Information Security Assurance Statement

IRIS Employee Verification Connector (EVC)

INFORMATION SECURITY ASSURANCE STATEMENT OF IRIS Employee Verification Connector (EVC)

Document Control	
Version number	4.0
Owner	Vimal Patel – Product Owner, EVC
Date of last update	18/11/2024
Document type	Information Security Assurance Statement
Replaces	Version 3.0
Approved by	David Kisiaky, Senior Product Manager
Approval date	11th December 2024
Data protection impact screening	N/A
Date of next formal review	9/12/2025

Contents

0 OBJECTIVE OF THIS DOCUMENT

The purpose of this Information Assurance Security Statement 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.

0.1 Description of the data processing carried out by Employee Verification Connector

IRIS has partnered with Experian and Equifax 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 Experian or Equifax.
- 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 Experian or Equifax.
- Experian or Equifax 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 and Equifax.
- 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 and Equifax 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
Employment Type	Pay Frequency
Most Recent Hire Date	Base Pay Rate Description
Base Pay Rate	

- To verify employment & earnings, Experian and Equifax 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.

1 STATEMENT OF ASSURANCE

IRIS will ensure that:

- 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.

- We will meet our regulatory and legislative requirements.
- We will produce, maintain and test Business Continuity plans.
- We will provide information security training to all our staff.
- We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
- 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.

2 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.

3 EMPLOYEE VERIFICATION CONNECTOR ORGANISATIONAL SECURITY

Data protection and information security at IRIS Software Group is controlled by the IRIS Information Security and Governance Forum. This forum 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 Senior Compliance Manager
- Other key security leads within the company

The Information Security and Governance Forum 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:

1. 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.

2. 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.

3. 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.

3.1 Organisational security at IRIS Group level

With Employee Verification Connector, the product manager/director is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering Payroll Solutions to ensure Employee Verification Connector 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 Employee Verification Connector, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

Employee Name	Department	Designation
Fran Williams	Product	Senior Product Director – Payroll & Managed Services
David Kisiaky	Product	Senior Product Manager
Paul Nunn	Engineering	Lead Developer
Chris Ruddy	HCM Engineering	Development Manager

Thomas Derbyshire	Customer Service/Support	Senior Manager, Customer Services
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group

The Employee Verification Connector 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 Employee Verification Connector.

Measures are "appropriate" if they have been identified through risk assessment. ISO27001 certification is audited annually by an external assessor. Internal compliance with Group ISMS is also annually reviewed by the Group Compliance team. Annual external 3rd Party Penetration testing is carried out for cloud services with weekly vulnerability scanning. Date of last external Employee Verification Connector penetration test: 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 on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner's Office.

Group IT/Dev Ops teams 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 GDPR guidance/best practice for personal data.

3.2 IRIS Support staff could have access to your data to fulfil the support aspect of the Employee Verification Connector Solution.

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.

During employment

The responsibility for ensuring that processes and procedures are both established and maintained are held with IRIS / Employee Verification Connector Managers. Employees, third parties and contractors are mandated to read, and sign a document to confirm understanding of their responsibilities. In the event of the use of an external party, controls are put in place to restrict the level of data they have access to in line with group policy and this activity is supervised and relevant risk assessments have taken place.

In addition to local procedure, IRIS Group also require the completion of corporate policy training and the subsequent testing of this knowledge through the company compliance portal. This testing is repeated as frequently as is reasonable for all employees, third parties and contractors.

In the unlikely event of a security breach, the governing policy or procedure would be re-reviewed and amended to ensure stricter compliance moving forwards. IRIS places the onus on employees for their adherence to security protocols and a disciplinary procedure is enforced for non-compliance. If no improvement is found to employee performance under the afore mentioned disciplinary, employment is terminated as set out in the terms of the procedure.

Termination and change of employment

In the event of an employee terminating their employment contract with IRIS, the following departments are notified and the following actions take place:

Department	**Action**
Employee Manager	To notify Group HR and Group IT, revoke log in credentials from internal systems required for role.
Group HR	To restrict access to internal systems, HR portal and notify Payroll.
Group IT	To close off network access, organise recovery of assets, revoke other access (Office 365 account, Cloud accounts, VPN access).

Upon instruction from HR of a person leaving IRIS , that person's access to confidential areas shall be restricted immediately, culminating in:

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

All employees have been contracted to a non-disclosure clause in their contracts that still remains applicable after termination.

4 ACCESS CONTROL

The purpose of the Access Control Policy is to ensure that information systems resources and electronic information assets owned or managed by IRIS are available to all authorised personnel. The Policy also deals with the prevention of unauthorised access through managed controls to create a secure computing environment.

Access controls to network, operating system and applications shall be set at an appropriate level on need to use basis, which minimizes information security risks yet allows the business activities to be carried without undue hindrance. This is managed as per the Organisational Security section in conjunction with the IT Manager and Information Asset Owner and in accordance with the IRIS Group Access Control Policy.

Access is granted on the least privileged rule basis consistent with an individual's job/role responsibilities.

The following levels of user exist within the Employee Verification Connector 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 Experian or Equifax.

- 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 Connector 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 and Equifax unless prior consent is gained.

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

Access to cloud-based administration consoles for privileged IRIS' IT Department and IRIS users is mandated with password authentication.

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

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

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

4.1 Password and Authentication Policy

This policy describes the authentication requirements for accessing internal computers and networks and includes those working in-house as well as those connecting remotely. Every person, organisation or device connecting to internal IT resources and networks must be authenticated as a valid user before gaining access to IRIS's computer systems, networks and information resources.

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.

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

5 PHYSICAL AND ENVIRONMENTAL SECURITY

Employee Verification Connector follows guidance set out in our IRIS group Physical Access policy.

- Physical entry controls - Entry to the site is restricted to key fob or key pad entry. Only IRIS employees have access to the area payroll is completed in.

- Securing offices, rooms and facilities – Physical security is employed at greater levels where higher risk or classification of a more sensitive nature of data is identified.

- Protecting against external and environmental threats - IRIS has a robust business continuity plan, however we also place a great importance on our first defence. We are protected by a failover line in the event we lose connectivity due to environmental damage, we also have the ability to move the entire site remote or transfer ownership to a satellite office at a moment's notice.

  IRIS Group have invested heavily into our cyber defences, these are controlled by IRIS Group IT. We have also moved customer data into an ISO-secure cloud-based environment which adds additional layers of security to your information.

  IRIS became a paperless office in January 2020.

  - Working in Secure Areas – In the event a third party needs access to a secure area within the physical site, they are escorted at all times by facilities. Additional measures are covered under the topic "Human Resources Security".

  - Delivery and loading areas – Deliveries are taken at reception with no access granted to unauthorised people.

5.1 IRIS Equipment

For IRIS teams / employees:

Equipment	Description
Equipment siting and protection	Access to critical computing resources or infrastructure is physically restricted to authorised personnel with access controlled by keys, swipe cards or a key pad lock.
Protection against power failures and disruptions	The physical site has taken adequate measures to prevent disruption. Installation of a failover line in the event of loss of connectivity.
Equipment maintenance	Regular maintenance is carried out on equipment as per the recommendations of the manufacturer. A maintenance log is held on site and maintained by designated Facilities personnel.
Removal of assets	Any physical assets to be moved from one place to another place within the office and outside the office must require prior approval from Senior Management. A register of all assets taken off site is kept and maintained by the Site Leader and shared with Group IT.
Security of equipment and assets off-premises	Guidance is outlined in mandatory policy document.
Group IT: Working from home manual	With considerations on Information Security, use of the Group's VPN. Two Factor Authentication is implemented for access to all secure areas of the network.
Unattended user-equipment	IRIS enforces a clear desk policy. Staff laptops & IT assets are sited in a secure office area, information displayed on screen may be confidential. All computers revert to screen saver mode at timely intervals and staff are mandated to logoff from sessions and ensure any paper is securely disposed of.
Clear desk and screen policy	IRIS went paperless in January 2020. In line with our Clear Desk Policy, employees and contractors are made aware of their responsibilities to ensure that data is protected at all times, we also have locked shredding cabinets for the secure disposal of notepads and post-it notes, if required. All employees and contractors are expected to lock their computer screens, as a redundancy procedure, IRIS Group IT set screens to auto lock after 5 minutes and will require a password from the user to unlock.

5.2 Media handling

Media Handling	Description
Management of removable media	IRIS sets out the acceptable usage of removable media in Information security and acceptable use summary Policy. It is not permitted to create a copy of protected data on unauthorised devices.
Disposal of media	IRIS sets out responsible use of data in our IRIS Data Protection Policy, including secure disposal and audit of media.

6 OPERATIONS SECURITY

Operations Security	Description
Documented operating procedures	Backups, 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.
Capacity management	Resources are monitored, tuned and protections made of future capacity requirements to ensure systems continue to perform at optimum levels.
Separation of development, testing and operational environments	Development and production environments are separated and managed through documented and automated deployment pipelines. Access to infrastructure is restricted through IP restriction lists. Developers do not have access to production environments, unless authorised for a specific purpose i.e. Product Deployment / Support.
Protection from malware	IRIS uses Microsoft to protect against malicious software and this is centrally monitored. All client machines are auto updated on connection to the network or via internet. 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).

Back-ups	The backup of all IRIS processing server systems falls under the remit of the Group IT Director. All data is backed up at least nightly and transmitted to a secure UK-based cloud back-up location. Restoration tests are made and documented on a regular basis, not less than annually.
Event logging	Both environment and software products have independent audit logs of activities carried out within each. Environment audit is maintained and monitored at Group IT and Infrastructure level and Product is reviewed by Employee Verification Connector Management.
Protection of log information	Log information and Audit trails are managed at Group IT level in line with outlined roles and responsibilities to prevent tampering of data. On a software product level, these controls have been locked at development stage, no user has the ability to manipulate information held within.
Clock synchronisation	IRIS Group IT controls clock settings, ensuring that synchronisation is enabled to a real time clock set at local standard time.
Control of operational software	Installation of software on desktop payroll production systems is managed through package managers to minimise the risk of corruption of operational systems.
Management of technical vulnerabilities	Penetration testing for integrated web-applications 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.
Restrictions on software installations	Group IT regularly review acceptable use and monitor or restrict installations that have not yet been deemed safe. Requests to install new software must be authorised by Group IT if not already placed on a safe list.

7 COMMUNICATIONS SECURITY

Communications Security	Description
Network security	All integrated web-applications are maintained and tested to a high standard of security. The integrity of client data is ensured through a quality hosted environment that holds more than appropriate accreditation outlined within this document
Security of network services	We employ the use of Cloud-Based Technology that houses personal data in UK Data Centres hosted by Azure, that uses world class security protocols to ensure security compliance (accreditation details in 'Organisational Security' section).
Segregation of networks	The Employee Verification Connector (EVC) and its data are physically and logically separated in the hosted environment. EVC is independent of all other business IRIS transacts, and controls are in place to ensure that only authorised persons have access.
Electronic messaging	IRIS employees are subject to audited training on 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, IRIS 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.

7.1 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 and Equifax processes the data (e.g. Standardise/ add metadata). The data is then passed securely via Experian and Equifax to the Consumer Service Provider. Experian and Equifax 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.

Dependent on the service, the use of email is minimised for queries and all personal identifiable data is removed from the contents of email transactions in direct reply to a query. All employees receive audited training against this requirement.

Information transfer policies and procedures – Employee Verification Connector clearly outlines the procedures within the IRIS Data Protection Policy held at local level for the teams. It is meticulous in the process that must be followed to prevent risk occurring when transferring information between Employee Verification Connector and Client.

8 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Securing application services on public networks - Where possible, integrated web-applications enforce the use of TLS 1.2 as a communication protocol.

9 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Security in Development and Support Processes	Description
System change control procedures	Major system changes are reviewed by the Architectural Review Board (ARB) mentioned previously in this document.
Technical review of applications after operating platform changes	IRIS test all product updates against a range of supported environments and software. Regression testing is completed to review the overall product impact of any system changes.
Restrictions on changes to software packages	Changes to software development inhouse is 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 suites 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.

9.1 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.

10 SUPPLIER RELATIONSHIPS

10.1 Supplier service delivery management

Supplier service delivery management	Description
Monitoring and review of supplier services	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.
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 security and data protection teams ensure potential suppliers are subject to due diligence in line with data protection laws and security standards.

List of third parties and sub-processors involved in Employee Verification Connector processing customer data 23rd November 2023.

10.2 IRIS Group Entities

IRIS Group Entities	Description
IRIS KPO India	Our Support Functions processes may be processed by our India Support function. IRIS KPO use our internal secure IRIS VPN connection. A detailed risk assessment is carried out annually to ensure continued process review of security requirements. A full Customer Assurance document is also available on request.

10.3 External Suppliers which are Data Processors

External Data Processors	Data Location	Description
Experian	UK	Authorised external data partner for the purpose of online verification of employment and income, for employees applying for financial products such as mortgages, loans and tenancy agreements.
Equifax	UK	Authorised external data partner for the purpose of online verification of employment and income, for employees applying for financial products such as mortgages, loans and tenancy agreements.

11 INFORMATION SECURITY INCIDENT MANAGEMENT

Management of information security incidents and improvements

In all instances, any desktop or cloud 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 software manager and / or product manager and corrective actions are logged and tracked to execution.

Information security incidents must follow this process, but in addition will be triggered 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

11.1 Information security continuity

Information Security Continuity	Description
Planning information security continuity	During adverse situations, Employee Verification Connector have a number of secure ways to ensure the continuity work carried out.
Implementing information security	Employee Verification Connector continues its use of the Local Data Protection Policy in the event of a BCP scenario. We also utilise the Working From Home Procedures policy and Acceptable Usage policy.
Verify, review and evaluate information security continuity	Employee Verification Connector / IRIS review all policies as often as required but no less than once per year.

11.2 Redundancies

Redundancies	Description
Availability of information processing facilities	All systems and data have been loaded into secure cloud based environments (Azure) to ensure continuity.

12 COMPLIANCE

12.1 Compliance with legal and contractual requirements

Legal and Contractual Requirements	Description
Identification of legislation and contractual requirements applicable to Employee Verification Connector	Within the scope of the role performed, processors, managers and software provisions will defer to HMRC Regulations for PAYE, attachment of earnings documentations provided by courts and terms and conditions with client. IRIS makes every effort reasonable to inform its clients of any major changes to legislation within these areas.
Protection of records	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. For audit trail purposes, only company information is retained to keep a record of the opt out.
Privacy and protection of personally identifiable information	Covered within Employee Verification Connector privacy policy both at local and IRIS group level.
Regulation of Cryptographic Controls	Employee Verification Connector has been developed using market leading encryption methods. These fall well inside the scope of existing legislation and additional security measures such as MFA have been built in to the existing framework. Personal data is stored in MS SQL with data encrypted at rest using 256-bit AES encryption.

12.2 Information security reviews

Information Security Reviews	Description
Compliance with security policies and standards	Local policies are reviewed as regularly as required but no less than annually. This is to ensure that all relevant standards are being met and have been implemented in full. Group level compliance reviewed annually.

12.3 Data Protection – quick reference

Contact	Details
IRIS Group Data Protection Officer	Vincenzo Ardillio – dataprotection@iris.co.uk
Data protection owner for Employee Verification Connector	David Kisiaky – david.kisiaky@iris.co.uk

Categories of personal data processed as part of the Employee Verification Connector provision:

- Employees – identifiable through payroll processing
- Contractors – identifiable through payroll processing (CIS)

12.4 Location of personal data processing

All personal data is held within the Employee Verification Connector database. In all instances, information is held on secured and encrypted network drives held in the UK and only accessible by those authorised to access it.

On occasion, IRIS may use support engineers and third parties located in the USA and 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.

12.5 Employee Verification Connector Retention of data

- Rationale for retention: The total period covered for online verification and employment income is up to 12 months
- Any employee records that have not been updated for at least 15 months, or have a leave date of more than 15 months ago, is automatically deleted from the Employee Verification Connector platform

12.6 Data subject rights

- As part of the GDPR options the employees can initiate a subject access request to access the data held on the Employee Verification Connector.
- An employee can also request a 'Right to Delete' and 'The Right to Restrict'. The 'Right to Delete' will delete all the existing data on the Employee Verification Connector and prevent any future data transmission
- The 'Right to Restrict' does not delete historic data but prevents future data transmission
- Both of these options prevent any data being sent to the thrid party.

13 AVAILABLE APPENDICES

Details	
Azure	https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance/
IRIS Desktop Payroll – Customer Information security assurance statements	Available on Request
Staffology Due Diligence	Available on Request
Staffology Payroll Group Data Protection Statement	Available on Request
IRIS Working from Home Policy	Available on Request
IRIS Group Acceptable Use Policy	Available on Request
IRIS Personal Data Incident Reporting and Investigation Procedure	Available on Request

Heathrow Approach
470 London Road,
Slough,
SL3 8QY
0344 815 5555
hcmproduct@iris.co.uk