Product name: **KashFlow Payroll**

Information Security Assurance Statement

Document control	
Version number:	4.0
Owner:	Craig Worton
Date of last update:	28th March 2024
Document type:	Information Security Assurance Statement
Replaces:	Information Security Assurance Statement – 22nd November 2023
Approved by:	Fran Williams
Approval date:	28th March 2024
Data protection impact screening: N/A	
Date of next formal review:	2nd November 2024

Document Control

Version	Date	Amendment	Amended by	Role
1.0	13/08/2020	Initial Document created	Leanne Oxley-Hold	Product Owner
2.0	21/11/2022	Review draft and update in accordance with the new Customer Information Security Template	Claire Treadwell	Product Director
	22/11/2022	Draft amendments & outstanding questions regarding roles	Craig Worton	Product Owner
	23/11/2022	Draft amendments & outstanding questions regarding architecture	Marko Kennedy	Senior Architect
	20/01/2023	Final amendments after DPO review	Claire Treadwell	Product Director
3.0	24/11/2023	Document Update	Craig Worton	Product Owner
4.0	28/03/2024	Document update to add *Processing locations and international transfers*	David Kisiaky	Product Manager

Contents

Information security assurance statement (ISAS)

The objective of this document

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

Description of the data processing carried out by KashFlow Payroll

- KashFlow Payroll is an online payroll solution provider, designed to simplify the process of paying employees.
- The product is a web-based product hosted in UK data centres, and processes all data necessary to provide HMRC with the correct information for running an employee's payroll.
- Types of personal data fields include full name, date of birth, national insurance number, and any attachment of earnings or additional payslip items, as required for the running of payroll.
- We hold data for System Administrators running payroll on the KashFlow Payroll system, and any employees whose data is processed on the system.

Processing locations and international transfers

- On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security and 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.

Statement of Assurance

KashFlow Payroll 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.

KashFlow Payroll Organisational Security

KashFlow Payroll 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 ***Risk Steering Committee***. 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 Risk Steering Committee approve 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 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 (MetaCompliance). 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 KashFlow Payroll

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

- KashFlow Payroll Product Owner – Craig Worton
- KashFlow Payroll Development Manager – Chris Ruddy
- KashFlow Payroll Support Services – Rachel Wadsworth

The KashFlow Payroll team keeps 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 KashFlow Payroll.

Measures are "appropriate" if they have been identified through risk assessment.
Date of last KashFlow Payroll risk assessment review: 16/11/2022

The KashFlow Payroll 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 KashFlow Payroll team and for monitoring our compliance with 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 KashFlow Payroll's IT systems and for keeping systems reasonably up to date. Some sections of KashFlow Payroll are managed in Microsoft Azure, compliance documents for Azure can be found here https://docs.microsoft.com/enus/azure/compliance/.

KashFlow Payroll's Development systems are managed by the local development team based in the UK.

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

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

KashFlow Payroll Human Resource Security

KashFlow Payroll staff will have access to your data. But will only access your data when necessary, for example dealing with ticket you have raised with support, that requires further investigation.

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

- KashFlow Payroll managers are made aware of their responsibilities to ensure that established policies and procedures are adhered to by external parties, contractors, and employees through the use of internal audited MetaCompliance training
- KashFlow Payroll employees, third parties, and contractors receive appropriate awareness training and regular updates in organisational policies and procedures as relevant to their job function
- Corporate policies and training are administered via MetaCompliance
- A formal and communicated disciplinary process is implemented to handle KashFlow Payroll employees who have committed a security breach

Termination and change of employment

- Upon instruction from HR of a person leaving KashFlow Payroll, 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 Group that person's access will be varied accordingly
- All development is carried out in-house and no external contractors or parties have access to your data

KashFlow Payroll Access Control

The following levels of user exist within the KashFlow Product:

- **Development System Administrator** – Access to all tabs and all functions. Limited to owners of the KashFlow Payroll Product on a needs only basis. No direct access to customer data, but can view customer user accounts in order to resolve issues and help support the product
- **Customer User Manager** – Customer access to create and maintain user access rights at tenant level. Can access all areas of the KashFlow Payroll System, within own Tennant. Cannot access any other data for other tenants.
- **Employee** – has no ability to access, change or amend anything in KashFlow Payroll. Employee accounts are managed by the account manager
- **Support** – the ability to carry out limited functions to help with customer queries and to view account details. Support accounts are granted internally by the KashFlow development team

Review of user access rights – We encourage customers to regularly review user access to ensure that accounts access rights are maintained and remove access no longer require access, such as those who have left the company.

Use of privileged utility programs – System Administrators can control user access rights from within the product.

Password management system - User access to the application is granted via username and password. Password strength policy is enforced via the software. Passwords are encrypted and hashed using the Argon2 algorithm in the KashFlow Payroll database.

KashFlow Payroll account holders can request to change the email address of the registered account in the unlikely event they are unable to change it within the software, (such as the current account holder has left the company at short notice). KashFlow Payroll Support has procedures in place to verify the authenticity of the request together with a list of required identifiable information of the original account holder and company. The Support Team maintains an audit trail in such cases.

Internal system access control

KashFlow Payroll developers have access to internal development systems and data. Operations staff have access to production databases. All are accessed through windows authentication (linked to the internal movers /leavers process) unless otherwise stated.

- **Management of secret authentication information of users** - Secure log-on procedures – All internal accounts must use two-factor authentication to access any internal systems. 2Factor Authentication sessions expire every few days
- **Management of privileged access rights** - Privileges are allocated on a need-to-use basis; privileges are allocated only after the formal authorisation process
- **Removal or adjustment of access rights** - All employee access is managed through the formal employee starters / internal movers / leavers processes
- Access to systems is requested by the KashFlow Payroll Development Manager via an internal support ticket to operations
- Access to source code is managed via internal code repositories with these accounts and the above request process, all code is peer-reviewed
- **Access to program source code** - Deployment of code is automated through an approved and gated process to negate the need for KashFlow Payroll developers to have any access to the production systems
- **Secure log-on procedures** - Access to any environments with customer data is additionally controlled through the use of VPNs and IP restrictions

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

Encryption (cryptology)

KashFlow Payroll enforces the TLS 1.2 protocol on all connections to the application.

KashFlow Payroll physical and environmental security

No servers are held at any IRIS premises. The following datacentres are used with accompanying compliance documents:

- **ByteMark** – used for hosting development environments - https://www.bytemark.co.uk/company/certifications/
- **Rackspace -** used for hosting production environments - https://www.rackspace.com/en-gb/compliance
- **Azure** - used for hosting some reporting sections - https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance

Equipment

All IT equipment has an enforced lock policy, where passwords are managed by multi-factor authentication. All IT equipment is maintained properly. Disposal of equipment or media handling devices shall be in strict accordance with WEEE recycling standards and be fully certificated by Safe PC Disposal (SPD). Destruction of confidential information (in paper form) shall be affected and certificated by Shred IT. Safe PC Disposal (SPD) Shred IT) are ISO 9001 and ISO 14001 accredited.

All employees conduct annual Acceptable Use training annually which is recorded in the company compliance system, MetaCompliance.

Media handling

Portable physical media is not needed by KashFlow Payroll engineers. In the event of being used in the future, IRIS 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 Security software. Individual Client security requirements may from time to time necessitate specific authorisations being prior arranged with Group IT.

Operations security

Documented operating procedures – Backups, the transmission of information between environments, and equipment maintenance are all fully managed services by suppliers listed in this document. All suppliers are independently audited against ISO 27001 standards.

Change management - Change management controls have been implemented to ensure satisfactory control of all changes. Major architectural changes are reviewed by an architecture review board (ARB) to discuss security, service level, and complexity issues.

System releases are reviewed and approved by the Change Advisory Board (CAB), without approval software releases cannot go live.

Capacity management –The use of resources is monitored, tuned, and optimised, to ensure future capacity requirements continue to perform at optimum levels.

Separation of development, testing, and operational environments – development and production environments are hosted by different companies in different data centres. Access to infrastructure is restricted through IP restriction lists. KashFlow Payroll developers do not have access to production environments. Deployment is automated through automated deployment pipelines.

Protection from malware – IRIS Information Services is responsible for protecting KashFlow Payroll developer machines to protect against malicious software. This is monitored using central processes. Firewalls are in place. Mimecast is used to provide comprehensive email filtering (not only to preclude spam but also to scan attachments more effectively to counteract viruses and other malware).” The protection of production environments is maintained by Rackspace.

Back-ups - Full backups of production databases are taken of the KashFlow Payroll databases every night and before every release. Incremental backups are taken every 30 minutes.

Event logging - Systems are configured for recording user activities, exceptions, faults and information security events.

Control of operational software – Installation of software on KashFlow Payroll production systems (other then the OS that Rackspace is responsible for) is managed through package managers to minimise the risk of corruption of operational systems.

Management of technical vulnerabilities – Penetration testing for KashFlow Payroll is planned annually to be undertaken by a third party. Security is considered during backlog refinement and discussed as part of the overall product backlog and workload. Any changes which have security implicants are reviewed by the Architecture Review Board and implemented in accordance with their recommendations.

Restrictions on software installations – KashFlow Payroll developers do not have access to install any software on production systems. Installation of dependencies is managed by operational engineers through package managers.

Protection of log information – Error, Support, and GP report logs are stored in the system. They reside within the KashFlow payroll database with relevant security and can only be accessed with the relevant database credentials.

Clock synchronisation - Across all IRIS cloud environments, clock synchronisation uses NTP (Network Time Protocol). Typically, this is driven from the hosting provider's connection to an atomic clock.

Communications security

Network security – The IRIS-hosted operations team is responsible for ensuring that appropriate security mechanisms and segregation are in place, together with appropriate service levels for cloud-hosted services (hosted in Azure). All production environments are hosted by Rackspace. Suppliers are appropriately audited and checked for compliance. Access is controlled through IP restrictions, VPNs, two-factor authentication, and the use of firewalls. Application and database servers remain separated with secure communication between servers.

Electronic messaging – IRIS employees are subject to audited training on the appropriate use of electronic communication, particularly with sensitive and/or personal information. In cases where customer information needs to be shared for fault-finding purposes (such as support / develop liaison), these are controlled through restricted access CRM systems requiring multi-factor authentication.

Confidentiality or non-disclosure agreements - As required, KashFlow Payroll uses NDAs and maintains signed agreements to protect confidentiality. The requirements for confidentiality or non-disclosure are identified, reviewed, documented regularly by IRIS, and communicated through training plans.

Agreements on information transfer – The KashFlow Payroll standard terms of business and End User Licence Agreements 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.

How we transmit confidential information to customers
Where customer data need to be reviewed. A support agent will request permission to review the system. This requires express permission from the KashFlow customer. All support activity is logged in the relevant CRM.

System acquisition, development and maintenance

Information security requirements analysis and specification - Information security requirements are considered during backlog refinement by the team. Any significant security implications will be taken to an architectural review board (ARB) with an enterprise architect and a security architect to sign off.
Securing application services on public networks – All services on KashFlow Payroll enforce the use of TLS 1.2 as a communication protocol.

Security in development and support processes

System change control procedures – Major system changes are reviewed by the ARB. System releases are reviewed by the CAB prior to release.

Technical review of applications after operating platform changes – Suppliers such as Rackspace are responsible for updating and security patching application environments critical software like operating systems. Other software requests (such as updates to dependency software) are managed through the product backlog by the development team, approved through a CAB, and tested as with any other release. The IRIS operational team monitors these environments following changes through standard monitoring and diagnostic processes. Quality engineers run weekly regression suits that constantly evaluate the expected behaviour of the application.

Restrictions on changes to software packages – Updates to software packages are strictly controlled through package managers (NuGet and Chocolatey). Vendor-supplied software modifications should be made through standard maintenance. Changes to software development in-house are subject to change control procedures.

Secure system engineering principles - Principles for engineering secure systems have been established, documented and maintained by the IRIS architecture team and are used as part of an internal training plan for all developers (Architecture Corpus).

System testing – All system and application changes are subject to an appropriate combination of manual, automated and regression testing comprised of testing suits managed by the internal quality engineers on the KashFlow Payroll team. All features are tested before being accepted through a series of environments before they enter the production environment.

Secure development environment - The organisation has appropriately assessed the risks associated with individual system development and integration efforts that cover the entire system development lifecycle. Development environments are assessed for suitability and security by the Architectural Review Board.

Test data

Protection of test data - Copies of production databases are not used, and live production data is not used for testing purposes. Development, QA, and staging environments have a series of stock/dummy data and manually entered data of fictitious companies and employees for the use of testing.

Supplier relationships

Information security in supplier relationships

External suppliers (such as Rackspace or Microsoft) do not have access to KashFlow Payroll information. Supplier service delivery management Monitoring and review of supplier services – Rackspace and other suppliers are independently audited by third parties against ISO 27001/9001 standards. IRIS review these audits and SOC reports annually to assess if supplier relationships meet the standards for continuation.

Supplier service delivery management

Managing changes to supplier services – In addition to the assessment of supplier audits, if a new supplier needs to be selected for any reason, the IRIS internal compliance team is responsible for choosing an appropriate supplier based on ISO 27001 standards. After appropriate assessment, the Group Compliance Manager is responsible for such decisions.

Summary of sub-processors

List of third parties and sub-processors involved in IRIS Group has a section 28 EU-GDPR sub-processor agreement in place with RackSpace Ltd which provide UK hosting services for the KashFlow Payroll service. RackSpace certifications include ISO27001, AICPA-SOC (formerly known as SAS70) and PCI-DSS.

IRIS also has sub-processor agreement with Cybage Software Private Ltd for consultancy services. Please Cybage Data Protection Policy here https://www.cybage.com/sites/default/files/2024-04/Cybage_Data_Protection_Policy_10_September_2021_0.pdf

Microsoft Azure compliance documents can be found here Azure compliance documentation | Microsoft Learn. In both cases, these suppliers do not have access to customer data.

Information security incident management

In all instances, any KashFlow Payroll critical incidents (whether relating to information security or not) are managed through the "Critical Incident Management Process", handled, and coordinated by the IRIS Critical Incident Manager. Incidents are prioritised and classified as part of this process. The process outlines stakeholder communication with a focus on customer communication during an incident resolution. A post-incident review is then drawn up by the incident manager and/or Product Manager and corrective actions are logged and tracked to execution. Information security incidents follow this process and will be triaged by the Group Data Protection Officer. The IRIS Group Data Protection Officer will report a summary of all data protection incidents to the IRIS Information & Security Governance Group and maintain a list of learning outcomes and actions arising from incidents, with the aim of ensuring Information Asset Owners follow through on those actions. This process will also be used internally for any issues discovered during development, and training is provided for staff to promote awareness of this process.

Business continuity – Information security aspects

Information security continuity

Information security reviews technical security reviews are carried out on an ad-hoc basis. The ARB reviews any fundamental changes to architectural proposals. Security vulnerability tests aim to be conducted annually. The results of the tests are triaged with the Group Security Architect and prioritised in the product backlog. Wherever possible, automated tests are written within the application to ensure security / compliance changes within the product are part of automated testing.

Redundancies

Availability of information processing facilities – The KashFlow Development team and Dev Ops maintain a list of KashFlow third-party components, any dependencies risk are identified.

Compliance

Compliance with legal and contractual requirements

KashFlow Payroll is HMRC recognised Software and undergoes the HMRC recognition program on an annual basis, to ensure compliance is maintained. Further details around the scheme can be found here: Find payroll software that is recognised by HMRC - GOV.UK (www.gov.uk)

Privacy and protection of personally identifiable information – KashFlow Payroll is subject to the standard IRIS Privacy Policy: https://www.iris.co.uk/privacy-policy/

Intellectual Property Rights (IPR) – Contracts of employment include clauses protecting the Intellectual Property Rights of all IRIS Software Group products

Data Protection – quick reference

Basic Information

Category	Details
Registered/ Postal Address	IRIS Software Group Ltd Heathrow Approach 4th Floor 470 London Road Slough SL3 8QY
Contact details of an authorised EU representative (if applicable)	IRIS Software Group Ltd Heathrow Approach 4th Floor 470 London Road Slough SL3 8QY
Company website	**https://www.iris.co.uk/** Payroll Software | Cloud Payroll | KashFlow
Co Number	02683800
Group Ownership	Owned by IRIS Software Group
Registered with ICO	Yes - https://ico.org.uk/ESDWebPages/Entry/Z3435366
Group Data Protection Officer	**Name:** Vincenzo Ardilio Email: dataprotection@iris.co.uk. Vincenzo is a qualified practitioner with over 20 years' experience. Data Protection Act 2018 / GDPR Practitioner Certificate.
Data Protection Owner for KashFlow Payroll	**Name:** Craig Worton **Email:** craig.worton@iris.co.uk

Types of Data

Category	Details
Personal Data processed	**Customer Clients** Contact Details Phone Numbers First Name Full Name **Customer Employees** Contact Details Home Address Personal Email Phone Numbers Work Email Address **Employee Information** Contract Type Hours of Work Job Title Role Office location Record of Absence/ Time Tracking/ Annual Leave Salary Wage Start Date

	Financial Bank Account Number **Government Identifiers** National Insurance Number (NINO) **Personal Identification** Date of Birth First Name Surname Full Name Gender Martial Status Nationality Unique Perosnal Identifer **Professional Experience & Affiliations** Professional Memberships & Trade Union Membership deductions and expenses may be processed through the system **Travel & Expense** Expense Details **User Account Information** Account Number Account Password **Users** Cookie Information IP Address **Contact Information** Contract Details Personal Email
Purpose for which personal Data is processed under the product/ service	KashFlow Payroll is an online payroll solution designed to simplify the process of paying employees.

Location of personal data

Category	Details
Hosted Environments	RackSpace
Data Centres	All data centres are hosted in the UK
Service provision i.e. Support Services	Support Services are located in the UK

Retention of data

Category	Details
Data Deletion	Customers have control of their own data. Customer can request for all data to be removed, this would be done via the support team. HMRC recommend that data is kept for 5 tax years and current to ensure proper records are kept and maintained. HMRC can ask to review this data for audit purposes.

Data subject rights

Category	Details
Data Deletion	Customers have control of their own data. Customers can request for all data to be removed; this would be done via the support team. HMRC recommends that data is kept for 5 tax years and current to ensure proper records are kept and maintained. HMRC can ask to review this data for audit purposes.