurance

IRIS KashFlow 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 KashFlow Organisational Security

IRIS KashFlow is part of the IRIS Software Group.

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 KashFlow

The product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering IRIS KashFlow to ensure IRIS KashFlow 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 KashFlow, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- Masih Ahmed – Product Manager
- Carly Barton – Engineering Lead
- Thomas Derbyshire – Support Lead
- Paul Onions – Product Director

The IRIS KashFlow 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 KashFlow.

Measures are “appropriate” if they have been identified through risk assessment.
Date of last IRIS KashFlow risk assessment review: October 2023. Last Penetration Test 15th January 2024

The IRIS KashFlow 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 KashFlow 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.

IRIS Development Operations are responsible for the operation and integrity of IRIS KashFlow’s IT systems and for keeping systems reasonably up to date.

IRIS KashFlow’s Development systems are managed by IRIS Group IT, supported by an offshore engineering team.

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

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

IRIS KashFlow human resource security

IRIS KashFlow employees may, under controlled circumstances, have access to your customer's data, and that of their clients', this is to assist customers with the investigation of support issues. Access to production data is controlled by requests to the Operations team and read only access is granted. The production data is also encrypted to protect sensitive data.

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 Meta Compliance portal (now Known as Knowbe4)

- 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 a role that involves IRIS KashFlow, that person's access to confidential areas shall be restricted immediately, culminating in:
    - Full removal of access to any part of the corporate network
    - 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.

KashFlow Access Control

- IRIS KashFlow is password protected requiring a minimum of 5 characters and containing a mixture of upper- and lower-case characters, special characters and numbers.
- The password rules are enforced through the software
- Multi-factor authentication is required utilising a memorable word and can be enabled by an accountant's admin and this is enforced for all users linked with that account.
- In KashFlow, there are 5 roles: A Master Administrator, Standard, Manager, Sales, Purchasing and Basic user

    - Master Admin - full access to all areas
    - Standard - full access to all areas, excluding the ability to manage users
    - Manager - full access to all areas excluding banking and manage users
    - Sales - access to customers, quotes and invoices, but not to add sources, projects, accounts (to the chart of accounts) or to manage stock
    - Purchasing - access to suppliers, purchase orders, purchase invoices, but not to add projects or accounts (to the chart of accounts)
    - Basic - access to customers, quotes, invoices, suppliers, purchase orders and purchase invoices, but not add sources projects, accounts (to the chart of accounts) or manage stock.

- In KashFlow Connect there are 2 roles – A Master administrator and a Client Manager.
  - Master Administrator: Full Access
  - Client Manager: do not have access to detach client, global client settings, manage additional users, branding setting and any other feature the Master Admin doesn't want them to have access too

- The audit trail will show what the amendments were, when they happened and the user who performed the changes.
- Our support team will ask for the user to confirm their name and one of the following: their address and email address.

LogMeIn is used by our Support team if there is a requirement to remotely connect to a user's device. Remote connections are recorded. Any personal data that may be displayed on the user's device would be captured during the session. Customers have a measure of control over the use LogMeIn. For example, customers may instruct their users not to accept remote connections from our Support team, but this would have an impact on the level of support that can be provided.

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

IRIS KashFlow has ISO 27001 Certification

- **User registration and de-registration** – There is a formal registration and de-registration procedure with records of shared user ID approvals
- **User access provisioning** – The user admin area access is provision based on roles and permissions. The various roles exist are Support, Sales senior, Finance etc. These roles are based on job role requirement.
- **Management of privileged access rights** – The allocation and use of access privileges are restricted in multi-user information system environments. The privileges are allocated on need to use basis. An account creation and access allocation is done through an ops ticketing system.
- **Management of secret authentication information of users** – The passwords are hashed and controlled through a formal management process. The users have been asked to go through the 2 step authentication process while logging into the application. Also, the users required to accept the terms and conditions on first time login or whenever the terms and conditions are gets updated.
- **Removal or adjustment of access rights** – On change of employment users won't be able to access the internal applications. The access will be revoked automatically.

- **Secure log on procedures** - The access to information system is attainable only via a secure log-on process.

- **Password management system** - There exists a password management system that enforces various password controls such as individual password for accountability, store passwords in encrypted form, not display passwords on screen or in plain text.

- **Access to program source code** – The tools like Snyk and SonarQube are in place to check for any vulnerabilities.

Access to a user's account becomes available after obtaining consent from the user to log in for support-related activities. Once support access is enabled, individuals with access and appropriate permissions in the admin app can impersonate and log into the user's account. The granted support access will automatically expire after a few days.

Encryption (cryptology)

- KashFlow data and documents pertaining to customers and their clients is encrypted at rest using industry accepted best practices. This is currently Argon 2 encryption.
- All communications between the KashFlow service(s) and end users are encrypted using industry accepted best practices. This is currently TLS 1.2.

All encryption methods are reviewed regularly and upgraded as technology improves.

IRIS KashFlow physical and environmental security

IRIS does not maintain physical servers or other infrastructure for IRIS KashFlow. All infrastructure is hosted by Rackspace, and as such, IRIS Rackspace inherits the physical and environmental controls implemented by Rackspace. Details may be found on the Rackspace website https://www.rackspace.com/en-gb/compliance

Access to IRIS resources and equipment is subject to Group IT Policies.

Operations security

- **Documented operating procedures:** Confidential data like bank transactions is not accessible directly. The SOP is in place to support operational activities.

- **Change management:** The production updates are governed by CAB (Change Approval Board).

- **Capacity management:** The production environments are monitored on regular basis with the tools like DATADOG and SQL monitor.

- **Separation of development, testing and operational environments:** The environment segregation is in place Example: Feature, UAT, staging and production.

- **Protection from malware**: Only DevOps have the rights to access the production environments limiting the exposure of log availability. We also ingress the Windows Application , System , Security logs and product logs into our external monitoring system Datadog for 15 days. Logs digested into Datadog are immutable and there for tamper proof. Logs are also transferred to our SumoLogic system which hold logs for 15 months with the same setup as Datadog.

- **Back-ups:** *The backup of all processing server systems falls under the remit of the Group IT Director. Dev* Ops back up books database and get restored in Support Keybooks on daily basis (override on daily basis). The SQL servers for KashFlow are in a Managed Back Up area within Rackspace which means there is a daily differential / incremental backup with a weekly full backup and is held on a rolling 28 days offsite..

- **Event logging:** DATADOG is being used for this purpose.

- **Protection of log information:** Only DevOps have the rights to access the production environments limiting the exposure of log availability. We also ingress the Windows Application , System , Security logs and product logs into our external monitoring system Datadog for 15 days. Logs digested into Datadog are immutable and there for tamper proof. Logs are also transferred to our SumoLogic system which hold logs for 15 months with the same setup as Datadog.

- **Administrator and operator logs:** As above for the logs locations etc however we also perform "Privileged Access Reviews" on a regular basis, we also are in the process of implementing a Privileged access management system (PAM) system CyberArk in the coming weeks.

- **Clock synchronisation:** All servers are set via group policy using synchronized time servers set within the DC settings. These point to verified external time sources on the GMT - London time set.

Capacity management

- Smoke tests on the test environment are performed to ensure the system continues to run at Optimum levels
- Engineering Team actively seeks to identify performance bottlenecks in an effort to drive down the footprint of the system
- App insights is used by the team and Operations to Monitor Production

Separation of development, testing and operational environments

- The Production environment is separate to the Development and testing environments which are both individual environments

Control of operational software

- Any changes to the software require CAB approval before they can be released to production.

Management of technical vulnerabilities

- Pen testing is typically done once a year by an external company and this was last performed on 15/01/2024.
- The team consult the IRIS Group Security Architect if required in relation to any security issues and vulnerabilities should they arise.

Communications security

Network controls

- IRIS KashFlow is hosted on Rackspace which employs pessimistic security to ensure 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 Rackspace.

Segregation of networks

- IRIS KashFlow is hosted on private Rackspace infrastructure and uses separate infrastructure for development, test, and production environments.

Transmission of 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.

System acquisition, development and maintenance

- Before features are developed, or changed, an Architecture Review Board reviews and approves the technical architecture being proposed. If changes are required these are fed back to the teams. This process includes a full security review including, but not limited to attack surface & vector analysis and encryption requirements.

- All data transfer within the KashFlow application infrastructure is secured and encrypted using the latest industry accepted standards. Similarly, all access to the KashFlow application across public networks is secured and encrypted using the latest industry accepted standards.

Security in development and support processes

- Security is considered at all stages of development. Designs are taken (when necessary) to an Architecture Review Board which helps direct any security concerns to the Security Architect

- Jira is used to specify and track work. Requirements are fed into teams by Product Owners / Manager and prioritised by the Product Owner/ Manager. Jira tickets are worked by the teams and must meet a documented Definition of Done before they are accepted. Changes are demonstrated to Product Owners, Product Managers and wider stakeholders.

- Testing is performed and documented throughout the development process. Automation tests are built to help ensure future changes do not impact the application.

- Documented principles and procedures are stored in Confluence. Any gaps are identified during the design process and added to the documentation.

- 3rd party platforms such as Rackspace are Risk Assessed and approved by Group IT. Development environments are secured using the standards set by Group IT. Development approaches are assessed by a Security Architect.

- 3rd party development resource is contractually obliged to meet IRIS standards for security and testing. IRIS retains the IP for all work performed. Work performed by 3rd party developers is processed through the same pipeline as internal developers with the same automated security checks etc.
- KashFlow applications are regularly penetration tested.

- Test procedure is documented in a Master Test Plan. Individual tests and test results are documented within Jira and TestRail.

Test data

- All test data is depersonalised/obfuscated before being used in test environments. Developers and testers do not have access to production data.

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.

Supplier relationships

Information security in supplier relationships

Information security policy for supplier relationships: Development, bug fixing and enhancements for IRIS KashFlow are carried out by a team in Cybage. All Cybage employees have the same checks and follow the same compliance procedures as FTE employees. Any customer data shared with Cybage for purpose of bug fixing is scrambled unless specific authorisation from the customer is attained first.

Supplier service delivery management

Monitoring and review of supplier services: Managing changes to supplier services –If a new supplier needs to be selected for any reason, IRIS follows a Supplier due diligence process which assesses any potential supplier data protection and security arrangements.

Managing changes to supplier services: IRIS has a supplier management policy and each product has a Customer Assurance Statement which details the third-party suppliers involved with any one product, where updates to our suppliers or agreements are notified to customers with updates to that document. We also as a company, use OneTrust as a platform to manage supplier due diligence and security questionnaires for suppliers on onboarding and by annual review.

List of third parties and sub-processors involved in KashFlow service processing customer data correct as at 19/01/2024

The following payment processors are used to facilitate the online payment of customers' client's invoices.

- Global Payments
- UNIpaaS
- IRIS Pay
- GoCardless
- Worldpay
- Square
- Stripe
- PayPal

PayVector (also know as AI Coropration) is used to take Subscription payments

KashFlow has an integration with Zapier a third party which automates the creation of customers and invoices with KashFlow

KashFlow has an integration with cloudPOST – allowing users to print and post their invoices to their clients

KashFlow has an integration with Dropbox allowing users to store documents

KashFlow Connect has an integration with Openspace allowing Accountants to upload documents securely

Information security incident management

Management of information security incidents and improvements

- In the event of an information security incident, KashFlow follows the IRIS Group incident management policy.

- Personal data incidents are investigated by the KashFlow 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 KashFlow service to any set of Clients, such critical incident must be immediately reported to the Critical Incident Manager and or the Information Asset Owner.

Compliance

Information security reviews

- IRIS KashFlow is not hosted at premises maintained by IRIS. Disaster recovery, hardware fail-over and information security continuity is managed by Rackspace.
- Infrastructure configurations are stored and managed as 'images' and all code and application configuration is stored and managed within version control software. This is currently Rackspace. -

Data Protection – quick reference

- IRIS Group Data Protection Officer – Vincenzo Ardilio

  dataprotection@iris.co.uk

- Data protection Manager for IRIS KashFlow– Masih Ahmed –

  masih.ahmed@iris.co.uk

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

All KashFlow data will be stored and processed within the UK and Western Europe.

Retention of data

Data will be stored in IRIS KashFlow until such time as a customer deems it no longer required or is required to remove it. Currently, customers are able to delete client data from IRIS KashFlow.

KashFlow reserves the right to delete expired account data greater than two years

The customer is responsible for exporting their data should they wish to leave KashFlow

Ops back up books database and get restored in Support Keybooks on daily basis (override on daily basis). The SQL servers for KashFlow are in a Managed Back Up area within Rackspace which means there is a daily differential / incremental backup with a weekly full backup and is held on a rolling 28 days offsite.

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