# Information Security Assurance Statement of IRIS KPO

| Document Control | | |
|---|---|---|
| Version number | : | 1.5 |
| Replaces | : | 1.4 |
| Release Date | : | November 25, 2024 |
| Document type | : | Information Security Assurance Statement |
| Prepared by | : | Data Protection Officer |
| Approved by | : | Senior Director – Operations |
| Approval date | : | November 25, 2024 |
| Date of next formal review | : | July 8, 2025 |

## Revision History

| # | Version | Date | Rational for Change | Change Description |
|---|---|---|---|---|
| 1 | 1.0 | 24th Nov 2020 | New Release | NA |
| 2 | 1.1 | 23rd Nov 2021 | Formal review | Regular updates |
| 3 | 1.2 | 15th Feb 2023 | Formal review | Updated the names and designations of newly appointed HR & ISO Department Head |
| 4 | 1.3 | 31st May 2023 | Formal review | Updated Statement of assurance, Data transmission through email, Data retention period and Disposal of data |
| 5 | 1.4 | 24th June 2024 | Formal review | Reviewed and made necessary changes to all the sections of the document for adequacy |
| 6 | 1.5 | 25th November 2024 | Interim review | New designations of the management security forum members updated in page # 7 |

# Table of Contents

# Information Security Assurance Statement

## Objective:

The Information Security Assurance Statement of IRIS KPO Resourcing (India) Private Limited (hereafter referred to as IRIS KPO) ensures transparency for customers regarding the security and personal data compliance of its services. This statement addresses all potential threats—internal or external, deliberate or accidental. Additionally, it aims to ensure legal compliance, maintain business continuity, minimize business risks, and maximize customer confidence in IRIS KPO's secure service provision.

## Description of the data processing carried out at IRIS KPO:

IRIS KPO is an accounting outsourcing company based in India, providing cost-effective, reliable and secure accounting data processing services to its customers. The objective of the services is to reduce cost and increase profit for the customers. IRIS provides various types of accounting related services, including services related to iXBRL, Payroll, Yearend, Bookkeeping, Snap invoice processing and Personal Tax.

## Statement of Assurance:

IRIS KPO will:

1 Put in place measures to protect customer information from breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to, personal data transmitted, stored or otherwise processed
2 Meet regulatory and legislative requirements
3 Produce, maintain and test business continuity plans
4 Provide information security training to all employees
5 Report and investigate information incidents (whether actual or suspected), in line with incident reporting procedure
6 Monitor compliance with Information security policy
7 Adhere to the record retention and disposal schedule

IRIS KPO 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 employees via company’s compliance portal.

## Organisational Security:

IRIS KPO is committed to fulfilling its obligations under UK Data Protection Act 2018 and any associated privacy legislation that affects how IRIS KPO uses or handles personal data. IRIS KPO has framed data protection policy to give assurance to customers and employees. Also, operations at IRIS KPO are ISO 27001 and 27701 certified.

This document includes high-level description of the procedures in place that must be followed, to ensure that personal data is handled in a responsible, accountable and secured manner.

IRIS KPO will use personal data legally and securely regardless of the method by which it is collected, stored and processed over on-premises servers, cloud or other storage media/devices.

The company believes that the success depends on the appropriate handling of personal data and by following best practices to maintain client confidence. IRIS KPO upholds privacy and handles personal information in an accurate and lawful manner.

Data protection and information security at IRIS KPO is controlled by Management Security Forum. This forum meets once in six months and includes:

- Senior Director - Operations
- Data Protection Officer
- IT Head
- All Functional Heads

The Management Security Forum discusses policies relating to information security and data protection of the services that IRIS KPO delivers. Following policies and procedures ensures information security at operations and organisational level.

- **Data & Privacy Protection Policy** – this policy ensures protection of customer's data and privacy

- **Acceptable Usage Policy** – this sets out acceptable usage standards that all employees within IRIS KPO are required to adhere

- **Security incident and weakness reporting** – this acts as the guideline for reporting and investigating all security incidents within IRIS KPO

The above policies are communicated to all stakeholders at IRIS KPO and are hosted on company's compliance portal.

The members of Management Security Forum are as follows:

| # | Employee Name | Department | Designation |
|---|---|---|---|
| 1 | Venkata Ramana Talapalli | Senior Management | Senior Director - Operations |
| 2 | Manickam Babu | IT & Admin | Associate Director - IT |
| 3 | Hariharan Subramanian | HR & Training | Director – Human Resources |
| 4 | Shini Krishna Bhaskaran | Finance & Accounts | Director – Finance |
| 5 | Srikanth Puranam | ISO | Director - Operations & Data Protection Officer |
| 6 | Vijay Ganesan | IT Applications | Senior Manager – Applications |
| 7 | Manoranjan Pattanayak | iXBRL, BK, Snap, PTR | Director – Operations |
| 8 | Saravanan Thyagarajan | APS - Yearend | Director – Operations |
| 9 | Srihari Sethumadhavan | Payroll and CRO | Senior Manager – Operations |

The Functional Heads mentioned above are the single point of contacts for routine security and data protection enquiries. They work closely with their managers and processors involved in delivering the jobs to ensure that services rendered are in line with IRIS KPO policies and Information Security Management System.

The IT Support team at IRIS KPO secures customer data by implementing appropriate measures to protect customer's data from accidental or unlawful destruction, alteration, unauthorised disclosure or access to data while being stored, transmitted or otherwise processed by or on behalf of IRIS KPO.

The Management Security Forum members ensure that adequate records are created and maintained to support compliance, verification and inspection.

The Data Protection officer at IRIS KPO is responsible for providing advice and guidance to IRIS KPO employees and monitors compliance related to information security and data privacy. IRIS KPO Data Protection officer works closely with IRIS Software Group Data Protection Officer and seeks guidance from them on a timely basis. IRIS Software Group Data Protection Officer is the designated contact for the Information Commissioner's Office.

Operations, IT Support and IT Applications teams are responsible for maintaining the integrity of the customer data. Awareness to employees on information security and data privacy is imparted at regular intervals during their employment.

## Human Resource Security:

- Resource planning is done by the functional heads with the approval from Senior Director - Operations and the same is communicated to the recruitment team via email along with a ticket being raised via an internal helpdesk portal
- Job description is shared with the recruitment team to identify suitable candidates

### Prior to Employment:

- The candidate's education and experience certificates, and ID proofs are duly verified against original documents at the time of joining. HR onboarding team certifies the copies during verification
- All employees accept and sign IRIS KPO Non-Disclosure Agreement at the time of joining

### During Employment:

- All permanent resources are subject to background verification (BGV) by an external agency. As part of the verification process, the candidate's employment history of past 5 years and their permanent address is being verified. If the candidate is found to have falsified his/her records (BGV Status: Red), the employee is terminated with immediate effect
- All new hires receive appropriate awareness training and regular updates with regards to organisational policies and procedures in a timely manner. They undergo ISO & GDPR awareness training and take mandatory assessment as part of the onboarding process. Additionally, they also undergo annual refresher training on General Data Protection Regulations
- Any security or data privacy breach by employees will lead to disciplinary action

### Resignation/Termination/Team Transfer:

Based on the communication from HR department on any voluntary resignation by employees or termination due to disciplinary measure, IT Support will take the following actions:

#### Resignation/Termination

- Full removal of access from organization network
- Collection of all IT assets from the concerned employee

#### Team Transfer

- In the event of a person being transferred from one department to another, access is revoked and reassigned as per the new requirements

## Access Control Policy:

The purpose of the Access Control Policy is to manage access controls as per the internal access requirements and prevent unauthorised access within the IRIS network.

Access controls to network, operating system and applications shall be set at an appropriate level on need to use basis, which minimizes information security risks yet allows the business activities to be carried without undue hindrance.

Information access at IRIS KPO is managed through secure and multifactor authentication.

Privileged access is managed through secure and multifactor authentication (where applicable), which is being reviewed periodically by IT Head.

An audit trail is maintained to monitor unauthorised access within IRIS KPO network.

Remote access to a customer's network shall always be subjected to customer's prior written (or otherwise validated) consent or request. Access to customer's network would be through VPN or remote assistance software.

### Password and Authentication Policy:

This policy describes the authentication requirements for accessing internal computers & networks and includes those working in-house as well as those connecting remotely. Every person, organisation or device connecting to internal IT resources and networks must be authenticated as a valid user before gaining access to IRIS KPO's computer systems, networks and information resources.

### Customer setup in IRIS KPO Applications & Portals:

**Changes in the access level:**

All user-level access changes are requested through helpdesk ticket with process owner approval and based on which IT Applications team makes necessary changes.

Customers are restricted to end user-level access to login to the portals.

Only IT Applications team has the super admin access to make any changes to the applications.

IRIS KPO warrants customers that its applications & portals will not seek to circumvent, compromise or change the customer's security controls, and IRIS KPO will not change the customer's software configurations (without proper authorisation) and no 'back door' password or other methods of remote access into IRIS KPO's software shall exist.

### Data Transmission through Email:

- Customers are advised to avoid transmitting job information having personal data via email as they would become GDPR non-compliant. Usage of Resourcing job portal and customer RDP server is emphasized for transmitting data to be GDPR compliant at all times

### Encryption Policy (Cryptography):

- Cryptographic methods and data encryption products recommended explicitly by regulators / customers / any other interested party are given highest priority
- Necessary security controls are considered to safeguard the interests of the customer and IRIS KPO, such as protecting the encryption passwords and keys, wherever applicable. E.g., physical/ logical access controls and awareness on secure handling of keys
- IRIS KPO shall use cryptographic controls in compliance with all relevant agreements, laws, and regulations
- When identifying the level of cryptographic protection following shall be taken into consideration (Where applied / used)
    - Type / Quality of Algorithm / Encryption
    - Length of Keys
    - Export / Import Controls, if any
    - National Regulations, if any

## Physical and Environmental Security:

IRIS KPO secures IT resources from harm, abuse or exploitation with tight access controls to critical computing devices.

Also, necessary controls are in place to restrict physical access to the premises of the organization. The restriction of physical access may vary from one area to another within the premises.

Processing servers are in a secured server room at IRIS KPO office premises and therefore protected from unauthorised access, damage, loss or compromise. UPS protection is provided, and the office is further protected by biometric access system and fire suppressant capacity in line with local fire safety regulations.

All IT equipment shall be properly maintained, and disposal of equipment or media handling devices shall be in strict accordance with recycling standards and would be fully certificated by approved e-waste disposal vendor. Confidential information (in paper form) shall be properly maintained and disposed by KPO facility department on a need basis with the approval of risk owners.

IRIS KPO enforces clear desk and clear screen policy at all times and is strictly monitored at regular intervals.

IRIS KPO is protected by CCTV surveillance with 68 channels. These CCTVs capture footages, which are maintained for a defined period for any investigation. The stored data is protected with access control as prescribed to maintain confidentiality. Access to the CCTV system and stored images are restricted to admin head only. Access is provided to other admin representatives on the approval of admin head based on the need and such activities are recorded for documented reference. The same is being communicated to CCTV executive committee.

### Third-Party Access Controls:

- Supplier/vendor who requires access to the information and to the information processing facilities of the organisation need to have prior consent of the organisation's authorised representative
- Physical access is restricted as per business need and will be reviewed as appropriate
- Information security roles and responsibilities for all personnel of supplier's team are defined, documented and signed by the supplier
- All suppliers are governed by individual NDAs
- All supplier team members are provided with user training and awareness and are governed by Acceptable usage policy of information assets
- Disciplinary action is taken against security breaches as applicable

## Equipment Maintenance:

### Storage and Movement:

- Hardware that stores critical information is stored in secured areas under additional physical access control
- Equipment like servers, printers to name a few will not be moved without the prior permission of IT head
- Installation of hardware is managed by IT department

### Maintenance/Operations - Hardware:

- All IT equipment of IRIS KPO is managed by IT department only

### Maintenance/Operation (including modifications) - Software:

- With respect to purchased software, no modifications are made to the source code
- With respect to open-source software, modifications to the application are made within the terms and conditions that govern the IPR/copyright
- Changes to IRIS application software developed in-house is restricted to IT Applications team only

### Data Retention Period:

Any personal data & customer data provided with instructions to IRIS KPO will be retained along with the instructions for six years (default standard retention period for HMRC records). Unless otherwise stated, the retention time starts at the end of the financial year in which the file or record was closed. Details on the HMRC retention period can be accessed here.

## Media Handling:

- Employees cannot connect to any external storage media
- Data Storage media is handled or transported upon approval from IT Head with utmost care to protect from unauthorised access, theft or loss

### Data Centre:

The data centre is monitored round the clock and is restricted to IT team using biometric authentication.

### Asset Movement:

Physical assets are moved from one place to another within/outside the office with prior approval from IT head. Movement of assets is captured in gate pass / outward register.

### Disposal of Data:

- Information assets will be deleted from the working folders
- Customer data from backups will be deleted once the retention period for the same is over
- Files and folders that have crossed retention period are listed out and approval is sought from DPO before deletion

### Disposal of Hardware:

- Disposal of hardware is done only after prior permission from scrap disposal committee
- Where disposal is by means of sale to a third party, information from the hardware is permanently deleted by formatting the hard disk or other storage media of the equipment
- Where disposal is by means of physical destruction, it is ensured that the equipment or item is irreversibly destroyed in a safe manner

### Disposal of Software:

- Software that is no longer in use would be uninstalled by IRIS KPO IT team from time to time

## Operations Security:

IT team is responsible for keeping systems reasonably up to date.

Functional heads are responsible for human resource planning for their respective teams and the same is communicated to the HR department. IT Support team receives the projection from the HR department and based on which IT infra procurement is planned.

All IT infra requirements, which are treated as capital expenditure are procured, subject to the approval from senior director-operations.

All support and operational activities (e.g. production, backup, transmission of confidential information, equipment maintenance etc.,) associated with information processing and communication are documented and maintained.

### Change Management:

Change management at IRIS KPO is carried out in a controlled manner so that required changes can be implemented without adverse impact to the operations and customers. This process also addresses management of technical vulnerabilities, which would require change management.

### Separation of Development, Testing and Operational Environments:

Development and testing facilities are isolated from production facilities and on segregated networks.

### Protection from Malware:

Anti-virus policy is in place to protect networks, systems and equipment from malicious code and malware. Anti-virus software versions are closely monitored and kept up to date. Anti-virus logs are reviewed, and appropriate actions are initiated promptly.

The external perimeter defence for IRIS KPO network is protected through firewall.

### Back-ups:

Operational data on IRIS KPO servers are backed-up at night and transmitted to a secure cloud back-up location by IT Team. Restoration tests are made and documented on a regular basis at periodic intervals. Customers are responsible for ensuring data back-up at their end.

### Event Logging:

IRIS KPO IT team maintains access logs of user activities, exceptions, faults and information security events on IRIS KPO servers and systems. IRIS KPO IT team and hosted operation teams maintain logs on all user activities for IRIS KPO applications (Portals & Software) and for customer data. Only authorised users have access to log and in accordance with the IRIS KPO access control policy.

### Management of Technical Vulnerabilities:

IRIS KPO IT team works closely with the production team on regular patch updates for operating system and software. For the portal cloud service, third-party security penetration testing is carried out and appropriate action is taken on the findings every year.

Technical vulnerabilities related to operating systems are monitored through Sophos AV control console. Additionally, technical vulnerabilities related to software used at IRIS KPO is monitored through websites of software vendors.

## Communications Security:

### Network Controls, Security and Network Segregation:

IRIS KPO IT team is responsible for the implementation and management of firewalls and segregation of network services to ensure protection of IRIS KPO's networks and connected services. IRIS KPO hosted operations teams are responsible for ensuring appropriate security mechanisms and segregation, together with appropriate service levels for cloud hosted services such as Job portals.

### Electronic Messaging:

- IRIS KPO staff comply with the acceptable usage policy
- Confidential information exchange through email is restricted
- Emails carry security disclaimer
- Access to mailbox is through multifactor authentication
- Email attachments are allowed only on a need basis. All attachments having confidential information are password protected
- Employees do not send vital job information/jobs via email and guide the customer to use job portals
- Bulk email is sent with the approval of functional head

## Application Design, Development and Maintenance:

IRIS KPO IT applications team is responsible for application design, development and maintenance in accordance with the design and development control procedures.

They specialise in the development and support of internal applications for accounting services and are privy to confidential information, not least to personal data, which is subject to the General Data Protection Regulation. IT applications team ensures that its applications are designed with robust information security. This includes coding for security of desktop and cloud applications and with reference to OWASP guidelines.

All IRIS KPO developed applications incorporate appropriate controls and audit trails and validation of input data, internal process and output data.

All source codes are treated as highly confidential and employees with authorised access strictly adhere to the use of the appropriate IRIS KPO development tooling for the purpose of checking codes in its entirety. IT Applications team is responsible for controlling access to the respective department's development and support environments.

All versions due for release undergo release management process to ensure that changes to issued software are controlled and thoroughly tested with high quality.

### Application User Login Creation:

Relevant department (Customer Relationship Office / CRO) sends the request to IT applications team via Helpdesk for new customer user login creation. The login ids are created with basic privileges.

For internal users (IRIS KPO employees), once the training is completed, process owners shall raise a request with IT applications team and required access privileges are created by the IT applications team.

## Supplier Relationships:

### Information Security in Supplier Relationship Policy:

This policy ensures that suppliers who may have access to customer data are properly & regularly assessed, published to those customers whose data may be involved and engaged under a data protection compliant contract.

The scope of this policy includes all suppliers, contractors, outsourced agencies, third parties, and vendors who have access to the information of the organisation, or who handle/manage the information on behalf of the organisation at IRIS KPO Resourcing (India) Private Limited.

IRIS KPO ensures that the suppliers are aware of all the local and regulatory laws applicable to the organisation and be compliant. Additionally, suppliers are aware of all the contractual and standard requirements of the organisation, which they shall abide, and stringent action is taken for any deviation.

## Information Security Incident Management:

IRIS KPO has documented procedures to handle information security incidents.

### Management of Information Security Incidents and Improvements:

An information security incident involves the loss or misuse of any personal or business sensitive data held by IRIS KPO regardless of the format. This includes electronic data held within IRIS KPO systems and physically held information.

### Procedure for Dealing with Information Security Incidents

#### Reporting an Information Security Incident:

- All employees at IRIS KPO have been instructed to report information security incidents to their supervisors immediately and post which the incident needs to be brought to the attention of IRIS KPO Data Protection officer
- If an information security incident is caused by an external contractor, this is reported through their IRIS KPO contact. The team which manages the external party will initiate appropriate action in consultation with senior management, UK Legal and Compliance team

- IRIS KPO Data Protection Officer reports all information security incidents to IRIS Software Group Data Protection Officer

**Organizational Management of Information Security Incidents:**

- Senior Director, Operations is notified about all information security incidents. Preventive action is being taken by the Incident Management team (IT, Process Owner & IRIS KPO Data Protection Officer) to avoid recurrence of such incidents and any recurring incidents are considered and mitigated through risk management process

## Business Continuity – Information Security Aspects:

### Business Continuity Policy:

The purpose of the IT Business Continuity Policy is to ensure that IRIS has the appropriate resources available for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving business continuity capability that will enable the company to manage any business continuity disruption.

### Business Continuity Management:

IRIS KPO has established a process to ensure business continuity at all times. This involves identifying business continuity needs and framing, implementing and testing the continuity plans.

**Purpose and Scope – Business Continuity Plan:**

The purpose of IRIS KPO Business Continuity Plan is to enable the operation teams to manage an incident that disrupts normal operations and working practices.

The Business Continuity team comprising of senior director – operations, functional heads and other critical team members are responsible for implementing the action plan during any disaster.

## Compliance:

### Compliance with Legal and Contractual Requirements:

Senior director - Operations will identify the possible legislations/regulations (local and foreign) that the company shall comply with.

### Applicable Legislations/Regulations:

- Intellectual Property Rights
- General Data Protection Regulation (GDPR)

### Policy on Intellectual Property Rights Compliance:

IRIS KPO ensures compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products.

**Policy Statement:**

- Licensing policy of proprietary software products is always complied with
- Ownership of materials governed by Intellectual Property Rights is honoured
- Employees are not allowed to bring in any software or download any software without prior approval from IT team

### Compliance with Security Policies and Standards:

Management Security Forum members regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements at IRIS KPO.

## Data Protection – Quick Reference:

**Data Protection Officer for IRIS KPO – Srikanth Puranam** (srikanth.puranam@iriskpo.in)

**<<End of Document>>**