



IRIS | My ePay Window

Information Security Assurance Statement

My ePay Window

INFORMATION SECURITY ASSURANCE STATEMENT OF MY EPAY WINDOW

Document Control	
Version number	1.1
Owner	Nigel Francis – Product Director, Desktop Bureau
Date of last update	04/04/2024
Document type	Assurance Statement
Replaces	N/A
Approved by	Fran Williams – Senior Product Director
Approval date	TBC
Data protection impact screening	N/A
Date of next formal review	31/12/2025

0	Contents	
1	OBJECTIVE OF THIS DOCUMENT	5
1.1	Description of the data processing carried out by My ePay Window	5
1.2	Data subject rights	6
1.3	Encryption: Data in transit and rest	6
1.4	Cookies	6
1.5	Availability	6
2	STATEMENT OF ASSURANCE	7
3	MY EPAY WINDOW ORGANISATIONAL SECURITY	8
3.1	Organisational security at IRIS Group level	9
3.2	Organisational security for My ePay Window	10
3.3	IRIS Support staff could have access to your data to fulfil the support aspect of the My ePay Window Solution.	11
4	ACCESS CONTROL	13
4.1	Password and Authentication Policy	13
5	PHYSICAL AND ENVIRONMENTAL SECURITY	15
5.1	Rackspace Managed Hosting	16
5.2	IRIS Equipment	18
5.3	Media handling	19
6	OPERATIONS SECURITY	19
7	COMMUNICATIONS SECURITY	21
7.1	How we transmit confidential information to customers	21
8	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	22
9	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	22
9.1	Test data	22
10	PROCESSING LOCATIONS AND INTERNATIONAL DATA TRANSFERS	23
11	SUPPLIER RELATIONSHIPS	23
11.1	Supplier service delivery management	23
11.2	IRIS Group Entities	24
11.3	External Suppliers which are Data Processors	24
12	INFORMATION SECURITY INCIDENT MANAGEMENT	25
12.1	Information security continuity	25
12.2	Redundancies	26
13	COMPLIANCE	27
13.1	Compliance with legal and contractual requirements	27
13.2	Information security reviews	27
13.3	Data Protection – quick reference	28
13.4	Location of personal data processing	28
13.5	MY EPAY WINDOW Retention of data	29

13.6 Data subject rights.....29

14 AVAILABLE APPENDICES 30

1 OBJECTIVE OF THIS DOCUMENT

The purpose of this information security assurance statement is to provide customers of the My ePay Window payslip portal by IRIS with transparency as to the security and personal data compliance of this product and associated products 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 My ePay Window as a thoroughly secure software and service. Controls are described that are in place both within IRIS and where applicable, specifically with reference to the My ePay Window service.

1.1 Description of the data processing carried out by My ePay Window

IRIS's My ePay Window service provides a cloud self-service payslip and payroll collaboration facility that enables Employees and Employers to access their payslips, P60s, P11Ds, P45s, CIS statements directly from a secure web site, thereby reducing costs and offering the highest level of service 24 hours a day, 365 days a year.

- Various IRIS Payroll Software offerings are able to publish pay data to My ePay Window. Please refer to each payroll software product documentation for its compatibility with Myspaywindow and for the pay documents that can be processed and distributed via My ePay Window.
- The IRIS desktop payroll processing software that interoperates with My ePay Window can be hosted on the client's own IT infrastructure in which case client payroll data is held and processed by the client, or the software can be hosted on the IRIS hosting service or a third-party hosting service in which case software, client data and processing is at the specified hosting service.
- Staffology Payroll by IRIS is a cloud payroll solution that is hosted on MS Azure is able to publish pay documents to My ePay Window.
- The IRIS desktop payroll software whether hosted locally by the client or at a hosting service, and Staffology Payroll, transmit data securely to the IRIS My ePay Window self-service cloud portal service for information distribution to users/employees.

Once users have been invited and have created a My ePay Window account, payroll department users, Employer users and Employees can self-administer password and username resets. All users can also opt to enable two-factor (2FA) authentication for their accounts if this is not enforced for all users by default by their Employer or Service Provider. They can also opt to enable outbound email notifications in addition to the automatic 'in portal' notifications.

The My ePay Window service and site allows a Payroll department user and Employer user to securely exchange various payroll documentation and to notify one another when this happens:

- If email notifications are enabled, email notifications are sent as follows:
- Employees: A daily summary email for all notifications received in the preceding 1hr
- Payroll Department and Employers users: An Hourly summary email for all notifications received in the preceding 1hr
- Payroll department users: Instant email notification for Employer document uploads and Employer consent withdrawal
- The Service Provider is able to publish and notify when payroll Software generated reports (including P60s, P11ds, P45s, CIS statements and Auto-Enrolment letters) are sent directly to the Employer user's My ePay Window account and also to their Employees.

- Employers are able to upload various documents and notify the Service Provider when such documents are waiting for their attention.

1.2 Data subject rights

My ePay Window processes personal data lawfully and for the purposes of payroll processing and to allow our clients to provide various payroll statements relating to their employees according to UK employment legislation. All users of IRIS My ePay Window, must consent to their information being available on the service as part of the site registration process and with sight of the My ePay Window service privacy policy. Any users declining consent are referred to their 'Employer' (for discussion) and their account registration is stopped.

1.3 Encryption: Data in transit and rest

Data is encrypted in transit via SSL (AES256) & TLS 1.2 protocol between the IRIS Payroll desktop software applications and the My ePay Window self-service portal and Data and documents on the My ePay Window service are encrypted at rest to AES256.

1.4 Cookies

The My ePay Window Service uses cookies. A cookie is a small piece of data that the Website transfers to the user's hard drive. It contains simple information about the user's identity but no personal information from which a living individual can be identified. Cookies are used for the following purposes:

- Session Cookies: these are necessary to enable secure access. You may disable these in your browser settings, but this will mean the website will not function correctly.
- Analytics Cookies: We use Gainsight analytics cookies to collect information about how My ePay Window is used (these do not directly identify anyone or any company) and to help us improve the product. You may disable these in your browser settings.

1.5 Availability

- Service window - IRIS anticipates the period of greatest use of My ePay Window is between 21st of the month and 5th of the following month. IRIS will ensure that routine maintenance and, wherever practicable, upgrades avoid this critical period so that such work is undertaken between 6th and 20th of any month and that, routine maintenance or an upgrade is planned between 21st and 5th of the month. Customers will be informed at least 5 days' in advance of such maintenance.
- Service availability - Save during routine maintenance and upgrades IRIS will use reasonable endeavours to ensure that My ePay Window will be available at least 98% of the time within each calendar month between the hours of 8.00am and 8.00pm

2 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.

3 MY EPAY WINDOW ORGANISATIONAL SECURITY

IRIS 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 My ePay Window uses or handles personal data. The statement of assurance (see 2.0) is provided in order to assure our customers and staff of our commitment to data security.

Additionally, this document sets out the My ePay Window 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 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 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 My ePay Window respects privacy and treats personal data lawfully and correctly.

Supporting accreditations held by My ePay Window are:

- ISO27001
- **Cyber Essentials** (Planned 2024)
- ISO9001

Our support function also holds the following accreditations:

- ISO9001 (Support Function)
- ISO27001 (Support Function)

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

- ISO27001
- ISO9001
- ISO14001
- SOC 1
- SOC 2
- SOC 3
- FedRAMP
- HITRUST
- IRAP
- CJIS
- PCI-DSS

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 My ePay Window

With My ePay Window, 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 My ePay Window 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 My ePay Window, 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
Chris Malcolm	HCM Engineering	Engineering Director, Staffology
Nigel Francis	Product	Product Director, Bureau desktop payroll
Laurence Robinson	HCM Engineering	Software Engineering Manager, My ePay Window
Thomas Derbyshire	Customer Service/Support	Senior Manager, Customer Services
Yellie P Williams	Professional Services	Professional Services Director
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group

The My ePay Window 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 My ePay Window.

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 My ePay Window penetration test: 19th April 2023

The My ePay Window 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 My ePay Window 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 My ePay Window's IT systems and for keeping systems reasonably up to date.

My ePay Window Development systems are managed by a local internal development team.

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

Client defined classifications: Client information and materials processed, stored or transmitted by My ePay Window shall be handled strictly in line with GDPR guidance/best practice for personal data.

3.3 IRIS Support staff could have access to your data to fulfil the support aspect of the My ePay Window Solution.

My ePay Window support staff do not have general access to My ePay Window Employee payroll data, except for the information shared with them by clients during the course of a individual support case investigation and sufficient for them to escalate to the My ePay Window development team. Only designated IRIS My ePay Window software developers can access the My ePay Window database.

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 / My ePay Window 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.

For My ePay Window 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.

In addition, we also offer users the ability to add additional authentication in their My ePay Window accounts via either 2-step and Two-factor Authentication (2FA). Either of these additional security options can be enforced by Employer level users and Payroll department (Bureau) users for all the users/employees in their organisations.

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 / My ePay Window warrants to Clients that it will not seek to circumvent, compromise or change the Client's security controls, and My ePay Window 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 PHYSICAL AND ENVIRONMENTAL SECURITY

My ePay Window 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 Rackspace Managed Hosting

The My ePay Window service is hosted on IRIS's dedicated UK Rackspace managed service environment:

Equipment	Description
Physical Security	<p>Physical Security includes locking down and logging all physical access to the Rackspace data centre.</p> <ul style="list-style-type: none"> • Data centre access is limited to only authorised personnel • Badges and biometric scanning for controlled data centre access 24x7 security camera monitoring at all data centre locations Access and video surveillance log retention • 24x7 onsite staff provides additional protection against unauthorised entry • Unmarked facilities to help maintain low profile • Physical security audited by independent firms annually
Network Infrastructure	<p>Network Infrastructure provides the availability guarantees backed by aggressive SLAs.</p> <ul style="list-style-type: none"> • High-performance bandwidth provided by multiple network providers Elimination of single points of failure throughout shared network infrastructure • Cables properly trunked and secured • Proactive network management methodology monitors network route efficiency • Real-time topology and configuration improvements to adjust for anomalies • Network uptime backed by Service Level Agreements • Network management performed by only authorised personnel • Virus and Malware protection provided by Sophos • Cisco firewall technology provides protection from Internet and Rackspace public network • Access to Network from IRIS via DUO authenticated VPN client • Application traffic is protected by AlertLogic intrusion detection devices, Cisco ASA firewalls, port restrictions on F5 load balancers, and at the endpoints,
Human Resources	<p>Human Resources provides Rackspace employees with an education curriculum to help ensure that they understand their roles and responsibilities related to information security. Reference checks taken for employees with access to customer accounts.</p>

	<ul style="list-style-type: none"> • Employees are required to sign non-disclosure and confidentiality agreements. • Employees undergo mandatory security awareness training upon employment and annually thereafter.
Operations Security	<p>Operational Security involves creating business processes and policies that follow security best practices to limit access to confidential information and maintain tight security over time.</p> <ul style="list-style-type: none"> • ISO 27001/2 based policies, reviewed at least annually • Documented infrastructure change management procedures • Secure document and media destruction • Incident management function • Business continuity plan focused on availability of infrastructure. • Independent reviews performed by third parties • Continuous monitoring and improvement of security program
Environmental Controls	<p>Environmental Controls implemented to help mitigate against the risk of service interruption caused by fires, floods and other forms of natural disasters.</p> <ul style="list-style-type: none"> • Dual power paths into facilities • Uninterruptable power supplies (minimum N+1) • Diesel generators (minimum N+1) • Service agreements with fuel suppliers in place • HVAC (minimum N+1) • Smoke detectors • Flood detection • Continuous facility monitoring
Security Organisation	<p>Security Organisation includes establishing a global security services team tasked with managing operational risk, by executing an information management framework based on the ISO 27001 standard.</p> <ul style="list-style-type: none"> • Security management responsibilities assigned to Global Security Services • Chief Security Officer oversight of Security Operations and Governance, Risk, and Compliance activities • Direct involvement with Incident Management, Change Management, and Business Continuity.

5.2 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.

5.3 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.(see 6.1)
Change management	Change management controls have been implemented to ensure satisfactory control of all changes. Routine My ePay Window updates are subject to weekly 'Change Board' review and sign-off prior to deployment. 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). (see 6.1 for My ePay Window)

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.
My ePay Window Backups	Weekly full backups and daily incremental backups are carried out at Rackspace Ltd. Daily backups are maintained securely for 4 weeks offsite.
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 My ePay Window DevOps 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. Rackspace Ltd controls clock settings for the My ePay Window environment ensuring that servers adhere to 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. Installation of software on My ePayWindow production servers is via designated IRIS development engineers only and in agreement with IRIS DevOps team.
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 implications are reviewed by the Architecture Review Board. Weekly vulnerability scanning is carried out on the My ePay Window production servers and critical & high severity updates applied within 14 days.
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 Rackspace Ltd, that uses world class security protocols to ensure security compliance (See 6.1 and accreditation details in 'Organisational Security' section).
Segregation of networks	The MyePaWindow web application and its data are physically and logically separated in the hosted environment. The My ePay Window environment 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.

Data is encrypted in transit via SSL (AES256) & TLS 1.2 protocol between the IRIS Payroll desktop software applications and from Staffology Payroll to the My ePay Window self-service portal and Data and documents on the My ePay Window service are encrypted at rest to AES256.

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 – My ePay Window 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 My ePay Window 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 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.
Vulnerability Testing	My ePay Window is subject to automatic code vulnerability scanning and product management and engineering staff are alerted to any vulnerabilities requiring remediation. High severity vulnerabilities are prioritised and scheduled for deployment as quickly as possible.

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 PROCESSING LOCATIONS AND INTERNATIONAL DATA TRANSFERS

On occasion, Rackspace Ltd engineers and third parties located in USA maybe used for 24/7 production environment support. In any such instance, Rackspace Engineers have no access to the My ePay Window database information.

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.

11 SUPPLIER RELATIONSHIPS

11.1 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 My ePay Window processing customer data 23rd November 2023.

11.2 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.

11.3 External Suppliers which are Data Processors

External Data Processors	Data Location	Description
Rackspace Ltd	UK	Hosting services for the IRIS My ePay Window service. Certifications: ISO27001, AICPA-SOC & PCI-DSS.
Mailgun (Sinch)	US	Mailgun is used by IRIS My ePay Window for system generated email delivery (No Payroll data is transmitted in email content or attachment). This process is covered by the EU Standard contract clauses for data transfers to third countries. Note: The EU considers that the US provides comparable safeguards to those of the EU and ensures an adequate level of protection for personal data transferred from the EU to certified organisations in the US
Brevo	EEA	Brevo is used by IRIS My ePay Window for system generated email delivery (No Payroll data is transmitted in email content or attachment).
Sales Cloud via Salesforce	UK	Our support function uses Sales Cloud to provide customer ticketing, communication, live chat and query resolution management.
OKTA	UK	OKTA is My ePay Window & IRIS Software identity management provider and helps companies manage and secure user authentication into applications.

12 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

12.1 Information security continuity

Information Security Continuity	Description
Planning information security continuity	During adverse situations, My ePay Window have a number of secure ways to ensure the continuity work carried out.
Implementing information security	My ePay Window 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	My ePay Window/IRIS 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 environments (Rackspace Ltd) to ensure continuity. IRIS service level agreement terms provided by Rackspace Limited, provides 100% availability of the network and repair of any problem hardware component within one hour of identification, additional time may be required to rebuild a RAID array or to reload operating systems and or applications.

13 COMPLIANCE

13.1 Compliance with legal and contractual requirements

Legal and Contractual Requirements	Description
Identification of legislation and contractual requirements applicable to My ePay Window	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	My ePay Window is a pay data delivery portal and data is retained in accordance with its data retention policy (see section 14.5). Source Payroll data is held in the source Payroll processing software and held in accordance with that software's retention policy
Privacy and protection of personally identifiable information	Covered within My ePay Window's privacy policy both at local and IRIS group level.
Regulation of Cryptographic Controls	<p>My ePay Window 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.</p> <p>Personal data is stored in MS SQL with data encrypted at rest using 256-bit AES encryption.</p>

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.
My ePay Window Security Penetration testing	The My ePay Window website undergoes annual penetration testing and any findings are remediated as soon as practicably possible

13.3 Data Protection – quick reference

Contact	Details
IRIS Group Data Protection Officer	Vincenzo Ardillio – dataprotection@iris.co.uk
Data protection owner for My ePay Window	Nigel Francis – nigel.francis@iris.co.uk

Categories of personal data processed as part of the My ePay Window Service provision:

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

13.4 Location of personal data processing

All personal data is held within the My ePay Window database and on electronic documents from client communicating this data to My ePay Window. 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.

13.5 MY EPAY WINDOW Retention of data

- Payslips, P60s, P11Ds, P45s, CIS statements are retained for at least 12 months and for the duration of processing of the client's data on My ePay Window
- Auto enrolment letters are retained for 12 months after which they are auto-deleted
- Any documents uploaded to My ePay Window will be available for at least 3 months and the Website will warn you in advance of any deletions so that you can download information in advance.
- If an Employee leaves an Employer their data and access to it will be maintained for 15 months, during which information can be downloaded as required. After 15 months their account will be disabled and after a further 1 month their data will be anonymised.
- Client's who have not accessed or uploaded new data in the preceding 12 months will be deemed to be no longer using the IRIS My ePay Window service and will have their accounts blocked and their data will be anonymised after a further 3 months.
- We may use aggregated information for the purposes of monitoring use of the Website. Such aggregated information may be provided to third parties. These statistics will not include information which can be used to identify any individual, Client Company or client entity or the nature of its employment or business.
- For the avoidance of doubt, we shall not use any personal data held on the Website for any marketing purposes.


13.6 Data subject rights

My ePay Window processes personal data lawfully and for the purposes of payroll processing and to allow our clients to provide various payroll statements relating to their employees according to UK employment legislation. All users of IRIS My ePay Window, must consent to their information being available on the service as part of the site registration process and with sight of the My ePay Window service privacy policy. Any users declining consent are referred to their 'Employer' (for discussion) and their account registration is stopped.

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 their IRIS payroll software support desk.. 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 AVAILABLE APPENDICES

Details	
Rackspace Managed Hosting	https://www.rackspace.com/en-gb/compliance
IRIS Desktop Payroll – Customer Information security assurance statements	Available on Request
Staffology Due Dilligence	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



IRIS | My ePay Window

IRIS Software Group
Heathrow Approach
470 London Road,
Slough,
SL3 8QY
0344 815 5555
hcmproduct@iris.co.uk
<https://www.iris.co.uk/products/iris-my-epay-window/>