Product name: **IRIS Employee Verification Connector (EVC)**

Information Security Assurance Statement

Document control

Version number:	2.0
Owner:	David Kisiaky
Date of last update:	7th March 2023
Document type:	Information Security Assurance Statement
Approved by:	Fran Williams
Approval date:	3rd April 2024
Data protection impact screening:	
Date of next formal review: 9th December 2024	

Document Control

Version	Date	Amendment	Amended by	Role
1.0	23/02/2023	Initial Document created	Claire Treadwell & Paul Nunn	Product Director
1.1	07/03/2023	Amended to include feedback from review	Claire Treadwell	Product Director
2.0	03/04/2024	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 the Employee Verification Connector 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 IRIS as a thoroughly secure software and service provider.

Description of the data processing carried out by Employee Verification Connector

- IRIS has partnered with Experian to integrate their Work Report™ solution to simplify the process of applying for loans, mortgages, and tenancy agreements. The online service will allow employees to instantly verify their employment status and associated income, removing the manual process of gathering employment and income data
- The employee applies for a mortgage, loan, or other financial application online. The provider asks them to provide evidence of employment and earnings
- During the process they are asked if they wish to verify earnings and employment via Work Report™
- If the employee agrees, they provide basic details like their National Insurance number and the name of the employer, then explicitly confirm that they consent to verify their data using Work Report™
- Work Report™ checks if the employer is an IRIS customer. If the employee is found within the given employer records, the details supplied are then verified in seconds
- The employee income information is securely held by IRIS. The data never leaves IRIS and is not provided to any third parties other than Experian Work Report™.
- The information is only verified after the employee provides their consent online.
- All data is hosted in UK data centres, and processes all data necessary to provide Experian with the following information:

Employee information	
Surname	Employment Leaver Date
Date of Birth	Job Title
National Insurance Number	Annual Income Currency
Payroll ID	Gross Basic Annual Salary
Post Code	Year to Date Gross Income

Employer Name	Year to Date Net Income
Employment Start Date	Pay Date
Contracted Hours	Pay Frequency

- To verify employment & earnings, Work Report™ requires information about employment status, tenure, and gross and net income. Depending on the kind of financial product applied for, the period of earnings to be verified can be between 3 and 12 months.

Statement of Assurance

Employee Verification 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.

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.

Employee Verification Connector Organisational Security

Employee Verification Connector 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 Technical Officer (CTO)

- IRIS Group IT Security Director
- IRIS Group Data Protection Officer
- IRIS Group Senior Compliance Manager
- Other key security leads within the company

The Risk Steering Committee approves IRIS Group-level policies relating to information security and data protection, which IRIS products must comply with. There are Group policies and a detailed Information Security Management System (**ISMS**). The key Group-level documents 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 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 documents 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 Employee Verification Connector

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

- Employee Verification Connector Product Manager – David Kisiaky
- Employee Verification Connector Lead Developer – Paul Nunn
- Employee Verification Connector Development Manager – Chris Ruddy
- Employee Verification Connector Support Services – Thomas Derbyshire

The Employee Verification Connector 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 the Employee Verification Connector.

Measures are “appropriate” if they have been identified through risk assessment.
Date of last Employee Verification Connector risk assessment review:9th December 2023.

The Employee Verification Connector 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 Employee Verification Connector 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 Employee Verification Connector's IT systems and for keeping systems reasonably up to date. Some sections of Employee Verification Connector are managed in Microsoft Azure, compliance documents for Azure can be found here: https://learn.microsoft.com/en-us/azure/compliance/

Employee Verification Connector'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 Employee Verification Connector (including acquired software licences) in a fixed assets system.

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

Employee Verification Connector Human Resource Security

Employee Verification Connector data is encrypted using AES-256 encryption using Microsoft Service-Managed Keys. Development only has access to live data in the event of service failure.

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. This is refreshed annually.

During employment

- Employee Verification Connector 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 training.
- Employee Verification Connector 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 our Learning Management Platform.
- A formal and communicated disciplinary process is implemented to handle Employee Verification Connector employees who have committed a security breach.
- Training is conducted annually and non-completion of training, impacts the company bonus scheme.

Termination and change of employment

- Upon instruction from HR of a person leaving Employee Verification Connector, 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

Employee Verification Connector Access Control

The following levels of user exist within the Employee Verification Product:

- **Development/DevOps Lead** -Limited to owners of the Employee Verification Connector Product on a needs-only basis. No direct access to customer data, but can view analytics and error logs in order to resolve issues and help support the product.

- **Employee** – has no ability to access, change or amend anything in Employee Verification Connector. They only access the service, when submitting a financial application and consenting to verify their data via the Work Report™ solution.

- **Support** – the ability to carry out limited functions to help with customer queries. Support accounts are granted internally by the Employee Verification Connector development team

Review of user access rights – End users do not have access to the Employee Verification Service data. All data is held within the secure IRIS network. End users provide data to the service on submission of the FPS. Users have full control over which companies provide data to the service and can 'Opt-Out' per company. No employee data would be provided to the service in this scenario. Any employees within that company could not take advantage of the IRIS Employee Verification Connector, they would need to manually submit data to the provider. This could slow down the application process.

Use of privileged utility programs – Customers can control which companies provide data to the service.

Employee Consent - Employees provide consent to verify their employment data when conducting the financial application process. Individual consent is not required in the product. No employee data is provided to Experian unless prior consent is gained.

Internal system access control

Employee Verification Connector developers have access to internal development systems and data. Operations staff have access to production databases. All are accessed through Office 365 Active Directory 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 Employee Verification Connector 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 Employee Verification Connector 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, Employee Verification Connector development teams do not have access to live customer data via the main payroll product.

Encryption (cryptology)

Employee Verification Connector enforces the TLS 1.2 protocol on all connections to the application.

Employee Verification Connector physical and environmental security

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

- **Azure UK Data Centres -** used for hosting application services and data storage - https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance
- OAuth 2.0 Client Credentials Managed By Apigee - used for client authentication and routing – https://docs.apigee.com/api-platform/faq/hipaa-configuration-guide-edge-public-cloud

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 Employee Verification Connector engineers.

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 in separate azure subscriptions with their own access restrictions. Access to production infrastructure is restricted through IP restriction lists as well as user permissions. Employee Verification Connector 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 Employee Verification Connector developer machines to protect against malicious software. This is monitored using central processes.
Firewalls are in place and each individual resource has its own network security restrictions. The protection of production environments falls both on Microsoft and IRIS.

Back-ups - Full Backups are taken every 240 minutes i.e. 4 hours, have a retention period of 8 hours and 2 copies are retained. (this is currently under review to increase the retention period).

Event logging - Systems like Datadog are configured for recording user activities, exceptions, faults, and information on security events.
IRIS commits to ensuring any failure of service is resolved within the time scales below:

Priority Level	Description	Response Time	Resolution Time
Critical Issue (P1)	A major system failure removing service, or a major feature of it, to one or more clients. Such a problem will have a serious impact on the operation of the system and may prevent use of the licensed software. For the avoidance of doubt, any failure of the functionality of the Supported Service which affects security, or regulatory compliance is deemed material;	15 minutes	1.5 hours
Priority 2	Major feature unusable. This is a problem that does not prevent the licensed software being operable, but will have a serious impact on the Client's day to day operation of the system. It only affects specific areas where a workaround can be utilized within the system.	15 minutes	2.5 hours
Priority 3	Minor feature unusable. This is a problem that does not prevent the licensed software from being operable, but will have a minor impact on the Client's day to day operation of the system.	15 minutes	18 hours
Priority 4	Is a problem that affects an aesthetic feature of the licensed software and/or an error in the documentation This level of problem will have no adverse impact on the operation of the system, and will be assessed in line with other development commitment	15 minutes	35 hours

Control of operational software – Installation of software on Employee Verification Connector production systems are managed through package managers to minimise the risk of corruption of operational systems.

Management of technical vulnerabilities – Penetration testing for Employee Verification Connector 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 – Employee Verification Connector 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 report logs are stored in the system. They reside within the Employee Verification Connector 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 by 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 in Azure. 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.

Confidentiality or non-disclosure agreements - As required, Employee Verification Connector 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 Employee Verification Connector 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
Employee Data is only verified, via the service, if the employee has provided consent during the financial application process. If no consent is provided, no data is provided. No data is saved during the verification process.

Data is anonymised when the validation request reaches a terminal status (Expired/ Success/ Failed) i.e. as soon as the request fails or data is returned to the consumer service provider. Data is stored in the data warehouse for interrogation purposes only.

When Data is interrogated by the 3rd party, Experian Work Report processes the data (e.g. Standardise/ add metadata). The data is then passed securely via Experian to the Consumer Service Provider. Experian then deletes the data. Data is then deleted in line with the consents and contracts with the Employee (Consumer) and the data may be held in audit logs for up to 6 years per regulatory requirements it is used in a regulated decision.

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 Employee Verification Connector 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 Azure 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). 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 Employee Verification Connector 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 Microsoft) do not have access to Employee Verification Connector information. Supplier service delivery management Monitoring and review of supplier services – Microsoft 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 the appropriate assessment, the Group Compliance Manager is responsible for such decisions.

Summary of sub-processors

The list of third parties and sub-processors involved in EVC
IRIS Group has a section 28 EU-GDPR sub-processor agreement in place with Microsoft Azure which provides UK hosting services for the Employee Verification Connector service.

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.

Experian processes the data via their Work Report™ solution if the employee provides consent during the financial application process. If the employee consents to this, their data will be provided to a third party (of their choosing).

Information security incident management

In all instances, any Employee Verification Connector 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 IRIS Development team and Dev Ops maintain a list of IRIS Employment Verification Connector third-party components, and any dependencies risk are identified.

Compliance

Compliance with legal and contractual requirements

Privacy and protection of personally identifiable information – Employee Verification Connector 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/** **https://www.iris.co.uk/products/iris-employee-verification/**
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 Employee Verification Connector	**Name: David Kisiaky** **Email: David.kisiaky**@iris.co.uk

Types of Data

Category	Details
Personal Data processed	**Customer Employees** Contact Details Home Postcode Personal Email Phone Numbers Work Email Address **Employee Information** Contracted Hours Hours of Work Job Title Role Salary Wage Individual Pay Period Details Start Date **Government Identifiers** National Insurance Number (NINO)

	Personal Identification Date of Birth Surname Unique Personal Identifier **Contact Information** Mobile Number
Purpose for which personal Data is processed under the product/ service	Employee Verification Connector provides the ability for employees to verify Income and Employment during the financial application process. Earnings are verified in real time, simplifying the process.

Location of personal data

Category	Details
Hosted Environments	Microsoft Azure
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. If a company is 'opted out' of the service, all employee data is removed from the Employee Verification Connector. Company information is retained, to identify companies that have opted out of the service.

Data subject rights

Category	Details
Data Deletion	Customers have control of their employee data. If a company is 'opted out' of the service, all employee data is removed from the Employee Verification Connector.