Information Security Assurance Statement

IRIS Payroll Services
on Employer Portal

INFORMATION SECURITY ASSURANCE STATEMENT OF IRIS PAYROLL SERVICES ON EMPLOYER PORTAL

Document Control	
Version number	V1.3
Owner	Brona Grogan (Senior Director, Managed Payroll & Offshore Services)
Date of last update	31/01/2025
Document type	Assurance Statement
Replaces	V1.2
Approved by	Fran Williams
Approval date	31/01/2025
Data protection impact screening	N/A
Date of next formal review	01/02/2026

CONTENTS

1.0 OBJECTIVE OF THIS DOCUMENT

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

1.1 Description of the data processing carried out by IRIS Payroll Services

IRIS Payroll Services Is a payroll outsourcing department under the IRIS family. We offer end-to-end payroll processing functions using the latest in secure cloud hosted technology. The objective of the service is to reduce cost and increase profit of our clients. IRIS Payroll Services provides various types of payroll related services such as employee record maintenance, payroll calculations, HMRC reporting, accounts journal output, BACS processing to employees and 3rd parties, payslip distribution and payroll queries. We have robust data security measures in place to ensure that our customer's data is protected in every way.

2.0 STATEMENT OF ASSURANCE

IRIS Payroll Services will ensure that:

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

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

3.0 IRIS PAYROLL SERVICES ORGANISATIONAL SECURITY

IRIS Payroll Services is committed to fulfilling its obligations under the Data Protection Act 2018, General Data Protection and Regulation (GDPR – EU law) and any associated privacy legislation that affects how IRIS Fully Managed Service uses or handles personal data. IRIS Payroll Services has produced the Statement of Data Protection Policy to give this assurance to our customers and staff. IRIS Payroll Services is BACS accredited certified by BAB.

In addition to the IRIS Payroll Services Statement of Data Protection Policy, this document sets out how responsibility for data protection and information security is designated. It includes high-level descriptions of the procedures in place that must be followed to ensure personal data is handled in a responsible, accountable and secure manner.

IRIS Payroll Services will use personal data legally and securely regardless of the method by which it is collected, recorded and used and whether we hold it within our products, on a Group or third-party network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

IRIS Payroll Services regards the proper management of personal data as crucial to the success of our business. Observing good data protection practice plays a huge role in maintaining customer confidence. We ensure that IRIS Payroll Services respects privacy and treats personal data lawfully and correctly.

Supporting accreditations held by IRIS Payroll Services are:

- ISO9001
- ISO27001
- CIPP Payroll Assurance Scheme (PAS)

We employ the use of cloud-based technology that houses personal data in UK Data Centres, that uses world class security protocols to ensure security compliance. The data that is stored by Rackspace and Azure is protected or regulated under:

- ISO/IEC 27001
- ISO 9001
- ISO 14001
- OHSAS 18001
- SOC (SSAE 18)
- SOC 2
- SOC 3
- PCI DSS Level 1
- FedRAMP JAB-ATO
- NIST 800-53
- FISMA
- NIST 800-53 (“DFARS”)
- CMMC
- CJIS
- ITAR
- FIPS 140-2

- HITRUST
- IRAP

As an additional layer of complexity, only employees granted access to view this data can only do so through the use of an internal group VPN.

IRIS uses in-house built payroll software (Employer Portal via Staffology Payroll) to deliver these services. Staffology Payroll will use personal data legally and securely regardless of the method by which it is collected, recorded and used and whether we hold it within our products, on a Group or thirdparty network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

Supporting accreditations held by Staffology Payroll are:

- HMRC Approved Payroll Software
- ISO27001
- Cyber Essentials

IRIS Payroll Services and Employer Portal is part of the IRIS Software Group.

3.1 Organisational security at IRIS Group level

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
- 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.

3.2 Organisational security for IRIS Payroll Services

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

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

Employee Name	Department	Designation
Steve Hawley	Senior Management	Senior Director, Managed Payroll & Offshore Services
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group
Michelle Webb	Payroll Managed Service	Senior Manager, Client Payroll Services
Lynn Gaunt	Payroll Managed Service	Senior Manager, Client Payroll Services
Thomas Derbyshire	Customer Service/Support	Senior Manager, Customer Services
Yellie P Williams	Professional Services	Director, Professional Services
Tarka Duhalde	Finance and Accounts	VP, Financial Controller
Rob Brough	Sales Order Processing	Director, Revenue Operations
Justin Alford	Credit Control	Senior Manager, Credit & Collections
Fran Williams	Product	Senior Product Director – Payroll & Managed Services

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

Measures are "appropriate" if they have been identified through risk assessment. Date of last IRIS Payroll Services risk assessment review: October 2023.

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

The IRIS Group Data Protection officer is responsible for providing advice and guidance to the IRIS Payroll Services 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 are responsible for the operation and integrity of IRIS Payroll Services's IT systems and for keeping systems reasonably up to date.

IRIS Payroll Services's Development systems are managed by an internal development team.

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

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

IRIS Payroll Services staff will have access to your data in order to fulfil the Payroll Service:

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 Payroll Services 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 MetaCompliance 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 Payroll Services places the onus on the employee 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
Managed Services Management	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 Payroll Services, 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.

4.0 IRIS PAYROLL SERVICES 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. For IRIS Payroll Services user login, system enforced password complexity rules ensure that strong passwords are used and Users are responsible for keeping them confidential. Systems and information should be secured whenever left unattended.

All 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.

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

5.0 IRIS PAYROLL SERVICES PHYSICAL AND ENVIRONMENTAL SECURITY

IRIS Payroll Services follows guidance set out in our 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 Payroll Services 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 Payroll Services 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 Equipment

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 Payroll Services 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 Payroll Services 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 Payroll Services 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 Payroll Services sets out responsible use of data in our IRIS Data Protection Policy, including secure disposal and audit of media.

6.0 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. Desktop payroll developers do not have access to production environments, unless authorised for a specific purpose i.e. Product Support.
Protection from malware	IRIS Payroll Services utilises Kaspersky, 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 processing server systems falls under the remit of the Group IT Director. All data is backed up 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 IRIS Payroll Services 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. Ona 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.

7.0 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 Rackspace, that uses world class security protocols to ensure security compliance (accreditation details in 'Organisational Security' section). As an additional layer of complexity, only employees granted access to view this data can only do so through the use of an internal group VPN. These controls are reviewed annually.
Segregation of networks	The network client data and software used to process this data are held in separate networks to mitigate risk. These networks are independent of all other business IRIS transacts and controls are in place to ensure that only authorised persons have access to these drives.
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 Payroll Services 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

Dependent on the service provided, IRIS Payroll Services utilises a number of proprietary secure document sharing portals (IRIS OpenSpace, AMS, IRIS Staffology Employer Portal) to transmit client personal data between client and IRIS Payroll Services, we also send password protected documents issued by email direct from the software product. 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 – IRIS Payroll Services 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 IRIS Payroll Services and Client.

8.0 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.

9.0 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 suits managed by the internal quality engineers on the desktop 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.

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.

10.0 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 compliance team are responsible for choosing an appropriate supplier based on ISO 27001 standards. After appropriate assessment, the Group Compliance Manager is responsible for such decisions.

List of third parties and sub-processors involved in IRIS Payroll Services processing customer data 11th March 2021.

10.2 IRIS Group Entities

IRIS Group Entities	Description
IRIS KPO India	IRIS reserve the right to use all of our processing centres including our Indian off-shore function. IRIS KPO use our internal secure IRIS VPN connection alongside the security architecture Rackspace and Azure provides to process data within UK Servers. 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. IRIS KPO India also hold ISO27701 certification.
IRIS OpenSpace	Hosted environment to act as a secure document transfer system. Access is restricted and appropriate ISO controls exist. Data contained in the system is held within UK Data Warehouses and clients have full control over deletion of data.

10.3 External Suppliers which are Data Processors

External Data Processors	Description
Rackspace	Payroll Software and client data is held in a Rackspace hosted environment. All security protocols and accreditations are mentioned previously within this document.

Microsoft Azure Hosting (UK)	Payroll Software and client data is held in a Microsoft Azure hosted environment. All security protocols and accreditations are mentioned previously within this document.
Microsoft Azure Dev Ops (UK)	Staffology Payrolls development lifecyle is managed on Microsoft Azure Dev Ops, with 4th Line Support Tickets managed via the support & development functions on the platform.
Fresh Desk (EEA)	Our support function uses Fresh Desk to provide customer ticketing, communication, live chat and query resolution management.
Sales Cloud via Salesforce (UK)	Our support function uses Sales Cloud to provide customer ticketing, communication, live chat and query resolution management.
Send Grid (US)	SendGrid is a US provider of cloud-based transactional and marketing email delivery, management and analytics services.
OKTA (UK)	OKTA is Staffology Payroll & IRIS Software identity management provider and helps companies manage and secure user authentication into applications.

11.0 INFORMATION SECURITY INCIDENT MANAGEMENT

11.1 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.

12.0 BUSINESS CONTINUITY – INFORMATION SECURITY ASPECTS

12.1 Information security continuity

Information Security Continuity	Description
Planning information security continuity	During adverse situations, IRIS Payroll Services have a number of secure ways to ensure the continuity work carried out. All processors and managers are laptop users with access to the IRIS secure VPN. The installation of 3rd party software is strictly controlled with appropriate auditing in place detailed throughout this document.
Implementing information security	IRIS Payroll Services 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	IRIS Payroll Services review all policies as often as required but no less than once per year.

12.2 Redundancies

Redundancies	Description
Availability of information processing facilities	All systems and data have been loaded into secure cloud based desktop environments (Rackspace/Azure) to ensure continuity. We are able to move instances with ease using backups of the environment and a final redundancy available on the internal network accessible only through the IRIS VPN.

13.0 COMPLIANCE

13.1 Compliance with legal and contractual requirements

Legal and Contractual Requirements	Description
Identification of legislation and contractual requirements applicable to IRIS Payroll Services	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 Payroll Services makes every effort reasonable to inform its clients of any major changes to legislation within these areas.
Protection of records	Covered in the Business Continuity Plan Document
Privacy and protection of personally identifiable information	Covered within IRIS Payroll Services's Data Protection Policy both at local and group level.
Regulation of Cryptographic Controls	IRIS Payroll Services utilises an online Payslip Portal which has been developed using market leading encryption methods. These fall well inside the scope of existing legislation and additional security measures such as 2FA have been built in to the existing framework.

13.2 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.

13.3 Data Protection – quick reference

Contact	Details
IRIS Group Data Protection Officer	Vincenzo Ardillio – dataprotection@iris.co.uk
Data protection owner for IRIS Payroll Services (South)	Michelle Webb – michelle.webb@iris.co.uk
Data protection owner for IRIS Payroll Services (North)	Lynn Gaunt – Lynn.Gaunt@iris.co.uk
Data Protection Owner for Employer Portal via Staffology Payroll	Alex Hay – Alex.Hay@iris.co.uk

Categories of personal data processed as part of the IRIS Payroll Services provision:

- **Trade Union Membership** – identifiable through deductions made to employees
- **Information relating to criminal convictions and offences** – identifiable though court order fines processed through payroll

Categories of data subjects under the IRIS Payroll Services provision:

- **Employees** – identifiable through payroll processing
- **Trainees** – identifiable through payroll processing (apprenticeships)
- **Next of Kin** – identifiable on rare occasion where beneficiary payment needs to be made through payroll

13.4 Location of personal data processing

All personal data is held within payroll software databases and on electronic documents from client communicating this data to IRIS Payroll Services. In all instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it.

On occasion, IRIS Payroll Services may use IRIS employees in India as processors of this data. All relevant security requirements have been addressed and further information including their version of the Customer Assurance document is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

13.5 Retention of data

Data will be retained for a period of no more than 7 years for the purpose of assisting the customer in any HMRC audit that may take place. Data will then be permanently deleted. The exception to this would be in the event we are asked to investigate a case in relation to existing Anti-Money Laundering legislation, in this case, data can be retained for a period of up to 10 years.

IRIS will after the termination of the Services, will retain data for a period of 6 years before we delete all copies of the Personal Data in its possession or control, and procure that any relevant Sub-Processor does the same, unless the applicable laws of the United Kingdom or European Union require IRIS or that Sub-Processor to retain a copy of it.

Where we are under a direct legal obligation to retain records we will take steps to anonymise data, where possible.

IRIS EVC Connector used with Staffology Payroll retains data as follows: (See EVC details here):

- For the contracted or agreed duration of processing using IRIS software, employee pay details are uploaded per period to IRIS's MS Azure EVC connector environment sufficient to support income verification for between 3 to 12 months prior employment. Data is auto-deleted after a rolling 15 months
- If an Employee leaves their employer, their data will be auto-deleted after 15 months
- Each Employer's opt-in/out status is retained on IRIS's EVC connector so that Employees of participating employers can be processed accordingly or informed to verify their income by other means
- Data is permanently erased from IRIS's EVC connector when Employees or Employers opt out the service from Staffology Payroll

13.6 Data subject rights

The Client will remain the data controller and will have the responsibility for responding to rights requests from their employees or any other data subjects. Clients requiring assistance with a Data Subject Rights request can do so by email to the IRIS Payroll Services inbox. A response will be received within 2 working days. Where subject matter is comprehensive or more time is required to deliver the requested data, a client will be updated with realistic timescales to satisfy their request.

14.0 AVAILABLE APPENDICES

Details	
Rackspace	https://www.rackspace.com/en-gb/compliance/iso
IRIS KPO Assurance Statement	Available on Request
IRIS KPO Risk Assessment	Available on Request
IRIS Payroll Services 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
Azure	https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance
Staffology Due Dilligence	Available on Request
Staffology Payroll Group Data Protection Statement	Available on Request

IRIS
Heathrow Approach
470 London Road
Slough
Berkshire
SL3 8QY
0344 225 1525