



IRIS BioStore Information Security Assurance Statement

Document control

Version number: 1.0

Owner: Mand Beckett

Date of last update: 30/01/2024

Document type: Information Security Assurance Statement

Replaces:

Approved by: Claire Treadwell

Approval date: 14/02/2024

Data protection impact screening: 14/02/2024

Date of next formal review: 14/02/2025

Contents

Information security assurance statement.....	2
Objective of this document	2
Description of the data processing carried out by IRIS BioStore	2
IRIS BioStore Organisational Security	3
Statement of Assurance.....	3
IRIS BioStore human resource security.....	6
IRIS BioStore Access Control	6
Encryption (cryptology)	7
IRIS BioStore physical and environmental security	7
Operations security.....	7
Communications security	8
System acquisition, development and maintenance.....	8
Security in development and support processes.....	9
Test data	9
Processing locations and international data transfers	9
Supplier relationships	9
Summary of sub-processors	10
Information security incident management.....	11
Compliance	12
Data Protection – quick reference.....	13

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS BioStore by IRIS with transparency as to the security and personal data compliance of this product from all threats, whether internal or external, deliberate, or accidental. This document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS BioStore as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS BioStore

IRIS BioStore provides a range of solutions linking via IDManager.

- FasTrak CASHLESS Solution on Premises
- FasTrak Cashless solution Cloud Hosted
- IRIS BioStore Portal Cloud Platform
- Print Copy Solution Third Party
- IDRegistration
- IDAccess Third Party
- Visitor Solution Third Party
- Password Manager
- ID Logon On
- Library Solution Third Party

IRIS School Data Extractor

Most modern Management Information Systems provide a simple way for organisations to share data with third parties, such as IRIS BioStore. In most cases, IRIS School Data Extractor can be set up without any installation of software within the organisation.

IRIS School Data Extractor is used to export data from the organisation Management Information System (MIS), which is imported to IRIS BioStore products.

How IRIS School Data Extractor is set up depends on the MIS used by the organisation. The data controller (organisation) needs to set the permissions required for IRIS BioStore to extract the data.

IRIS BioStore integrates with all leading providers:

- Capita SIMS
- Advanced Progresso
- RM Integris
- Bromcom
- Scholar Pack
- and others

Where IRIS BioStore does not have direct integration, we use Wonde, a third-party data supplier. We are an accredited technical partner of Capita SIMS and have similar arrangements with other providers. Organisations have complete control and can terminate the automatic data sharing at any time. IRIS School Data Extractor software requires minimal IT administration but if help is required, a dedicated team of support staff are available to assist.

- All data is hosted in UK data centres.
- IRIS BioStore processes information related to students, including some personally identifiable information (PII):

Student information	
Surname	Admission number
Forename	Ethnicity
Date of Birth	Gender
Email	Religion
Address	Telephone numbers
Class, Year group, Registration group, School House group	School photograph records
Preferred communication language	Attendance records
Free school meal allowance	

- IRIS BioStore processes personally identifiable information related to establishment/organisation staff, including:

Employee information	
Surname	MIS ID
Forename	Job Title
Date of Birth	Gender
Mobile, home and work phone numbers	Email addresses
School Record, photograph records	Association with class, lesson, year, registration, or house groups

IRIS BioStore Organisational Security

Statement of Assurance

IRIS BioStore will ensure that:

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

IRIS ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, password-authentication, communication,

and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

Organisational security at IRIS Group level

Data protection and information security at IRIS Software Group is controlled by the *IRIS Privacy, Security and Compliance Steering Group*. This group meets at least quarterly and includes:

- Members of the Executive Committee
- The Chief Information Security Officer (CISO)
- IRIS Group IT Director
- IRIS Group Data Protection Officer
- IRIS Group Compliance Manager
- Other key security leads within the company

The Privacy, Security and Compliance Steering Group 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:

- [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.
- [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.
- [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.

Organisational security for IRIS BioStore

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

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

- IRIS BioStore Senior Product Manager – Mand Beckett
- IRIS BioStore Product Manager – Bev Thompson
- IRIS BioStore Product Owner – Adam Ferrol
- IRIS BioStore Development Manager – David Waugh
- IRIS BioStore Support Services – Tracey O'Brien

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

Measures are “appropriate” if they have been identified through risk assessment.

Date of last BioStore risk assessment review: 01/02/24

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

The IRIS Group Data Protection officer is responsible for providing advice and guidance to the IRIS BioStore 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.

Development Operations and the IRIS BioStore Product Owner are responsible for the operation and integrity of IRIS BioStore on premises solution, cloud hosted solution for Cashless, and for keeping systems reasonably up to date.

FasTrak Cloud Hosted Cashless Portal Development systems are managed by an Internal Development Operations team and the IRIS BioStore Product Owner.

Asset register: DevOps Director records and maintains a register of all assets, relevant to IRIS BioStore (including acquired software licences) in a fixed assets system.

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

IRIS BioStore human resource security

IRIS BioStore staff will have access to your data, where this is required for them to carry out their role.

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

- All staff are required to complete mandatory training regularly (at least once every 12 months) regarding data security, 3rd party access, phishing and social engineering attacks. Corporate policies and training are delivered using a system called KnowBe4 and completion is expected within 14 days of the material being made available. Adherence to this policy is monitored and controlled in employee 1:1's and performance reviews.
- All staff are required to follow the internal Incident Management process should a data breach occur, with full investigation and follow up carried out by an internal Incident Management team:
 - All of our employees have completed training around data protection and how to identify a data breach along with the responsibility to report any breach to our data protection officer.
 - If the data breach involves any schools data, we will inform the signatory (or suitably senior official at the school) of the data breach within 8 hours.
 - If the breach is reportable under GDPR, it will be reported by our data protection officer (via our data protection management tool) to the ICO within 72 hours.

Termination and change of employment

- 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.
 - Immediate removal of access to Office applications, including email, Teams and OneDrive
 - In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

IRIS BioStore Access Control

For each solution, the establishment/organisation back-office user's log in to each product interface using a separate application specific login. We recommend to our customers a password consisting of a minimum of 8 Characters, made up of a mix of upper and lower case and special characters.

Within each solution IRIS BioStore can allow privileged users by updating the permissions set within the application software. The details of who and what data can be accessed by a privileged user is accessible to the customer within the help files stored in the application software.

For systems hosted on premises, the customer has control of these access rights and can modify them without IRIS BioStore support.

For cloud hosted FasTrak, the customer can request from the IRIS BioStore support, credentials to allow them to amend access themselves. An audit trail is kept in the support ticketing system in Service Cloud.

Authentication is managed using a leading authentication platform, Okta, which has rules and controls set for minimum password strength, management and suspicious activity. New users are sent an email which requires them to set their password before being able to access the product.

IRIS Staff Access Control

The IRIS BioStore team use Service Cloud, a support ticketing system, Salesforce, our Customer Relationship Management System, and Office 365. All systems require password authentication for access. Access is only granted to employees of IRIS BioStore with legitimate need.

If an employee leaves, their access to the systems is revoked by central IT.

All IRIS BioStore source code is restricted using source control, which provides a full audit trail of changes.

For the avoidance of doubt, IRIS BioStore ensures to customers that it will not seek to circumvent, compromise or change the customer's security controls, and IRIS BioStore will not change the customer's software configurations (without proper authorisation), and no 'primary' password or other method of remote access into [product/service name]'s software shall exist.

Multi-factor authentication is required for those with administration privileges within the Okta platform.

Encryption (cryptology)

All data is currently 256bit Advanced Encryption Standard (AES) encrypted.

IRIS BioStore physical and environmental security

IRIS BioStore has a version of the FasTrak Cashless solution, which is hosted by Iris using RACKSPACE Cloud, a cloud-based secure storage facility which is restricted by biometric authentication and 24x7x365 surveillance.

For all other solutions, the data is stored on the establishment/organisation premises and they control the access to data.

IRIS School Data Extractor stores data securely within Amazon Web Services (AWS).

Operations security

For each solution, the establishment/organisation back-office user's log in to each product interface using a separate application specific login.

We recommend to our customers a password consisting of a minimum of 8 Characters, made up of a mix of upper and lower case and special characters.

Within each solution IRIS BioStore can allow privileged users by updating the permissions set within the application software. The details of who and what data can be accessed by a privileged user is accessible to the customer within the help files stored in the application software. For systems hosted on premises, the customer has control of these access rights and can modify them without IRIS BioStore support. For cloud hosted FasTrak, the customer can request from the IRIS BioStore support, credentials to allow them to amend access themselves. An audit trail is kept in the support ticketing system in Service Cloud.

The IRIS BioStore team use Service Cloud, a support ticketing system, Salesforce, our Customer Relationship Management System, and Office 365. All systems require password authentication for access. Access is only granted to employees of IRIS BioStore with legitimate need.

If an employee leaves, their access to the systems is revoked by central IT.

All IRIS BioStore source code is restricted using source control, which provides a full audit trail of changes.

For the avoidance of doubt, IRIS BioStore ensures to customers that it will not seek to circumvent, compromise or change the customer's security controls, and IRIS BioStore will not change the customer's software configurations (without proper authorisation), and no 'primary' password or other method of remote access into [product/service name]'s software shall exist.

Change Management processes are in place to review and approve any changes made to products, environment and infrastructure.

Capacity is monitored automatically and any notable changes highlighted and reviewed.

Development is carried out on separate environments, for engineers, testing and then being deployed to production environments.

IRIS BioStore uses tools to detect malicious software and all connections to machines containing PII are only authorised from the corporate VPN. This VPN requires an email, password and MFA to access. Firewalls and firewall rules are in place and access is logged and actively monitored.

Communications security

All IRIS BioStore data servers are located behind a VPN, firewall and access control. Users are limited to read-only access where possible. Where higher access levels are required this is granted table-by-table. Each customer has it's own unique identifier and has it's own set of tables based on that identifier. The system is designed to only allow users from that customer's organisation access to their own tables, hence only their own data.

IRIS BioStore has a policy in place for the acceptable use of email, instant messaging and other electronic communications. No PII is permitted to be shared via email and can only be shared using our customer case management platform.

All 3rd party suppliers, vendors and contractors have confidentiality or non-disclosure agreements in place which are reviewed, documented and reflect the product/service's needs for the protection of information.

System acquisition, development and maintenance

All new information systems, features and suppliers go through a thorough review process. This includes, but is not limited to:

- System architects
- Security specialists
- Engineers
- Product Managers and Owners
- Support, on-boarding and professional services teams

Security in development and support processes

Security is foremost in all phases of software development and documented in a secure development policy. Solution designs are reviewed by Architects and security specialists and automatic code and vulnerability scanning is in place.

All system changes are controlled by the use of formal change control procedures, meeting weekly to review and discuss planned changes. Where changes are needed urgently a shorter, more succinct process is in place and procedures are in place to review where a high occurrence of urgent changes are requested for a particular product.

Application systems are automatically tested after changes to the operating system.

Once changes are released both automated and manual testing is completed to validate the change being made and to ensure that other negative changes have not been introduced.

Test data

IRIS BioStore uses test data which is generated randomly and is not associated with any customer or data subject. Where staff need to use real contact information for testing access to this is limited and regularly reviewed.

Processing locations and international data transfers

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & 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.

Supplier relationships

Information security in supplier relationships

All new suppliers and contractors complete an in-depth new supplier security Due Diligence document, which is reviewed by the IRIS IT Security Team to ensure our strict compliance procedures are met. The Due Diligence document covers the following:

- Information Security Policy
- Integration with IRIS BioStore software
- Access Controls
- Training
- Education and Training
- Asset and Inventory Management
- Environment and Network
- Data Information and Security

Supplier service delivery management

Quarterly meetings are held with all suppliers where the agenda is:

- Current Service Levels
- New ideas for Product
- Current functionality of product

All new product requests and services have a process to be signed off by the IRIS BioStore Chief Financial Officer and Senior Product Director.

Summary of sub-processors

- Universal Smart Card (card printing services)
- Osborne Technologies Ltd (Visitor System)
- GroupCall (SMS Data extraction for use with partners where full integration is not in place)
- Payment Sense (Card Payments - for use alongside Cashless)
- Wonde (data extraction)
- iSAMS (MIS)
- Digital ID (Card Printing)
- Rackspace (cloud storage)
- AWS (cloud hosting for management of websites and apps)
- Okta (secure identity management)
- ServiceCloud (support ticketing system)
- Salesforce (Customer record management (CRM))
- IRIS ParentMail (Online payments)
- Gainsight (in-product help and analytics)
- Cybage

Information security incident management

Management of information security incidents and improvements

- All staff are required to follow the internal Incident Management process should a data breach occur, with full investigation and follow up carried out by an internal Incident Management team:
 - All of our employees have completed training around data protection and how to identify a data breach along with the responsibility to report any breach to our data protection officer.
 - If the data breach involves any schools data, we will inform the signatory (or suitably senior official at the school) of the data breach within 8 hours.
 - If the breach is reportable under GDPR, it will be reported by our data protection officer (via our data protection management tool) to the ICO within 72 hours.

All staff are required to follow the IRIS Group Incident Reporting Procedure to report security incidents to their department lead as quickly as possible and to raise a major incident via Teams, email or phone to the central Incident Management Team.

Information security problems and issues are reviewed regularly in team meetings and a joint decision made on whether to classify them as information security incidents that need to be reported through the corporate procedure.

Reports of breaches or suspected breaches are raised to our support team, usergroup or by email and these are prioritised and investigated immediately. Investigation can be carried out by support sessions, reviews of user and access logs and data comparison. If a breach is found to have taken place the documented incident process is followed and assistance requested from the Data Protection Office.

All critical incidents have a root cause analysis completed once the incident is closed and mitigating or supporting work identified and monitored by the Incident Management Team.

Compliance

Compliance with legal and contractual requirements

Identification of legislation and contractual requirements applicable to IRIS BioStore – IRIS is committed to providing high-quality, secure and compliant products. We comply to all relevant legislative and contractual requirements including GDPR and industry certifications such as Cyber Essentials and ISO certification. IRIS uses relevant software to help us maintain records related to this and to ensure that reviews are conducted regularly and by the relevant staff levels.

Important records of the organisation are protected from loss, destruction, falsification unauthorised access and unauthorised release.

Privacy and protection of personally identifiable information – IRIS' Privacy Policy is documented and published on our website here: <https://www.iris.co.uk/privacy-policy/>

Information security reviews

Independent review of information security – IRIS Privacy and Data Protection policies, processes, procedures, controls and control objectives are subject to regular independent reviews at planned intervals or when significant changes occur.

Technical security reviews are carried out using manual and automated tools to confirm information security objectives are achieved – this is achieved by regular PEN testing, vulnerability scanning, pipeline scanning and manual reviews of solution design and code.

Data Protection – quick reference

IRIS Group Data Protection Officer - Vincenzo Ardilio - dataprotection@iris.co.uk

Data protection owner for IRIS BioStore – Adam Ferrol – adam.ferrol@iris.co.uk

We will make your personal information available within the IRIS Software Group on a need-to know basis in order to achieve our legitimate business objectives. If we have sub-contracted any aspect of the product or services you are using, we may need to share your details with the relevant supplier, also on a need to know basis.

Location of personal data processing, hosting and access by IRIS agents

Customer personal data will be processed or stored in the EU.

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & 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.

Retention of data

IRIS BioStore is committed to the protection of data held whilst customers are accessing the system.

- If a customer cancels their agreement, their school setup is deleted from the **IRIS BioStore** system, meaning that all personal pupil and staff data is removed. The school is asked to remove all related software from their school systems.
- No paper copies of pupil or staff data are held at any time by **IRIS BioStore**. Access is solely via our secure systems for the purposes of guaranteeing Project Partners' full and comprehensive use of the system and to realise our aim of effective, first class customer service.

Data subject rights

- We are fully committed to support schools with any rights of access requests they have. This may come from a parent, student or member of staff at the school. We will respond to requests without undue delay and within one month of receipt.
- There are specific audit trails in the system to allow the user to export historical contact data from the system.
- We can export and share data, with written consent, in common formats like Excel and Word.