IRIS Software Group

Information Security Assurance Statement

Status	Published
Version	1.0
Prepared	1 October 2026
Scope	IRIS UK Accounting and HCM Products
Owner	Senior Director of Information Security
Approver	Chief Product Officer
Review cycle	Annual, plus on material change

1. Purpose and scope

1.1 This statement describes the technical and organisational measures IRIS Software Group applies to protect customer personal data, for the purposes of Article 32 of the UK GDPR and clause 3 of the IRIS Customer Data Processing Terms.

1.2 It applies to every IRIS product and service for which a Product Annex is published in Appendix 2. Where a control differs by product, the difference is recorded in that product's Annex and nowhere else.

1.3 This statement does not vary the IRIS Customer Data Processing Terms or the IRIS General Terms and Conditions. Where there is any conflict, those documents prevail.

2. How to read this statement: deployment models and overlays

2.1 IRIS products are delivered under four deployment models. Your Product Annex states which model can apply to your service. Controls in this statement are marked with the models to which they apply.

Model	Description	Effect on responsibility
A	IRIS-hosted software as a service. IRIS operates the infrastructure on which the software runs.	IRIS holds all infrastructure controls described below.
B	Customer-hosted. The software runs on infrastructure the customer owns or procures.	Infrastructure controls marked Model B are the customer's responsibility. IRIS's internal access, development and support controls continue to apply in full.
C	Customer choice. The software may be deployed under Model A or Model B.	Both sets of clauses apply. The Product Annex records which deployment the customer has taken.
D	Managed service. IRIS personnel operate the service on the customer's behalf.	As Model A, with the additional provisions in section 20.

2.2 Four overlays apply only where the Product Annex says so: artificial intelligence (section 18), payments (section 19), managed service (section 20), and employment and income verification (section 21).

3. Statement of assurance

3.1 IRIS commits to: put in place measures to protect customer information from a breach of security; meet its regulatory and legislative requirements; produce, maintain and test business continuity plans; provide information security training to all staff; report and investigate information security incidents; and monitor compliance with the IRIS Information Security Policy.

3.2 IRIS does not create undocumented passwords, maintenance credentials or other undisclosed methods of remote access into its software. IRIS will not seek to circumvent, compromise or change a customer's security controls, and will not change a customer's software configurations without proper authorisation.

4. Governance

4.1 IRIS operates a group Information Security Management System. Security governance is exercised by a standing group forum chaired by the Senior Director of Information Security, which meets at least quarterly and reviews policy, risk, incidents and supplier assurance.

4.2 All IRIS products must meet, or be working towards meeting, the standards of the IRIS Information Security Management System, except those which hold their own certification under ISO/IEC 27001 or another recognised information security standard. Products in the latter category are identified in their Product Annex.

4.3 A risk assessment is performed for each product at least annually.

5. Certifications and independent assurance

5.1 IRIS Software Group holds the following certifications, all available upon request:

- ISO/IEC 27001, certificate number IS746670, issued by British Standards Institution (BSI), covering the following scope: development, implementation and support of Human Capital Management (HCM) software, Managed Payroll services, Education Management software and Finance & Accounting software in accordance with the IRIS BMS Scope Document and Statement of Applicability v2.0 22/01/2024.
- ISO/IEC 9001, certificate number FS746677, issued by British Standards Institution (BSI). Scope is as above for ISO27001.
- Cyber Essentials, certificate number b76f231c-92bd-49a0-855d-d55a349c9e92, issued by CyberSmart. Scope is whole organization.

5.2 Certification is audited annually by an external assessor. Internal compliance with the group Information Security Management System is reviewed annually by the IRIS compliance function.

5.3 Where a product holds certifications in addition to the group certificate, those are listed in its Product Annex. Where a product is not within the scope of the group certificate, the Product Annex says so.

5.4 Where infrastructure is provided by a third party, IRIS inherits that provider's physical and environmental controls. The provider's own certifications are published by the provider and are not reproduced here.

6. Personnel security

6.1 All staff and contractors are subject to identity, right to work, employment history and reference checks before appointment.

6.2 All staff complete information security and data protection training on appointment and at least every twelve months, covering data security, third-party access, phishing and social engineering. Completion is monitored and is a performance matter.

6.3 All staff accept the group Data Protection Policy, Incident Reporting Procedure and Information Security and Acceptable Use Policy. Confidentiality obligations survive termination. Breaches are handled under the disciplinary process.

6.4 On termination, access is revoked and assets recovered before departure. On a change of role, access is re-provisioned to the new role rather than added to.

7. Access control: IRIS personnel

7.1 Access is granted on a least-privilege basis, by role, and only where the role requires it. By default an IRIS employee has no access to customer data.

7.2 Access to any system holding customer personal data is only permitted from the IRIS corporate network, which requires multi-factor authentication.

7.3 Access to cloud administration consoles and other privileged interfaces requires authentication against the IRIS corporate identity provider, from the IRIS corporate network, which enforces multi-factor authentication at network level under clause 7.2. Privileged accounts are separate from normal user

accounts and are not shared. Where multi-factor authentication is additionally enforced at the console itself, the Product Annex says so.

7.4 IRIS support and engineering staff can access customer data where their role requires it. Support access operates in defined tiers:

Tier	What this tier can do
Standard support	View the customer's configuration and account information and interact with the product as the customer would, for diagnostic purposes.
Account administration	Create, deactivate and reactivate customer accounts and manage modules and entitlements.
Advanced support	View and compare customer-specific records, including personal data, in order to resolve a fault.
Data administration	Direct database access, including the ability to read, change and delete all customer records.

7.5 All access above standard support is individually named, logged, attributable and reviewed at least every six months. Access no longer required is removed. Every change to a user role is recorded in an audit log capturing the tenant, the account making the change, the account changed, the time in UTC, whether the role was assigned or removed, the role involved and the originating IP address. The audit trail applies to all users regardless of privilege level.

7.6 Models B and C-on-premise - Where the software runs on customer infrastructure, IRIS has no standing access. Access is by the customer's invitation, for a specific purpose, and is logged.

8. Access control: customer-facing

8.1 Multi-factor authentication is available to all users and can be enforced across an organisation by a customer administrator. Single sign-on is available. Where a product does not offer one of these, its Product Annex says so.

8.2 Where IRIS enforces a password policy, the minimum is at least ten characters including an upper-case letter and a number, enforced by the software. Where a product allows the customer to set its own policy, the Product Annex says so.

8.3 Customers are responsible for their own users' role assignments within the product.

9. Encryption

9.1 Customer personal data is encrypted at rest using AES-256 or an equivalent recognised standard.

9.2 Data in transit between the customer and the service, and between service components, is encrypted using TLS 1.2 as a minimum, and TLS 1.3 where supported by the client.

9.3 Encryption keys are managed throughout their lifecycle in accordance with the group encryption policy. Where keys are managed by a hosting provider, the Product Annex says so.

9.4 Models B and C-on-premise - Encryption of data held on customer infrastructure is configured by the customer. Where the encryption options available in the software differ from the standard above, the Product Annex says so.

10. Hosting, physical and environmental security

10.1 Models A, C-hosted, D - Except where the Product Annex states otherwise, IRIS does not own or operate data centre facilities. Infrastructure is provided by the hosting partner named in the Product Annex, and

IRIS inherits that partner's physical and environmental controls, including access control, surveillance, power resilience and fire suppression.

10.2 Models B and C-on-premise - Physical and environmental security of the infrastructure on which the software runs is the customer's responsibility.

10.3 IRIS offices holding customer data are access-controlled, and clear desk and screen locking policies apply.

11. Operations security

11.1 Operating systems and software are patched on a defined schedule. Critical security patches are applied within 14 days of release.

11.2 Code, web applications and infrastructure are regularly assessed for vulnerabilities in accordance with IRIS security policies and standards. Findings are triaged severity and remediated according to IRIS' patch management policy. Code carrying a critical vulnerability is blocked from deployment.

11.3 Anti-malware protection is deployed and centrally monitored across the estate, with signatures updated automatically. Inbound email is filtered for malware, spam and malicious attachments.

11.4 Removable media is disabled by default. Equipment and media are disposed of by a certificated destruction service.

11.5 Models B and C-on-premise - Patching of the operating system and infrastructure on which the software runs is the customer's responsibility. IRIS is responsible for patching the software itself.

12. Secure development and test data

12.1 Development follows a documented secure development lifecycle. Security is considered at design, designs are reviewed by architects and security specialists, and all changes require peer review and automated static and dependency analysis before release.

12.2 Development, test and production environments are segregated. Developers do not have standing access to production environments; access is granted for a specific authorised purpose and is logged.

12.3 Production data is not used in development or test as a matter of routine. Test data is created by the quality assurance teams. Where a fault cannot be reproduced with synthetic data, customer data is released only after a formal access request, and is destroyed as soon as it is no longer needed. Data shared with a development partner is scrambled unless the customer specifically authorises otherwise.

12.4 A formal change advisory process governs releases, with an expedited path for urgent changes that is itself reviewed.

13. Logging, monitoring and audit

13.1 User activity, exceptions, faults and security events are logged. Administrator and operator activity is logged separately, protected against alteration and reviewed regularly.

13.2 Authentication events are monitored by security monitoring tooling with alerting on anomalous activity. Alerts are actioned by the operations team, a 24x7 security operations function.

13.3 Logs are retained in active storage for 90 days, in warm storage for one year. Only nominated administrative accounts hold read access to log stores. Server clocks are synchronised to UTC against authoritative time sources.

13.4 Models B and C-on-premise - Audit logs are written to the customer's own servers. Retention and protection of those logs is the customer's responsibility.

14. Backup, restore and business continuity

14.1 Models A, C-hosted, D -Customer data is backed up at least daily and retained for a period proportionate to the recovery objectives stated within each Product Annex. Where a service differs, its Product Annex says so. Backups are encrypted and held in a separate location from the primary environment.

14.2 Restoration is tested at least annually and the test is documented.

14.3 Recovery point and recovery time objectives are stated in each Product Annex. Where no objective has been established for a service, the Annex says so.

14.4 IRIS maintains business continuity plans covering business and technical recovery. Plans are tested at least annually.

14.5 Models B and C-on-premise - Backup, restore testing and verification of data held on customer infrastructure are the customer's responsibility. IRIS's obligations are limited to the availability and recoverability of the software itself.

15. Penetration testing

15.1 Each service is subject to independent third-party penetration testing at least annually, and after any significant change. Automated security testing is performed more frequently, at the cadence stated in the Product Annex. Testing is performed by an independent provider holding a recognised industry accreditation.

15.2 Findings are prioritised, remediated and retested.

15.3 The date of the most recent test, the date of the next scheduled test, and a summary report are available on request under non-disclosure agreement.

16. Sub-processors

16.1 IRIS maintains a single group sub-processor register, published as Appendix 1 to this statement, listing third parties that process customer personal data on IRIS's behalf. For each the register states the name, a description of the processing carried out, and the country in which data is processed.

16.2 The register is a single list covering all IRIS software and services. Not every sub-processor is used for every product; which of them process data for a given service depends on the product, the modules enabled and the customer's configuration. The list applicable to a specific service is available on request.

16.3 Changes to sub-processors are notified in accordance with clause 4.1 of the IRIS Customer Data Processing Terms, giving customers the opportunity to object on grounds of non-compliance with data protection law.

16.4 Each sub-processor is appointed under a written contract imposing equivalent obligations, is assessed before appointment and reviewed annually, and IRIS remains liable for its acts and omissions.

16.5 Certain IRIS group entities act as sub-processors to other IRIS products. These are identified as such in the register.

16.6 Third parties that determine their own purposes for processing, including the employment and income verification partners in section 21, act as independent controllers and are identified separately in the register.

17. International transfers and offshore support

17.1 Customer data is stored in the location stated in the Product Annex. Where a sub-processor processes data in an additional location, that location is stated in the sub-processor register at Appendix 1 and the transfer is made in accordance with clause 17.4.

17.2 IRIS uses support and engineering teams outside the United Kingdom, in the countries listed in the Product Annex. Where those teams access customer data, they do so remotely into systems located in the region stated in the Annex; the data itself does not leave that region.

17.3 Access by a team outside the United Kingdom is granted at the customer's request for a specific purpose and is automatically removed thirty days after it is granted.

17.4 Where personal data is transferred outside the United Kingdom, the transfer is effected by way of Appropriate Safeguards as defined in, and in accordance with,the relevant international data transfer agreement or EU standard contract clauses as applicable. Transfers to a country benefiting from UK adequacy regulations are made on that basis.

18. Artificial intelligence and automated customer support

18.1 Where a service includes artificial intelligence features, they are identified in the Product Annex and the AI providers are listed in the sub-processor register.

18.2 Customer personal data is not used to train or improve any third-party AI model. Where an AI support agent references personal data provided during a conversation, that data is subject to the same access controls and retention rules as any other support interaction.

18.3 AI-generated responses draw on controlled source material. Outputs affecting a regulated calculation are subject to human review, and IRIS follows HMRC guidance on the use of generative AI in payroll software.

18.4 Customers can request human handling of any support interaction.

18.5 Where a product makes an automated decision with legal or similarly significant effect, the decision is identified to the data subject and a route to human intervention is provided.

19. Payments overlay

19.1 This section applies where the Product Annex records the payments overlay.

19.2 Payment processing is performed by the providers identified in the sub-processor register. Card data is not stored by IRIS.

20. Managed service overlay

20.1 This section applies where the Product Annex records deployment Model D.

20.2 IRIS personnel process customer data as part of delivering the service. Access is inherent to the service rather than exceptional, is role-based, and is subject to sections 6 and 7.

20.3 Where the service submits payments, the payment and banking providers are identified in the sub-processor register. Any accreditation IRIS holds for that purpose is stated in the Product Annex.

20.4 Statutory retention periods applying to the service are stated in the Product Annex, together with the obligation that requires them.

21. Employment and income verification

21.1 This section applies where the Product Annex records the verification overlay.

21.2 Where enabled, the service transmits employment and income information to authorised verification partners so that an employee can verify employment and income when applying for financial products. The categories transmitted are Personal Information, Income Summary and Detailed Payslip Information, and the partners are named in the sub-processor register.

21.3 Those partners determine their own purposes for the processing and act as independent controllers, not as sub-processors of IRIS.

21.4 The functionality is optional. An employer may opt out at organisation level or for individual employees, in accordance with clause 4.4 of the IRIS Customer Data Processing Terms.

21.5 Records not updated for fifteen months are automatically deleted from the connector.

22. Incident management and breach notification

22.1 IRIS operates a documented incident management process with defined severity levels, a named incident manager, root cause analysis for critical incidents and a post-incident review.

22.2 On confirming a personal data breach affecting customer data, IRIS notifies the customer without undue delay in line with ICO Guidance, and provides the information the customer needs to meet its own obligations.

22.3 As processor, IRIS does not notify a supervisory authority on the customer's behalf unless the customer instructs it to do so in writing.

23. Data retention, deletion and exit

23.1 Customer data is retained for the period stated in the Product Annex, together with the legal or regulatory obligation that requires it.

23.2 On termination, the customer has thirty days to extract or request a copy of their data. After that period IRIS deletes it, subject to any statutory retention obligation stated in the Annex.

23.3 On request, IRIS returns a copy of the customer's data in such form as the customer reasonably requests, in accordance with the IRIS Customer Data Processing Terms.

23.4 Models B and C-on-premise - Removal of the software and any data held on customer infrastructure is the customer's responsibility.

24. Compliance, audit rights and the assurance pack

24.1 IRIS makes the following available on request, under non-disclosure agreement where appropriate: the group ISO/IEC 27001 certificate and scope statement, a penetration test summary for the service, the IRIS delivery centre assurance statement and risk assessment, the group data protection statement, and supplier due diligence records.

24.2 Customer audit rights are as set out in clause 7 of the IRIS Customer Data Processing Terms.

24.3 This statement is reviewed annually and on material change. The version and review date are on the cover.

24.4 Data protection enquiries relating to this statement, including requests for the assurance materials listed above, should be directed to ProductOps@iris.co.uk.

Appendix 1 - IRIS sub-processor register

The table below lists the sub-processors engaged across IRIS software and services. Not every sub-processor is used for every product. Which of them process data for your service depends on the product you use, the modules you have enabled and your configuration.

A1.1 This register is maintained under section 16 of the core statement. Changes are notified in accordance with clause 4.1 of the IRIS Customer Data Processing Terms, which gives customers the opportunity to object on grounds of non-compliance with data protection law.

A1.2 The list of sub-processors applicable to a specific service is available on request.

A1.3 Where a sub-processor is used in more than one location, every location is stated and joined with an ampersand. A combined entry means the sub-processor may process data in any of the locations shown, not that it processes in all of them for every customer.

Sub-processors

Sub-processor	Description of the processing	Data location
6degrees	Data centre hosting for the international payroll file transfer service. Provides the physical infrastructure and does not access customer data.	UK
Abstract Group Ltd	Third-party software development partner supporting software development and DevOps processes.	UK & India
Accountis Europe Limited (Finastra)	Gateway service allowing submission of payments through the UK Bank Automated Clearing System.	UK
Amazon SES	Cloud-based transactional email delivery. Processes sender, recipient and copy-recipient names and contact details, and anything contained in the message body.	UK
Amazon Web Services	Hosting, storage and associated services for the cloud platform. Also used to provide automations and enhancements to customer services, including query resolution, management and communications.	UK & US
AMS	Managed file transfer, used for the secure exchange of payroll files between IRIS and the customer.	UK
Apigee (Google)	API management platform providing OAuth 2.0 client credentials and request routing for integrated services.	UK & EU
App Direct	Operates the IRIS Marketplace, enabling users to browse and purchase IRIS software digitally.	US
Bottomline (BACS PTX)	Used to transmit employee payments and other payroll-related third-party payments within the UK. Sign-up required.	UK
Brevo	System-generated email delivery. No payroll data is transmitted in message content or attachments.	EEA
Cybage Software Private Limited	Third-party software development partner supporting development, DevOps and defect resolution. Customer data shared for defect resolution is obfuscated unless the customer specifically authorises otherwise.	India
Datadog	Observability and monitoring, collecting logs, metrics and diagnostic data to support issue investigation and resolution. Logs may contain limited personal data such as user email addresses.	US
Freshdesk	Customer ticketing, communication and query resolution management. Processes contact details and support correspondence.	EEA

Gainsight (CX and PX)	In-product help, product usage analytics and customer health scoring. May process customer account, user profile, product usage and interaction data.	EU
Genesys Cloud	Web messaging, live chat and co-browse functionality for in-product support queries, including AI-assisted query routing.	UK
Global Payments	Used to facilitate the online payment of customers' clients' invoices.	US
GlobalSign	Enables customers' clients to securely and electronically approve and sign documents. Only the minimum data required to effect an approval or signature is transmitted.	UK
GoCardless	Used to facilitate the online payment of customers' clients' invoices.	EAA
Ideal Postcodes	Address disambiguation and completion from postcodes. Data is not retained by the provider.	UK
Integrity Print Ltd	Secure printing and postal distribution of payslips, P60s and P45s where delivery is required by post.	UK
Intercom (including Fin)	AI agent for customer service, generating responses from existing knowledge sources. May reference personal data a user provides during a conversation. IRIS does not use personal data as training data or for model improvement.	UK, US & EEA
IRIS Cerberus	IRIS group service providing a hosted secure document transfer environment. Access is restricted and data is held in UK data warehouses.	UK
IRIS KPO Resourcing (India) Private Limited	IRIS group company providing support services and payroll processing. Personnel connect over the internal IRIS VPN to process data held on UK servers.	India
Jira (Atlassian)	Development lifecycle management, with fourth-line support tickets managed through the platform.	UK
LogMeIn Rescue	Remote support connection to a user's device, initiated at the user's invitation for fault diagnosis.	EU
Marketo	Customer communications, campaign management and engagement tracking. Processes limited business contact and engagement data.	UK
Microsoft Azure	Hosting environment for software and client data, including database services and the employment verification connector.	UK, ROI & EEA
Microsoft Azure DevOps	Development lifecycle management, with fourth-line support tickets managed through the platform.	UK
Mimecast	Inbound and outbound email filtering, spam control and scanning of attachments for malware.	UK
Okta	Identity and authentication provider used within IRIS Identity, managing and securing user authentication into applications. Stores usernames, passwords and multi-factor credentials.	UK
PayPal	Payment processing where the customer enables the functionality.	US
PayVector (AI Corporation)	Used to collect subscription payments.	UK & North-west Europe
Payzaar Limited	Software provider for the online platform used to transfer data to and from clients, generate reports, track the end-to-end payroll cycle and distribute payslips.	EEA
Pendo	Product analytics, in-app guidance and NPS surveys. Processes user email addresses and in-app behaviour.	EU
Rackspace Ltd	Managed hosting, cloud storage and managed backup for the hosted environment.	UK
Reach Interactive	SMS delivery. Processes message content and recipient mobile numbers.	UK

Safe PC Disposal; Shred-It	Certificated destruction of IT equipment, media and confidential paper records, to WEEE standards.	UK
Salesforce (Sales Cloud and Service Cloud)	Customer ticketing, communication, live chat and query resolution management.	UK
SendGrid (Twilio)	Cloud-based transactional and marketing email delivery, management and analytics. Processes sender, recipient and copy-recipient details and anything contained in the message body. Not used where the customer sends through its own SMTP relay.	UK & US & EEA
Square	Used to facilitate the online payment of customers' clients' invoices.	US
Stripe	Card payment processing for invoicing, subscriptions and the purchase of storage and document signing credits. Only the minimum data required to effect a payment is transmitted.	US
Sumo Logic	Log aggregation and retention.	EU
Telleroo	Used to transmit employee payments and other payroll-related third party payments by Faster Payments within the UK. Sign-up required.	UK
UNIpaaS	Used to facilitate the online payment of customers' clients' invoices.	EU & UK
Voiceflow	AI chatbot component within the product.	US
Convera	International funds transfer for the international payroll service.	UK
Worldpay	Used to facilitate the online payment of customers' clients' invoices.	US
Zoho (ServiceDesk Plus)	Internal CRM and ticketing. Processes contact details and support correspondence relating to IRIS staff and clients.	EEA

Third parties acting as independent controllers

The following organisations determine their own purposes for the processing and are not sub-processors of IRIS. Where a service transmits data to them, that functionality is optional and may be opted out of in accordance with clause 4.4 of the IRIS Customer Data Processing Terms.

Organisation	Description of the processing	Data location
Equifax	Authorised external data partner for the online verification of employment and income, where an employee applies for a financial product such as a mortgage, loan or tenancy agreement.	UK
Experian	Authorised external data partner for the online verification of employment and income, where an employee applies for a financial product such as a mortgage, loan or tenancy agreement.	UK
Teal Connect Ltd	Authorised external data partner for the online verification of employment and income, where an employee applies for a financial product such as a mortgage, loan or tenancy agreement.	UK
TransUnion	Anti-money laundering and related regulatory checks performed against customers' clients and employees.	UK

Customer-initiated integrations

These are third parties a customer chooses to connect to an IRIS product. IRIS does not appoint them, they are not IRIS sub-processors, and the customer is responsible for its own relationship with them, including their processing locations.

Third party	Description

Accounts IQ, Adsum, Bottomline, Breathe HR, Cezanne HR, Ciphr, Cornerstone, Deputy WFM, Dext, Dropbox, FreeAgent, iFinance, Modulr, MyWorkpapers, Nest Pensions, Penfold Pensions, Peoples Pensions, QuickBooks, Quinyx, RotaCloud, Sage, Smart Pensions, Square, Sync Savings, Telleroo, Twinfield, WeWorked, Xero, Yapily, Zapier	Accounting, automation, bookkeeping, document storage, HR and HCM, open banking, payments and banking, pensions, and workforce scheduling services that a customer connects to an IRIS product using its own credentials.
Companies House; HMRC	Statutory submission and public register lookup, performed on the customer's instruction and in accordance with the relevant technical specifications.

Appendix 2 - Product Annexes

Each annex states the facts specific to that product. The core statement applies in full to every product except where an annex states otherwise. Where a product is delivered on the customer's own infrastructure, some controls necessarily sit with the customer. Those are listed under "Customer responsibilities", which brings together in one place the controls the core statement places with the customer under that deployment model. The table restates the core statement for convenience and records no departure from it Where a product implements a control differently from the core statement, the annex states what the product does.

IRIS Elements Platform

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	AI. Offshore support: India and Romania
Hosting, region and data location	Amazon Web Services, region eu-west-2 (London).
Certifications	• ISO9001; • ISO27001;
Personal data and data subjects	Client, Prospect and non-client names, addresses and contact details; directors and business officers. Article 9 or 10: no
Data retention and basis	Customer self-service deletion of user profiles, customers and records. IRIS retains its own business records under core clause 23
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Multi-factor authentication is available to all users. It can be mandated on specific user journeys where a third-party integration requires it.
9.1, 9.2	Data at rest is encrypted using AES-256 encryption. Encryption keys are managed via AWS Key Management Service (KMS), using an envelope encryption model in which a master key controls access to underlying data encryption keys. Key management and the encryption implementation are handled by AWS as part of the underlying managed database service. Data in transit is encrypted using TLS, with a minimum enforced protocol version of TLS 1.2 and support for TLS 1.3.
14.1	Backups are taken daily and retained for seven days.

Staffology Payroll

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	Payments (BACS and Faster Payments). Verification. AI. Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom. Sub-processor locations are stated in Appendix 1
Certifications	• ISO9001; • ISO27001; • Cyber Essentials • HMRC Approved Software Vendor • The Institute of Certified Bookkeepers (ICB) Approved Software Vendor • G-Cloud framework
Personal data and data subjects	Employee payroll and payment data. Data subjects: employees, trainees, and next of kin where a beneficiary payment is made through payroll. Article 9: yes, trade union membership identifiable through deductions. Article 10: yes, court order fines processed through payroll
Data retention and basis	Platform: customer-controlled, retained until deleted by a customer administrator. IRIS myePayWindow: documents at least 3 months, payslips and statutory documents at least 12 months, auto-enrolment letters 12 months, leavers 15 months then anonymised after a further month. Verification connector: rolling 15 months
Recovery objectives	Recovery point objective 4 hours. Recovery time objective 72 hours.
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Single Sign-On (SSO) can be configured via IRIS Identity (OKTA) Multi-factor Authentication (MFA) can be is option for Users via IRIS Identity (OKTA) and can be mandated at Employer level.
14.1	Back-ups are retained for a period of 30 days.
15.1	Automated security testing is performed weekly. Independent penetration testing is performed annually
23.1	Payroll data is retained on the platform until deleted by a customer administrator, so that the customer controls its own statutory retention period. IRIS deletes data on instruction and on termination under clause 23.2.

IRIS Accountancy Suite

Field	Entry
Deployment model	C - customer-hosted, IRIS-hosted, or hosted by a third party at the customer's choice
Overlays	Offshore support: India
Hosting, region and data location	The customer's own infrastructure, the IRIS hosting service, or a third-party host chosen by the customer. Support and telemetry data: United Kingdom
Certifications	None claimed.
Personal data and data subjects	Client accounting and tax records held by the practice, and employees of the practice's clients for P11D purposes. Article 9 or 10: no
Data retention and basis	Customer-controlled. IRIS retains its own business records under core clause 23
Recovery objectives	Customer-hosted: the customer's responsibility. IRIS-hosted: recovery objectives are managed as part of the IRIS hosting service. No product-specific recovery point objective (RPO) or recovery time objective (RTO) has been established for IRIS Accountancy Suite.
Annex date last confirmed	1 September 2026

Customer responsibilities where the software runs on customer infrastructure

This table applies where the customer has taken the on-premise deployment under Model B or C. It brings together the controls the core statement places with the customer, and records no departure from it.

Core clause	Customer responsibility	IRIS retains
7.6	Granting IRIS access when it is needed, for a specific purpose.	IRIS holds no standing access to the customer's environment. Access is by the customer's invitation and is logged.
8.2	Setting and enforcing password policy, through the customer's own environment and its own staff policies.	The software authenticates against the customer's environment. Multi-factor authentication is provided by that environment rather than by the product.
8.3	Role assignments for the customer's own users within the product. This applies under every deployment model.	IRIS provides the role model and the audit trail described at clause 7.5.
9.4	Configuring encryption of data held on customer infrastructure, and protecting account files exported locally in PDF or iXBRL format, which the product does not encrypt.	IRIS provides the encryption options available in the software.
10.2	Physical and environmental security of the servers on which the software runs.	No infrastructure controls under this deployment.
11.5	Patching the operating system and infrastructure on which the software runs.	IRIS patches the software itself.
13.4	Retention and protection of the audit logs the software writes to the customer's own servers.	IRIS provides the audit records described at clause 7.5.
14.5	Backup, restore testing and verification of data held on customer infrastructure.	IRIS's obligations are limited to the availability and recoverability of the software itself.
23.4	Removal of the software and any data held on customer infrastructure at exit.	IRIS deletes data held in IRIS-operated services under clause 23.2.

Product-specific position

Core clause	Product position
8.1	Access is controlled by role through the Master User account. The software authenticates against the customer's own environment, and multi-factor authentication is provided by that environment rather than by the product.

IRIS Cascade

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	Verification. AI: chatbot component. Payments (BACS and Faster Payments). Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom. Sub-processor locations are stated in Appendix 1 or Rackspace, United Kingdom. Sub-processor locations are stated in Appendix 1
Certifications	• ISO9001; • ISO27001; • Cyber Essentials (HR API Only) • HMRC Approved Software Vendor • G-Cloud framework
Personal data and data subjects	Human resources and payroll records for the customer's workforce
Data retention and basis	Customer-controlled, retained until deleted by a customer administrator. Thirty days are allowed to extract data following termination Article 9 and 10, yes – some values stored via built-in-fields, others via user-defined fields
Recovery objectives	Recovery point objective 4 hours. Recovery time objective 72 hours.
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1, 8.2	The product password policy applies to users authenticating with a username and password. Customers may instead, or additionally, authenticate against their own identity provider, in which case password policy and multi-factor authentication are controlled by that provider. Modern authentication is supported using OpenID Connect and OAuth 2.0.
9.3	Encryption keys are dedicated to the IRIS platform and are managed within the hosting environment.
15.1	Automated security testing is performed weekly. Independent penetration testing is performed annually

IRIS Payroll Services

Field	Entry
Deployment model	A - IRIS-hosted software as a service D - managed service operated by IRIS personnel
Overlays	Managed service. Payments (BACS and Faster Payments). Verification. AI. Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom. The service is delivered on the Staffology Payroll platform. Sub-processor locations are stated in Appendix 1

Certifications	• ISO9001;
	• ISO27001;
	• Cyber Essentials
	• HMRC Approved Software Vendor via
	  ○ Staffollogy Payroll
	  ○ IRIS Payrite
	  ○ IRIS Payroll Professional
	• SOC 1 Type 1
	• CIPP Payroll Assurance Scheme (PAS)
	• BACS Approved Bureau

Personal data and data subjects	Payroll data. Data subjects: employees, trainees and next of kin. Article 9: yes, trade union membership through deductions. Article 10: yes, court order fines processed through payroll
Data retention and basis	Current Tax Year + Prior Tax Years for HMRC and Six years for The Pension Regulator and Financial Crime. Verification connector: rolling 15 months
Recovery objectives	Recovery point objective 4 hours. Recovery time objective 72 hours.
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Single Sign-On (SSO) can be configured via IRIS Identity (OKTA) Where IRIS Payroll Services is run via the Employer Portal (Staffology Payroll), Multi-factor Authentication (MFA) is mandated for all users.
8.3	Customers are responsible for informing IRIS Payroll Services of any changes to User Access or Permissions in a timely manner.
9.1, 9.2	Data at rest is encrypted using AES-256. Data in transit is protected using TLS 1.2.
15.1	Automated security testing is performed weekly. Independent penetration testing is performed annually

IRIS Paycheck Plus

Field	Entry
Deployment model	A - IRIS-hosted software as a service D - managed service operated by IRIS personnel, delivered from Ireland
Overlays	Managed service. Payments (BACS and Faster Payments). Offshore support: India
Hosting, region and data location	Microsoft Azure, Republic of Ireland (ROI) data centres. This is the only in-scope service whose primary data location is outside the United Kingdom. Paycheck Plus Engage is a third-party platform supplied by Payzaar and located in the EEA

Certifications	• ISO9001;
	• ISO27001;
	• ISAE3402
	• HMRC Approved Software Vendor via
	  ○ Staffology Payroll
	  ○ IRIS Payroll Professional
	• BACS Approved Bureau

Personal data and data subjects	Payroll data. Data subjects: employees, trainees and next of kin. Article 9: yes, trade union membership through deductions. Article 10: yes, court order fines processed through payroll
Data retention and basis	Nine years to support HMRC and Revenue Commissioners audit, extended to up to ten years where anti-money laundering obligations apply
Recovery objectives	Recovery point objective and Recovery time objective are both 24 hours.
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Single sign-on and multi-factor authentication are available for external users of Paycheck Plus Engage on request. Two-factor authentication is applied to the online payslip portal.
8.3	Customers are responsible for informing IRIS Paycheck Plus of any changes to User Access or Permissions in a timely manner.

IRIS FMP International

Field	Entry
Deployment model	A - IRIS-hosted software as a service D - managed service operated by IRIS personnel
Overlays	Managed service. Payments (international funds transfer). Offshore support: India
Hosting, region and data location	United Kingdom data centres operated by 6degrees hold personal data, including the file transfer service. Microsoft Azure platform services in Ireland and the Netherlands support the online platform
Certifications	• ISO9001; • ISO27001; The hosting partner holds SOC Type I and Type II, ISO/IEC 27001, CREST and Cyber Essentials Plus. These are inherited controls under clause 5.5, not IRIS certifications
Personal data and data subjects	International payroll data. Data subjects: employees. Article 9: yes, trade union membership through deductions. Article 10: yes, court order fines processed through payroll
Data retention and basis	No more than six years, driven by anti-money laundering obligations
Recovery objectives	Recovery point objective and Recovery time objective are both 24 hours.
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Single sign-on and multi-factor authentication are available for external users of IRIS FMP International via Engage on request. Two-factor authentication is applied to the online payslip portal.
8.3	Customers are responsible for informing IRIS FMP International of any changes to User Access or Permissions in a timely manner.
11.3	Uploaded files are scanned for malware at ingestion.
13.2	A 24x7 managed detection and response service operates over the file transfer service and the network.

Troncmasters by IRIS

Field	Entry
Deployment model	A - IRIS-hosted software as a service D - managed service operated by IRIS personnel
Overlays	Managed service. Offshore support: India
Hosting, region and data location	Live data is held at an IRIS-operated facility in the United Kingdom, with backups replicated offsite within the United Kingdom
Certifications	• ISO9001; • ISO27001;
Personal data and data subjects	Tronc and payroll data. Data subjects: employees and trainees. Article 9: yes, health data through MATB1 certificates and fit notes
Data retention and basis	No more than seven years to support HMRC and Pensions Regulator audit, extended to up to ten years where anti-money laundering obligations apply
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.3	Customers are responsible for informing IRIS Troncmasters by IRIS of any changes to User Access or Permissions in a timely manner.
9.1	Offsite backups are encrypted using AES-128.
10.1	Live data is held at an IRIS-operated facility in the United Kingdom rather than at a third-party data centre.
14.1	Core systems are replicated offsite in real time.

IRIS Payroll Professional

Field	Entry
Deployment model	C - customer-hosted, IRIS-hosted, or hosted by a third party at the customer's choice
Overlays	Verification. Offshore support: India
Hosting, region and data location	The customer's own infrastructure, the IRIS hosting service, or a third-party host. The employee portal is hosted on Rackspace, United Kingdom. The verification connector is hosted on Microsoft Azure, United Kingdom
Certifications	• ISO9001; • ISO27001; • HMRC Approved Software Vendor
Personal data and data subjects	Payroll data for the customer's workforce. Article 9: no
Data retention and basis	Six years plus the current tax year, then automatically purged
Recovery objectives	Development and support services are recovered as quickly as practicable and in any event within 24 hours. Full business operations are recovered within 7 days
Annex date last confirmed	1 September 2026

Customer responsibilities where the software runs on customer infrastructure

This table applies where the customer has taken the on-premise deployment under Model B or C. It brings together the controls the core statement places with the customer, and records no departure from it.

Core clause	Customer responsibility	IRIS retains
7.6	Granting IRIS access when it is needed, for a specific purpose.	IRIS holds no standing access to the customer's environment. Access is by the customer's invitation and is logged.
8.3	Role assignments for the customer's own users within the product. This applies under every deployment model.	IRIS provides the role model and the audit trail described at clause 7.5.
9.4	Configuring encryption at rest of payroll data files held on customer or third-party infrastructure.	AES-256 is applied to data at rest in the IRIS-operated employee portal.
10.2	Physical and environmental security of the servers on which the software runs.	No infrastructure controls under this deployment.
11.5	Patching the operating system and infrastructure on which the software runs.	IRIS patches the software itself.
13.4	Retention and protection of the audit logs the software writes to the customer's own servers.	IRIS provides the audit records described at clause 7.5.
14.5	Backup, restore testing and verification of payroll data files held on customer infrastructure.	IRIS's obligations are limited to the availability and recoverability of the software itself, and to the recovery objectives stated in this Annex for IRIS-operated components.
23.4	Removal of the software and any data held on customer infrastructure at exit.	IRIS deletes data held in IRIS-operated services under clause 23.2. Payroll data files are automatically purged after six years plus the current tax year.

Product-specific position

Core clause	Product position
7.3	Customers manage authentication and authorization via internal Windows credentials

IRIS Payrite

Field	Entry
Deployment model	C - customer-hosted, IRIS-hosted, or hosted by a third party at the customer's choice
Overlays	Verification. Offshore support: India
Hosting, region and data location	The customer's own infrastructure, the IRIS hosting service, or a third-party host. The myIRIS and employee portals are hosted on Rackspace, United Kingdom. The verification connector is hosted on Microsoft Azure, United Kingdom
Certifications	• ISO 9001; • ISO27001; • HMRC Approved Software Vendor
Personal data and data subjects	Payroll data for the customer's workforce. Article 9: no
Data retention and basis	Desktop payroll data files: retained until deleted by an administrator. myIRIS portal: deleted after 15 months of inactivity; licence expires after 3 months without uploads; leaver access 90 days. Employee portal: at least 12 months, leavers 15 months then anonymised. Verification connector: rolling 15 months. Managed file transfer: up to 30 days. SFTP: 4 days
Recovery objectives	Not established for this product
Annex date last confirmed	1 September 2026

Customer responsibilities where the software runs on customer infrastructure

This table applies where the customer has taken the on-premise deployment under Model B or C. It brings together the controls the core statement places with the customer, and records no departure from it.

Core clause	Customer responsibility	IRIS retains
7.6	Granting IRIS access when it is needed, for a specific purpose.	IRIS holds no standing access to the customer's environment. Access is by the customer's invitation and is logged.
8.3	Role assignments for the customer's own users within the product. This applies under every deployment model.	IRIS provides the role model and the audit trail described at clause 7.5.
9.4	Configuring encryption at rest of desktop payroll data files held on customer or third-party infrastructure.	AES-256 is applied to data at rest in the IRIS-operated myIRIS and employee portals.
10.2	Physical and environmental security of the servers on which the software runs.	No infrastructure controls under this deployment.
11.5	Patching the operating system and infrastructure on which the software runs.	IRIS patches the software itself.
13.4	Retention and protection of the audit logs the software writes to the customer's own servers.	IRIS provides the audit records described at clause 7.5.
14.5	Backup, restore testing and verification of desktop payroll data files held on customer infrastructure.	IRIS's obligations are limited to the availability and recoverability of the software itself.
23.4	Deleting desktop payroll data files, which are retained until an administrator deletes them, and removing the software at exit.	IRIS deletes data held in the IRIS-operated portals and the verification connector under the periods stated in this Annex.

Product-specific position

Core clause	Product position
23.1	Desktop payroll data files are retained until deleted by an administrator, so that the customer controls its own statutory retention period.

IRIS My ePay Window

Field	Entry
Deployment model	A - IRIS-hosted employee portal. The feeder payroll software may sit on customer, IRIS or third-party infrastructure
Overlays	AI. Offshore support: India
Hosting, region and data location	Rackspace, United Kingdom
Certifications	• ISO 9001; • ISO27001; • Cyber Essentials
Personal data and data subjects	Payslips, P60s, P11Ds, P45s and CIS statements. Data subjects: employees and contractors
Data retention and basis	Payslips and statutory documents at least 12 months and for the duration of processing. Auto-enrolment letters 12 months. Uploaded documents at least 3 months
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Multi-factor Authentication (MFA) can be an elective option for an individual User via IRIS Identity (OKTA) and can be mandated at Customer or Client level.
15.1	Automated security testing is performed weekly.

IRIS Employee Verification Connector

Field	Entry
Deployment model	A - IRIS-hosted service
Overlays	Verification. Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom, with client authentication and routing via Apigee using OAuth 2.0 client credentials
Certifications	• ISO 9001; • ISO27001;
Personal data and data subjects	Employment and income data, transmitted to authorised verification partners at the employee's request. Data subjects: employees and contractors
Data retention and basis	Employee records not updated for at least 15 months, or with a leave date more than 15 months ago, are automatically deleted. Audit records may be held for up to six years where a regulated decision was supported
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
7.4	Development personnel do not have routine access to customer data.
15.1	Vulnerability scanning is performed weekly.

IRIS Recruitment

Field	Entry
Deployment model	A - IRIS-hosted applicant tracking system
Overlays	AI support agent and automated decision-making in the application process, with a route to human intervention under clause 18.5. Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom Sub-processor locations are stated in Appendix 1
Certifications	• ISO 9001; • ISO27001; • Cyber Essentials • G-Cloud framework
Personal data and data subjects	Candidate and employee recruitment records. Client-defined and may include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life and sexual orientation where the client configures it. Article 9: yes
Data retention and basis	Client-configurable per data type, default 24 months. Employee human resources records are retained six years after termination
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1, 8.2	Single sign-on and multi-factor authentication are available. The default password minimum is eight characters
9.1	Encryption of candidate data at rest using AES256
14.1	Database backups are taken weekly and retained for 4 weeks. Annual DR testing
15.1	Automated security testing is performed monthly and independent penetration testing annually.

Staffology HR

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	AI. Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom
Certifications	• ISO 9001; • ISO27001; • Cyber Essentials • G-Cloud framework
Personal data and data subjects	Employee records including name, address, contact details, date of birth, racial or ethnic origin, gender, political opinions, religious beliefs and health data. Data subjects: employees, students, volunteers and next of kin. These categories are not exhaustive because the product is highly configurable. Article 9: yes
Data retention and basis	As agreed in the contract. Data is deleted or returned at the end of the provision of services
Recovery objectives	Internal RPO is 1 hour, RTO is 48 hours
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1	Single sign-on (SSO) is available for internal and external users. Multi-factor Authentication (MFA) can be an elective option for an individual Users via IRIS Identity (OKTA) and can be mandated at Customer or Company level.
13.1, 13.3, 14.1	For the SQL Managed Instance : PITR : 35 Days, Weekly LTR : 4 Weeks For SQL Databases : PITR : 35 Days, Diff. backup frequency : 24 Hours, Weekly LTR : 4 Weeks
15.1	Automated security testing is performed weekly. Independent penetration testing is performed annually.

IRIS KashFlow

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	Payments (seven invoice processors, a subscription payment provider and open banking). Offshore support: India
Hosting, region and data location	Microsoft Azure, United Kingdom
Certifications	• ISO 9001; • ISO27001;
Personal data and data subjects	Accounting records, client and supplier contact data, payment data, and user information. Article 9 or 10: no
Data retention and basis	Customer-controlled. IRIS reserves the right to delete expired account data more than two years old
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Items to remediate before publication

Core clause	Current position
8.2	The application password minimum is eight characters, 1 upper case, 1 number, 1 special character.
8.1	The second authentication factor is a memorable word, which is a second knowledge factor rather than a true second factor.
13.3	Logs are retained for 15 days in the primary monitoring system. Any captured metrics are retained for 15 months.

IRIS OpenSpace

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	Payments (customer bills and fees, and the purchase of storage and document signing credits)
Hosting, region and data location	Microsoft Azure, United Kingdom and Western Europe
Certifications	None claimed for this product.
Personal data and data subjects	Documents exchanged between an accountancy practice and its clients, and the contact data required to route them. Document contents are customer-controlled and may contain special category data
Data retention and basis	Customer-controlled. Backups are held on a rolling 35-day cycle
Recovery objectives	Not established for this service
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1, 8.2	Multi-factor authentication is enabled by an accountant administrator and is then enforced for all users linked to that account. The password minimum is eight characters.
19.2	Electronic document approval and signature is provided by GlobalSign. Payment processing is provided by Stripe.

IRIS Firm Management

Field	Entry
Deployment model	A - IRIS-hosted software as a service
Overlays	Payments (customer bills and fees, and the purchase of storage and document signing credits)
Hosting, region and data location	Microsoft Azure, United Kingdom, USA
Certifications	• SOC 2
Personal data and data subjects	Documents exchanged between an accountancy practice and its clients, and the contact data required to route them. Document contents are customer-controlled and may contain special category data
Data retention and basis	Customer-controlled. Backups are held on a rolling 35-day cycle
Recovery objectives	Platform RTO 72h, RPO 1 hour (SQL ~5–10 min).
Annex date last confirmed	1 September 2026

Product-specific position

Core clause	Product position
8.1, 8.2	Multi-factor authentication is enabled by an accountant administrator and is then enforced for all users linked to that account.
19.2	Electronic document approval and signature is provided by GlobalSign. Payment processing is provided by Stripe.