ISAMS | INFORMATION SECURITY ASSURANCE STATEMENT

Document control	
Version number:	1.2
Owner:	Nicholas Clark – Product Manager
Date of last update:	20-02-2024
Document type:	Customer Assurance Statement
Replaces:	All previous
Approved by:	Claire Treadwell – Product Director
Approval date:	20-02-2024
Data protection impact screening: N/A	
Date of next formal review:	20-02-2025

TABLE OF CONTENTS

INFORMATION SECURITY ASSURANCE STATEMENT

OBJECTIVE OF THIS DOCUMENT

The purpose of this information security assurance statement is to provide customers of ISAMS 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 ISAMS as a thoroughly secure software and service provider.

DESCRIPTION OF THE DATA PROCESSING CARRIED OUT BY ISAMS

ISAMS is a Management Information System (MIS) or Student Information System (SIS). It brings together information about students and contacts as well as staff to allow the running of educational institutions. This includes assessment, attendance of staff and students, contact detail and the provision of medical data capture. Schools, groups and trusts may also add custom fields to collect any data.

- All data is hosted in UK data centres
- ISAMS holds data about Students, Staff and Teachers, Parents and other contacts
- This data is sensitive and classified as able to identify the above mentioned subjects personally (PII)

- Documents are also stored in the system, attached to Student, Contact or Staff records
- Student data consists of basic detail, medical and assessment data as well as passport, visa and financial information, photographs of the student for identification as well as safeguarding information and special needs data
- Contact data consists of basic detail plus contact history, financial payments history
- Staff detail consists of basic details, pay and contract information, bank details and details of their qualifications and contract

ISAMS Organisational Security

STATEMENT OF ASSURANCE

ISAMS 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.

The iSAMS platform and all associated modules and additions are developed sold exclusively by iSAMS (IRIS Software) in all markets that we operate in across the globe. Further, it is supported by iSAMS exclusively in all markets, all training is carried out by IRIS employees or consultants and all installation, project management and technical work is also carried out by our employees. Partners and third parties are able to develop against our API, but need approval both from iSAMS and the school as written agreements as well as a software key.

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 Officer (CIO)
- 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.

- 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.

ORGANISATIONAL SECURITY FOR ISAMS

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

- ISAMS Senior Product Manager – Nicholas Clark
- ISAMS Product Owners – Anna Robinson, Steven Israel
- ISAMS Development Manager – Andrew Williams
- ISAMS Support Services – Tracey O'Brien

The ISAMS 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 ISAMS.

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

Date of last ISAMS risk assessment review: December 2023

The ISAMS 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 ISAMS 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 Operations are responsible for the operation and integrity of ISAMS IT systems and for keeping systems reasonably up to date. ISAMS hosting is provided by Microsoft Azure.

ISAMS's Development systems are managed by our in house development teams.

Asset register: Engineering Manager records and maintains a register of all assets, relevant to ISAMS (including acquired software licences) in a fixed assets system.

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

ISAMS HUMAN RESOURCE SECURITY

Some ISAMS staff will have access to customer systems to help provide support, updates or other essential services.

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 undergo additional mandatory training in order to understand their responsibilities when it comes to customer data. This is updated at regular intervals and reinforced with special messaging and meetings for those who have the most access to this sensitive data.

- All IRIS employees also undertake training via our compliance portal in the more general aspects of safeguarding data.

- The standard disciplinary policy and process covers staff who are able to access customer systems.

TERMINATION AND CHANGE OF EMPLOYMENT

- A formal procedure exists for performing employment terminations or change of employment. This includes the requirement to maintain confidentiality after employment ceases. Upon instruction from HR of a person leaving ISAMS, 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.

ISAMS ACCESS CONTROL

Where our people are authorised to access customer systems, alongside the training and policy controls, many physical and technological controls exist to help manage access.

- Password complexity rules and 2FA are enforced across the estate. This means that where a member of our authorised staff accesses a customer system, there are extra 2 factor authentication rules and password complexity requirements in order to grant login. Where schools choose to turn off 2FA for certain users within their own system this account is limited in what it is able to do – for example, no data can be exported from iSAMS.

- These authorised users are assigned carefully in line with their job role and access need. The lowest level of access is given by default.

- Staff users accessing user systems are subject to extra logging. They login as a special administrative user and this is tied back to their organisational account to identify the person and a log is kept by default of everything they do within a system.

- As part of the ticket, a log of what we have done or been asked to do is kept. This becomes part of the customer history and can always be referred back to.

- Where we ask customers to make changes themselves, we will provide full support in doing so or refer them to published help guides.

- Customers are authenticated when they call, and only authorised and known people from a school can request changes are made. There are several levels of school user that can request changes, but any that do not come from the admin contact and are likely to cause changes to the system are checked first.

- Access rights are reviewed regularly for privileged users to make sure that nobody who should not have these rights keep them from longer than needed.

- Source code is not available to customers and carefully protected against any changes from outside. We do not permit customers writing any customised functionality to add the app.

- iSAMS does not use privileged utility apps for maintenance, everything is managed from our Backoffice portal and access to this is controlled as above.

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

ENCRYPTION (CRYPTOLOGY)

All data is encrypted in transit and at rest, therefore is encrypted for the entirety of the time it is within our systems and whilst being transmitted to the customer browser to at least TLS 1.2

ISAMS PHYSICAL AND ENVIRONMENTAL SECURITY

iSAMS data is hosted in Azure, Microsoft's cloud. Their security arrangements are set out at the following link:

https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

EQUIPMENT

Our hosted datacentres are provided by Microsoft Azure, their policies and procedures around equipment can be found here:

https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

While our staff are working on the iSAMS platform, they do so remotely on company computers which are secured with password protection, are locked when not in use and have policies to protect them from unauthorised use. All access to systems is logged and audited.

MEDIA HANDLING

Management of removable media – removeable media is not supported or used in the work that we do on the platform.

Disposal of media – Disposal of media is not something we do, we do not support use of removable media.

Physical media in transit – We do not allow or support the use of physical media in any format.

OPERATIONS SECURITY

DOCUMENTED OPERATING PROCEDURES

We have strict change management controls and operating procedures that are documented and templated. These changes much be approved by at least two people before testing, build or implementation

CAPACITY MNAGEMENT

We continually review capacity management plans, and can scale our capacity easily where needed. We update plans for the future regularly as the platform changes and grows. Capacity is monitored by a number of automations and can be scaled as needed as the platform requires or to react to specific situations or events such as high demand reporting periods, for example.

RELEASE MANAGEMENT

The iSAMS platform works on a continuous release basis, with rollbacks automated for recovery. Development and testing environments are split from production workloads and their networks are also separated.

VIRUS AND MALWARE PROTECTION

The iSAMS infrastructure is protected from malware by a number of controls such as defender in our Azure environment, Carbon black, CrowdStrike and antivirus and antimalware on all file uploads and storage. We perform penetration testing regularly (see section on this for detail) All network segments are firewalled from each other in line with policies and the highest industry standards.

BACKUP

We keep point in time backups of the transactional SQL databases for 30 days, allowing simple rollback of systems to a given time period. We take and maintain weekly full system backups, these are retained for 33 weeks each. These are immutable, therefore can't be amended or deleted so represent a very accurate system copy. After 33 weeks, these are automatically destroyed.

EVENT LOGGING

We log events across our infrastructure and these are monitored by automatic tooling and sent for further analysis on a proactive basis if required. Log information is protected and is external to our infrastructure.

ADMINISTRATOR AND OPERATOR LOGS

We maintain a logging audit of what is done to systems – where staff log into specific iSAMS systems this is logged fully in the audit log inside iSAMS. Where staff make changes to the database, this is logged by monitoring tools for audit where needed.

CONTROL OF OPERATIONAL SOFTWARE

IRIS computers are managed and software can only be installed on them using our admin by request tools, which allows logging and control over what is installed. Any software installation needs to be on a global supported software list which is vetted carefully.

MANAGEMENT OF TECHNICAL VULNERABILITIES

We manage technical vulnerabilities in several ways, to ensure that we are always maintaining the platform as well as we can, proactively.

We operate a number of internal scanning tools that are run by an internal team to scan the codebase and all associated systems regularly for vulnerabilities. The results are shared with the development director and prioritised in order of severity.

We regularly commission external, independent Penetration Testing (PEN Testing) of the whole iSAMS system – this is completed quarterly, more than the industry average of once per year. The results are shared internally and prioritised by the product and development teams.

We typically spend between 30 and 40% of our total development effort in keeping the platform secure and addressing new threats that have been identified either through our own testing and knowledge, or through external PEN testing. Where required, we are able to flex the number of developers where more serious vulnerabilities are identified, or where planned security work neds more input.

COMMUNICATIONS SECURITY

NETWORK CONTROLS

We implement both software and policy controls to make sure that access to networks is secure including MFA by default, no direct access to servers by RDP. We also make use of other technologies to help manage these controls.

ELECTRONIC MESSAGING

We maintain an acceptable use policy for use of email and messaging services.

CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS

Where needed, we have strict Non-Disclosure Agreements (NDAs) in place with our supplier. The protection of our IP, codebase, customer data and the security of our systems is paramount in these agreements.

HOW WE TRANSMIT CONFIDENTIAL INFORMATION TO CUSTOMERS

Where we need to send data to customers – backups, for example, they are made available via secure download secured with TLS and protected by OneTimeSecret keys locked to specific contacts that have been authorised by their organisation explicitly.

INFORMATION TRANSFER POLICIES AND PROCEDURES

Where information is transferred by document, electronic means or by phone, we have specific mandatory training and policies to make sure we are protecting our customer data.

AGREEMENTS ON INFORMATION TRANSFER

Where schools wish to use connections to transfer data to third parties, we build an agreement with them to enable the use of our API services which are secured with HTTPS and TLS 1.2 or better.

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 for both our own code and third party component. Regular penetration testing is conducted by independent CREST accredited providers.

Quality assurance starts in the earliest phases of design for every project, with developers testing changes throughout the whole agile lifecycle culminating in acceptance testing before every release. All changes are subject to a formal change control procedures with major changes going through a Change Approval Board review and an avenue for “standard changes” to allow low risk items to be released at a faster cadence.

Third party components are monitored through our Software Composition Analysis tooling providing us with an internal bill of materials and giving immediate notification of new vulnerabilities as they are discovered by the wider software development community.

TEST DATA

iSAMS testing data is generated by a custom software tool and is not associated with and identifiable subjects. On rare occasions where a change needs to be tested in a school environment, all actions are logged and the school works cooperatively with our engineering team.

PROCESSING LOCATIONS AND INTERNATIONAL DATA TRANSFERS

On occasion, IRIS may use engineers and third parties located in countries outside the UK for production environment support, deployment activities, access management and security & vulnerability management to support our international customers. In all these instances, information is held on secured network drives held in our datacenters 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

INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

We have a policy for third party security, but we do not allow external partners to access customer systems or data, it is supported by our own staff.

ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS

Where we have agreements for suppliers to access API services or provide us with a service or technology, security is an integral part of this agreement.

SUPPLIER SERVICE DELIVERY MANAGEMENT

MONITORING AND REVIEW OF SUPPLIER SERVICES

As mentioned earlier, we use tooling to monitor all aspects of the system including third party components and extensions, their security and performance.

MANAGING CHANGES TO SUPPLIER SERVICES

Suppliers sometimes require changes to the way we use, or they use, the iSAMS platform, these are carefully managed within a policy to make sure that our high standards are adhered to and customers are not adversely affected.

SUMMARY OF SUB-PROCESSORS

- Gainsight
- Microsoft
- SendGrid
- Cybage
- Clickatell
- Third party software components used in the iSAMS platform build
- If using Central:
    - 5Tran
    - Snowflake

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 join 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, 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.

BUSINESS CONTINUITY – INFORMATION SECURITY ASPECTS

Information security continuity

For hosted schools, we backup daily using Azure Backup Centre. All backups are immutable. Full backups are taken weekly and log backups taken every 30 minutes. We currently retain weekly full backups for up to 33 weeks and daily log backups for 30 days - these retention periods are subject to change. Requests for restores of data may be chargeable where data loss has not been caused by a fault in the product or service we provide.

Regular tests are undertaken to ensure that service can be restored from backups as part of the hosting providers Disaster Recovery process.

Disaster recovery, business continuity and data integrity processes are in place and reviewed regularly and monitored by DevOps, architects and security personnel.

Redundancies

The iSAMS hosted service is highly redundant. Our hosting provider, Microsoft Azure, hosts across multiple locations in the UK for our UK and European customers, and in the same way for other geographies we operate in to ensure physical redundancy. Backups are taken and processed as in the above backup statement.

We have documented business continuity processes and procedures, which are reviewed by our DevOps and architecture teams regularly.

COMPLIANCE

COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

Identification of legislation and contractual requirements applicable to iSAMS – 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.

The iSAMS platform is Penetration Tested (PEN Tested) on a **quarterly** basis by an independent third party, with results shared with product, development and management teams for immediate action.

Technical security reviews are carried out using manual and automated tools to confirm information security objectives are achieved – this is achieved by regular Penetration 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 iSAMS: Nicholas Clark – nicholas.clark@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 for UK and European customers is stored and processed within the UK.
Our infrastructure has a hub and spoke architecture, making it possible for us to leverage local datacentres in countries supported by the Microsoft Azure cloud across the globe. At present we use a

datacentre in Singapore to process data from schools in Asia. In the future, we are planning to use this in other geographies, but will consult with customers before we move any data. If you are unsure where your data is located, please ask us for help.

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

iSAMS 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 iSAMS system, meaning that all personal pupil and staff data is removed.

- The Company will retain history for a period (determined by the customer) before it is destroyed, in case of a later need on the school's part to access this information. During this period, all this data will be retained on secure back-up systems.

- No paper copies of pupil or staff data are held at any time by iSAMS. 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 allows 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.

- We support schools with their obligation under GDPR by providing a GDPR module in the iSAMS platform to manage requests.

- Where schools wish to leave the iSAMS platform, we offer them a copy of their database in a usable format with no undue conditions or restrictions as a .bak file.