IRIS OpenSpace

Information Security Assurance Statement

Document control
Version number: 2
Owner: Satinder Dhanda
Date of last update:19/04/2024
Document type: Information Security Assessment Statement
Replaces: NA
Approved by: Daniel McGrath
Approval date:19/04/2024
Data protection impact screening: No PIA Required
Date of next formal review: 01/04/2025

Contents

Information security assurance statement

Objective of this document

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

Description of the data processing carried out by IRIS OpenSpace

IRIS OpenSpace is an online client portal that facilitates the secure exchange of documents, request and issue of approvals and signatures, request and issue of data client capture, and the collection of online payments for services rendered.

The IRIS OpenSpace application is a SaaS web application, hosted with Microsoft Azure.

The storage and processing of personal data is limited to that required by IRIS OpenSpace and is sufficient for the purposes of executing it's features and capabilities.

The subjects of the information being processed is limited to the accountants, accountant staff members and their clients.

Personal data stored includes first name, last name, and email address for clients.

Personal data may be included within the files being exchanged between accountancy customers and their clients. The customer is in full control of the data shared.

Personal data we store for staff includes first name, last name, email address.

Statement of assurance

IRIS OpenSpace will ensure that:

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

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

IRIS OpenSpace Organisational Security

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 IRIS OpenSpace

At IRIS, the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering IRIS OpenSpace to ensure it 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 OpenSpace, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- Daniel McGrath – Product Director

- Satinder Dhanda – Product Owner
- Paul Isherwood – Engineering Lead
- Bryce Kane – Support Lead

The IRIS OpenSpace 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 OpenSpace.

Measures are "appropriate" if they have been identified through risk assessment.
Date of last IRIS OpenSpace risk assessment review: 31/05/2023.

The IRIS OpenSpace 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 OpenSpace team and for monitoring our compliance on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner's Office.

Group IT are responsible for the operation and integrity of IRIS OpenSpace's IT systems and for keeping systems reasonably up to date.

IRIS OpenSpace's development systems are managed by Group IT.

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

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

IRIS OpenSpace human resource security

IRIS OpenSpace staff will not have access to your client data.

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

- Corporate policies, procedures and training are administered per IRIS policy.

- A formal and communicated disciplinary process is implemented for situations where an employee may have committed a security breach. This process is owned by HR.

Termination and change of employment

Upon instruction from HR of a person leaving a role that involves IRIS OpenSpace, that person's access to confidential areas shall be restricted immediately, culminating in:

- Full removal of access to any part of the corporate network
- 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.

IRIS OpenSpace Access Control

- IRIS OpenSpace is password protected requiring a minimum of 8 characters and containing a mixture of upper- and lower-case characters, special characters, and numbers. The password rules are enforced through the software.
- Multi-factor authentication is optional and can be enabled by the customer's administrator user, and this is enforced for all users linked with that account.
- IRIS OpenSpace supports three user roles: Administrator, Staff User and Client User.
    - Administrator: These are accountancy practice staff that sign up and creates the practice account. They have the same rights as a staff user (see below) along with access to the settings area to administer users and practice details. They can also see the subscription details and issue payments to IRIS where necessary.
    - Staff user: These are a customer's staff members who can view and mange clients and send files to client users for action.
    - Client user: This is a client of the customer who can act upon requests issued by staff users. These requests may be document approval/rejection, upload requests and invoice payment requests.
    - Administrators and Staff users of the customer can access all documents that have been uploaded to the OpenSpace account.
    - Client users can only access documents uploaded to their specific area.
- All activities are recorded to an audit log that is accessible to customers. The audit shows any amendments made to documents/requests, what the amendments were, when they happened and the user who performed the change.

The IRIS Support team may from time to time use remote support tools such as LogMeIn or GoToAssist. All remote connections are recorded meaning any personal data that may be displayed on the user's device would be captured during the session. Customers have a measure of control over the use of remote support tools, customers may instruct their users not to accept remote connections from our Support team, but this would have an impact on the level of support that can be provided.

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

Encryption (cryptology)

Data and documents stored using IRIS OpenSpace are encrypted at rest using industry accepted best practices. This is currently 256-bit AES encryption.
All communications between the IRIS OpenSpace service(s) and end users are encrypted using industry accepted best practices. This is currently TLS 1.2.

All encryption methods are reviewed regularly and upgraded as technology improves.

IRIS OpenSpace physical and environmental security

IRIS does not maintain physical servers or other infrastructure for IRIS OpenSpace. All infrastructure is hosted by Microsoft Azure, and as such, IRIS OpenSpace inherits the physical and environmental controls implemented by Amazon. Details may be found on the Microsoft website: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Access to IRIS resources and equipment is subject to Group IT Policies.

Operations security

Change management

Changes are logged within JIRA and the release goes through CAB approval which includes a CAB release form which details what is in the release, reasons for the release, time of release, resources required, rollback actions.

Capacity management

We perform smoke tests on the test environment to ensure the system continues to run at optimum performance. The IRIS OpenSpace team actively seek to identify performance bottlenecks in an effort to drive down the footprint of the system. Tools such as Datadog and App Insights are used monitor production environments.

Separation of development, testing and operational environments

The IRIS OpenSpace production environment is separate to the development and testing environments, with processes in place to test and control the promotion of new code through each.

Control of operational software

Any changes to the software require CAB approval before they can be released to production.

Management of technical vulnerabilities

Tools such as Snyk, and other SAST and DAST tool sets, are used to proactively monitor IRIS OpenSpace for vulnerabilities so they can be remediated as soon as possible. Penetration testing is performed once a year by an external company and this was last performed on 31/05/2023.

Communications security

Network controls

IRIS OpenSpace is hosted on Microsoft Azure which employs pessimistic security to ensure only authorised access is allowed, from authorised locations.

Security of network services

Access is limited to IRIS employees only and the auditing is contained within Microsoft Azure.

Segregation of networks

IRIS OpenSpace is hosted on private Azure infrastructure and uses separate infrastructure for development, test, and production environments.

Transmission of confidential information to customers

No confidential information is sent between IRIS and the customer during onboarding as users register directly on the system. Training is carried out on-site or virtually and no confidential data is shared.

System acquisition, development and maintenance

Before features are developed, or changed, an Architecture Review Board reviews and approves the technical architecture being proposed. If changes are required to the technical approach, these are fed back to the teams. This process includes a full security review including, but not limited to attack surface & vector analysis and encryption requirements.

All data transfer within the OpenSpace application infrastructure is secured and encrypted using the latest industry accepted standards. Similarly, all access to the OpenSpace application across public networks is secured and encrypted using the latest industry accepted standards.

Security in development and support processes

Security is considered at all stages of development. Designs are taken (when necessary) to an Architecture Review Board which helps direct any security concerns to the Security Architect

Jira is used to document and track work. Requirements are fed into teams by Product Managers and prioritised by Product Owners. Jira tickets are worked by the teams and must meet a documented Definition of Done before they are accepted. Changes are demoed to Product Owners, Product Managers and wider stakeholders.

Testing is performed and documented throughout the development process. Automation tests are built to help ensure future changes do not impact the application.

Documented principles and procedures are stored in Confluence. Any gaps are identified during the design process and added to the documentation.

3rd party platforms such as Microsoft Azure are Risk Assessed and approved by Group IT. Development environments are secured using the standards set by Group IT. Development approaches are assessed by a Security Architect.

3rd party development resource is contractually obliged to meet IRIS standards for security and testing. IRIS retains the IP for all work performed. Work performed by 3rd party developers is processed through the same pipeline as internal developers with the same automated security checks etc.

Test procedure is documented in Master Test Plan. Individual tests and test results are documented within Jira

Test data

All test data is depersonalised/obfuscated before being used in test environments. Developers and testers do not have access to production data.

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

List of third parties and sub-processors involved in IRIS OpenSpace processing customer data correct as at 19/04/2024:

Cybage (India)
Stripe
GlobalSign
Microsoft Azure

Cybage (India) is a development partner of IRIS Software Group. Cybage employees working on IRIS OpenSpace are subject to all the same controls and data security principles as non-Cybage IRIS Software Group employees.

Stripe is used to facilitate the online payment of customers' client's bills and other fees, and to purchase online storage space and credits required for the digital signing and approval of documents.
All communication with the Stripe service(s) is encrypted, and only the minimum customer and client data required to affect a payment is transmitted to Stripe. The Stripe 'Privacy Centre' can be found at: https://stripe.com/privacy-center/legal

GlobalSign provides OpenSpace customers with the ability to allow their clients to securely and electronically approve and sign documents. All communication with the GlobalSign service(s) is encrypted, and only the minimum customer and client data required to affect an approval or signature is transmitted to GlobalSign. The GlobalSign privacy and data policies can be found at: https://www.globalsign.com/en/repository

Microsoft Azure is the sole hosting platform for OpenSpace services. Microsoft Azure privacy and compliance policies can be found here: https://docs.microsoft.com/en-us/azure/compliance/

Information security incident management

In the event of an information security incident then OpenSpace follows the IRIS Group incident management policy.
Personal data incidents are investigated by the IRIS Open Space team and in accordance with the IRIS group Incident Reporting and investigation procedure.

In the event of any critical incident that threatens or may reasonably be construed as threatening the information security of a Client or the continuity the IRIS OpenSpace service to any set of Clients, such critical incident must be immediately reported to the Critical Incident Manager and or the Information Asset Owner.

Business continuity – Information security aspects

Information security continuity

IRIS OpenSpace is not hosted at premises maintained by IRIS.

Disaster recovery, hardware fail-over and information security continuity is managed by IRIS DevOps in Microsoft Azure.

Infrastructure configurations are stored and managed by IRIS DevOps, and all code and application configuration is stored and managed within version control software.

Data Protection – quick reference

IRIS Group Data Protection Officer – Vincenzo Ardilio – dataprotection@iris.co.uk
Data protection owner for IRIS OpenSpace – Satinder Dhanda – satinder.dhanda@iris.co.uk
Categories of personal data processed as part of the product/service provision:

Categories of data subjects under the product/service provision:

- Individuals: forename, surname and email address.
- Businesses: Name and address

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

Customer data, and customer client data, in IRIS OpenSpace is stored with the UK and western Europe. Unless explicitly granted via the use of tools such as LogMeIn or GotoAssist, IRIS agents do not have access to customer or customer client data.

Retention of data

Data will be stored in IRIS OpenSpace until such time as a customer deems it no longer required or is required to remove it. Currently, customers are able to delete client data from IRIS OpenSpace.
When a customer decides to stop using OpenSpace then it is the customer's responsibility to remove their files, though they can request IRIS does this on their behalf.
The data is backed up in rolling backups for 35 days so after this point all the data will be removed permanently.

Data subject rights

All data subject access requests should be referred to our online terms and conditions and data processing terms on the IRIS website:
http://www.iris.co.uk/assets/Terms/IRIS-General-Terms-Conditions.pdf
http://www.iris.co.uk/assets/Terms/IRIS-Customer-Data-Processing-Terms.pdf