Information Security Assurance Statement of IRIS KPO

Document control		
Version number	:	1.3
Replaces	:	1.2
Release Date	:	09/06/2023
Document type	:	Information Security Assurance Statement
Owner	:	ISSO
Approved by	:	Director – Operations
Approval date	:	09/06/2023
Data protection impact screening:		No PIA required
Date of next formal review	:	08/06/2024 (1 year)

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	Changes in HR, ISO heads and designations
4	1.4	31st May 2023	Formal review	Updated statement of assurance, data retention and data disposal

Contents

Information security assurance statement of IRIS KPO

Objective:

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

Description of the data processing carried out by IRIS KPO:

IRIS KPO Resourcing (India) Private Limited is an accounting outsourcing company based in India, built by accountants, for accountants. IRIS provides cost-effective, reliable and secure accounting data processing services to our customers to the extent of their expectation. The objective of the services is to reduce cost and increase profit of customers. IRIS provides various types of accounting related services including services related to iXBRL, Payroll, Year End, Bookkeeping, Snap and Personal Tax processing.

Statement of assurance:

IRIS KPO 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
7 We will 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, passwords-authentication, communication and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

IRIS KPO Organisational Security:

IRIS KPO is committed to fulfilling its obligations under the Data Protection Act 2018, General Data Protection and Regulation (GDPR – EU law) and any associated privacy legislation that affects how IRIS KPO uses or handles personal data. IRIS KPO has produced the Statement of data protection policy to give this assurance to our customers and staff. Also, all services/operations in IRIS KPO's are ISO 27001 certified by BSI certification body.

In addition to the IRIS KPO Statement of data protection policy, this document sets out how responsibility for data protection and information security is designated. It includes high-level descriptions of the procedures in place that must be followed to ensure personal data is handled in a responsible, accountable and secure manner.

IRIS KPO will use personal data legally and securely regardless of the method by which it is collected, recorded and used and whether we hold it within our products, on a Group or third-party network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

IRIS KPO regards the proper management of personal data as crucial to the success of our business. Observing good data protection practice plays a huge role in maintaining customer confidence. We ensure that IRIS KPO respects privacy and treats personal data lawfully and correctly.

Organisational security at IRIS KPO level:

Data protection and information security at IRIS KPO is controlled by the Information Security and Governance Forum. This forum meets at least half-yearly and includes:

- Members of the Incident Management Team
- Members of Management Security Forum
- IRIS KPO IT Head
- IRIS Resourcing Data Protection Officer
- Other key security leads within the company

The Information Security and Governance Forum approves policies relating to information security and data protection, which IRIS KPO products must comply with all the requirements of compliance. There are three Group policies and a detailed Information Security Management System (ISMS). The three Group level policies are:

- **Data Protection Policy** – this sets out the roles and responsibilities for data protection compliance within the IRIS KPO. 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 KPO are required to adhere too.

- **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 KPO.

The above policies are communicated to all staff and relevant external staff within the IRIS KPO at least annually, using a dedicated training and policy management platform. Managers responsible for delivering IRIS KPO products and services are required to ensure local arrangements are in place to comply with those policies and to evidence this.

- IRIS KPO ISMS – This is the default security system for IRIS KPO. All IRIS KPO products must meet or be working towards meeting the standards of the IRIS KPO ISMS.

Organisational security for IRIS KPO services:

At IRIS KPO, 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 jobs to ensure services complies with the IRIS KPO policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

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

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

The IRIS KPO IT Support 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 KPO.

The compliance 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).

KPO Data Protection officer is responsible for providing advice and guidance to the IRIS KPO 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.

IT Support & IT applications teams are responsible for the operation and integrity of IRIS KPO service's and IT systems for keeping systems reasonably up to date.
IRIS KPO's Development systems are managed by IT Application and approved third-party vendor.

Asset register: IT Team & Production team will maintain a register of all assets, relevant to IRIS KPO's (including acquired software licences) in a fixed assets system.

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

IRIS KPO Human resource security:

- Required resource planning is done by HR Head along with Operations-Head and the same is drafted and communicated to the Recruitment Team by the respective Department Heads via Internal Helpdesk portal
- Every position is defined with the Job Description and the recruitment happen matching to the required skill sets and expertise

Prior to employment:

- The candidate educational & experience certificates are duly verified with reference to the Originals during the time of joining. HR Team recruitment certifies the copies for verification
- 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:

- The IRIS KPO Information Asset Owner is responsible for ensuring that Information Asset managers are made aware of their responsibilities to ensure that established policies and procedures are adhered to by external parties, contractors and employees
- IRIS KPO employees, third parties and contractors receive appropriate awareness training and regular updates in organisational policies and procedures as relevant for their job function by their designated IRIS KPO Information Asset manager. Organisation policies, security guidelines and other useful stuffs are administered via the KPO Human Resource Management System (HRMS) portal
- A formal and communicated disciplinary process is implemented to handle IRIS KPO employees who have committed a security breach
- Department or Process Training and mentor coaching to personnel is to be done internally, through on- the job training and evaluating the knowledge by metrics periodically
- All HR related information will be communicated to Management and Employees through HRMS/E-mail/Notice Board/MS Teams

Termination and change of employment:

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

- Full removal of access to any part of the organization 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 KPO that person's access will be varied accordingly

Termination:

Misconduct or violation of any Policy: IRIS HR Policy specifically calls for the termination of an employee due misconduct or violation of any Policy of the Company. Manager – HR with sufficient cause and verification of the facts shall initiate the process for termination of the staff on the approval of the HR Head.

- Prepare the Termination Letter and forward the same to the residential address of the staff
- Preserve the copy of the Termination Notice along with the acknowledgement of the courier in the staff file
- Update the record of HR as the candidate is terminated as on the date of Termination Notice Letter

IRIS KPO Access Control Policy:

The purpose of the Access Control Policy is to ensure that information systems resources and electronic information assets owned or managed by IRIS are available to all authorised personnel. The Policy also deals with the prevention of unauthorised access through managed controls to create a secure computing environment.

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. This is managed as per the Organisational Security section in conjunction with the IT Manager and Information Asset Owner and in accordance with the IRIS KPO Access Control Policy.

Access is granted on the least privileged rule basis consistent with an individual's job/role responsibilities. For IRIS KPO user login, system enforced Password complexity rules ensure that strong passwords are used and Users are responsible for keeping them confidential. Systems and information should be secured whenever left unattended.

All static user equipment must be kept in good order and used responsibly; all laptops shall be subject to the IRIS KPO Acceptable usage policy. Passwords must not be disclosed to colleagues or any third parties. As set out in IRIS KPO's standard HR Policies all personnel must maintain full conformance with company undertakings in respect of confidentiality.

Access to cloud-based administration consoles for privileged IRIS KPO IT Department and IRIS users is mandated with password authentication.

Server Operating System Access Control along with change and patch management shall at all times adhere to Microsoft's best practice and shall be administered by the KPO IT team in conjunction with the production managers in respect of their individual department's development and support environments.
All administration systems are monitored and audit trails produced together with email notification to the System Manager of any unauthorised attempts to access the corporate network.

Remote access to a customer's network shall always be subject to customer's prior written (or otherwise validated) consent or request and must be controlled either by using customers provided VPN and or remote assistance software which utilises SSL and provides a full audit trail.

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's computer systems, networks and information resources.

Customer setup in IRIS KPO Applications & Portal:

Changes in the access level:
All access level changes should be escalated to IT Application department through helpdesk with account manager and application owner approval.

Product/Service level changes will be accessible by only IRIS KPO IT Application team. Customers do not have facilities to change the access level. IRIS KPO Applications/Software program code can be accessible only by IT Application team.

For the avoidance of doubt, IRIS KPO warrants to customers that it 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 method 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-complaint. Usage of Resourcing job portal and customer RDP server is emphasized for transmitting data to be GDPR compliant all the time

Encryption Policy (cryptology):

- The purpose of the Encryption Policy is to ensure that encryption keys are securely managed throughout their life cycle. This includes their creation, storage and the manner in which they are used and destroyed
- This policy is designed in IRIS KPO to define acceptable practices and methods, providing guidance to enhance the reliability, effectiveness and quality of selecting and implementing cryptographic controls. Cryptographic controls are to be considered for data, which is sensitive or has a high value, is vulnerable to unauthorized disclosure or undetected modification while in storage or during transmission
- IRIS KPO IT policy ensures that encryption keys are securely managed throughout their lifecycle and in accordance with the IRIS KPO encryption policy
- Remote support sessions with IRIS KPO's staff are with staff consent, utilise SSL encryption and have a full audit trail
- Data is encrypted in transit via SSL (AES256)

IRIS KPO Physical and Environmental security:

The purpose of the Physical Access Policy is to protect IRIS KPO IT resources from harm, abuse or exploitation and describes the parameters for controlling the environmental conditions for critical computing devices.

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

Processing servers are located in a secure and locked server room in the IRIS KPO office 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 any disposals of equipment or media handling devices shall be in strict accordance with recycling standards and 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 quarterly basis with the approval of risk owners

IRIS KPO enforces a clear desk policy. Staff laptops & IT assets are sited in a secure office area, information displayed on screen (or on paper) may be confidential. All computers revert to screen saver mode at timely intervals and staff are mandated to logoff from sessions and ensure any paper documents are stored in locked filing/cupboards when their workplace is unattended.

IRIS KPO is protected under CCTV surveillance with 68 channels. These CCTVs capture images for the post investigation/breach purpose. The stored data will be protected with access control as prescribed, to maintain confidentially. Access to the CCTV system and stored images will be restricted to Admin Head only. Access can be provided to other Admin Manager/Representative on the approval of Admin Head based on the situations and such activities to be recorded as documented information. The same must be communicated to CCTV executive committee.

Access controls:

- All personnel part of the supplier's team who require 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 shall be restricted as per business needs, privileges shall be reviewed every quarter.
- Physical access restricted by badges and key access and such privileges are reviewed

Human Resource:

- Information security roles and responsibilities for all personnel of supplier's team are defined, documented and signed by the suppliers
- Additionally, they shall be governed by individual NDAs
- All supplier team members are provided user training and awareness and are governed by Acceptable usage Policy of information assets
- Disciplinary actions shall be taken against security breaches as applicable for the organisation's employees

Equipment Maintenance:

Storage and Movement:

- Hardware that store critical information should be in secure areas under additional physical access control
- Other equipment is like server, printers, etc. should not be moved without the prior permission from the SM
- Installation of hardware should happen only if authorized by the SM

Maintenance/Operations - Hardware:

- By default, only the owner of the asset can operate the hardware
- No person other than the owner (s) should operate hardware in secure areas like data centre without the permission of the SM

Maintenance/Operation (including modifications) - Software:

- With respect to purchased software no modification should be made to the source code
- With respect to open source software modifications to the application can be affected within the terms and conditions that govern the IPR/copyright
- Changes to application software developed in house will be initiated by the Production Manager

Data Retention Period:

Any personal data & customer data provided with instructions to IRIS Open Resourcing will be retained by us 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:

- IRIS KPO employees may only use prior authorised removable media supplied by IT Department. Such media will typically comprise encrypted external drives and memory sticks, all of which are password protected and their use duly monitored Security software. Unauthorised media handling devices will not work. Individual customer security requirements may from time to time necessitate specific authorisations being prior arranged with IT department
- Users shall not even try to visit Internet sites that contain obscene, hateful or other objectionable material
- Users shall not attempt to bypass Organizational surf control technology and shall not make or post indecent remarks, proposals or materials on the Internet
- Users shall not download software from the Internet or execute or accept any software programs or other code on the Internet
- E-mails or attachments from unknown sources should not be opened

Data Centre:

The data centre is monitored around the clock. Mantrap systems provide access only to authorised individuals. Technicians can then enter special rooms using key & biometrics authentication.

Asset Movement:
Any physical assets to be moved from one place to another place within the office and outside the office with prior approval from Senior Management and maintain the relevant document like gate pass, outward register.

Disposal of Data:
- Information assets will be deleted from the working folders
- All customer data from backups will be deleted once the retention period for the same is over
- Prior to deletion list out the details of the folders that have crossed retention stage and get the approval of the ISSO

Disposal of Hardware:
- Disposal of Hardware will be done only after prior permission from the senior management
- Where disposal is by means of sale to a third party, all information from the hardware has to be permanently deleted by formatting the hard disk or other storage media of the equipment
- Where disposal is by means of physical destruction, it has to be ensured that the equipment or item is irreversibly destroyed in a safe manner
- Where destruction of equipment happens offsite, all information will be permanently deleted before taking the equipment out or will be personally accompanied and destruction supervised by Senior Management.

Disposal of Software:
- Software's that are no longer in use can be uninstalled by IT
- The physical installation media (CDs or floppies, etc.) may be retained as per the requirement
- After the retention period is over the physical installation media may be disposed

Operations security:

All department heads are responsible for monitoring and projecting required usage of processing resources and or storage together with IT infrastructure team. IT team shall be responsible for keeping systems reasonably up to date. All purchases of additional or replacement processing resource shall be subject to a capital expenditure approval at senior management level.

Documented operating procedure:
All the support and operational activities (e.g. backup, transmission of confidential information, equipment maintenance etc.,) associated with information processing and communication facilities and related to IRIS KPO services has been documented and included in the Control of documented information.

Change Management:
- All versions due for release to any customer must have prior undergone IRIS KPO product risk owner and release management process to ensure that changes to issued software are controlled, have been thoroughly tested and are to a high quality.
- Any changes to the BEST/QMS/HRMS (Internal applications) etc. and Portals (iXBRL/Snap/IRJTS) to be scheduled to the weekend to enable all relevant risk owners to apply the changes, study the impact and to take decision on the same.
- Review and acceptance by the risk owner is mandatory before releasing the changes to live environment. This applies for emergency changes too.

Capacity Planning:

All department heads are responsible for monitoring and projecting required usage of processing resources and or storage together with IT infrastructure team. IT Team shall be responsible for keeping systems reasonably up to date.

Separation of development, testing and operational environments:

Development and testing facilities are isolated from production facilities and on segregated networks. Identify third party, which can develop the software as per the Purchasing and Subcontracting process.

Protection from malware:

Anti-Virus Policy:

This Policy is about protecting networks, systems and equipment from malicious code and malware. Laptops and mobile devices are most at risk as they may only be connected to the network periodically. The appropriate use of Anti-virus software will lessen the risk of the company experiencing this type of security incident.

Firewall Management Policy:

The purpose of the Firewall Management Policy is to ensure that the external perimeter defence for IRIS is configured, managed and maintained to prevent the occurrence of a major security threat.

Back-ups:

The backup of all KPO processing server systems falls under the remit of the IT head. All data is backed up nightly and transmitted to a secure cloud back-up location. Restoration tests are made and documented on a regular basis, not less than annually. Note that customers are responsible for ensuring that they backup their own on-premise data on a regular basis.

Event logging:

IRIS KPO IT team, maintain and access logs of user activities, exceptions, faults and information security events on IRIS KPO servers & systems. The IRIS KPO IT team and hosted operations teams maintain logs on all user activities for the IRIS KPO application services (Portal & Software) and for customer's data located in IRIS KPO provided hosted environments. Only authorised users have access to logging information and in accordance with the IRIS KPO access control policy.

Control of operational software:

IRIS KPO staff must abide by IRIS KPO IT policy, procedures, and this means only approved software can be used on IRIS systems/laptops.

Management of technical vulnerabilities:

IRIS KPO IT team and the production & support team ensure that internal systems are regularly patched with operating system and software updates. For the portal cloud service, annually third-party security penetration testing is carried out and appropriate action taken on the findings within specified maximum time-scales.

Monitor technical vulnerabilities related to operating systems through TrendMicro Worry free business control console and portal applications used by the organization by constantly referring to software vendor website.

Communications security:

Network Controls, Security and Network Segregation:

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

Electronic messaging:

- IRIS KPO staffs must comply with the IRIS KPO IT Acceptable usage policy
- Confidential information exchange through email will be restricted
- Emails will carry security classification and disclaimer
- Secured access to email will be provided based on user id, password
- Attachments to the emails are allowed only on need to use basis for the operational purpose. The user should protect confidential documents/attachments with password and password should be sent in separate approved medium by the organization
- Employees are instructed not send vital job information/jobs via email and guide the customer to use job portals
- The Bulk email should be sent with the approval of functional head. Functional heads should own the bulk email customer list and the Deputy Manager, Team Manager & TL or next level manager to send the email with approval of functional head only. Functional heads are responsible for reviewing and approving of bulk Emails with their respective functions

Confidentiality or non-disclosure agreements:

All the employees & service provider's confidentiality or non-disclosure agreements are identified, reviewed, documented and reflect the product/service's needs for the protection of information at IRIS KPO.

System acquisition, development and maintenance:

Design and Development Planning:

IRIS KPO IT Support & Application teams are responsible for the implementation and management of VPN access, Firewalls and the use of encryption and other security measures to ensure the protection of IRIS KPO application systems and connected services when new systems are implemented or changed. The IRIS hosted operations team are responsible for ensuring that appropriate security mechanisms and segregation is in place, together with appropriate service levels for cloud hosted services such as job portals and applications

IT Application plans and manages the design and development of IRIS KPO service in accordance with the design and development control procedure. Planning output is updated at appropriate stages as design and development progresses.

Design and Development Inputs:

Inputs relating to service requirements are defined as per the 'Design and Development Control Procedure'. This includes:

- Software Requirement Analysis

- System Analysis and Design
- Functional, Technical and Performance requirements design
- Applicable information derived from previous similar designs
- Any other requirements essential for design and development
- Application Assessment (Architecture, Design, Performance)

Design and Development Outputs:

The outputs of the design and development process are recorded and expressed in terms of requirements, calculations and analysis.

This process ensures that design and development outputs:

- To meet the design and development input requirements
- Provide adequate information to production and service operations
- Contain or reference product acceptance criteria
- Define the characteristics of the product that are essential for its safe and proper use

Design and Development Verification:

- Design and Development verification are defined, planned, executed and recorded by competent personnel to ensure that the design and development output meets the inputs
- Verification occurs much earlier in the development process, allowing stakeholders to fine-tune requirements while they are still relatively easy to change.

Design and Development Validation:

Design and development validation are ensuring that resultant products are capable of meeting the requirements for the specified application or intended use, where known, prior to release for delivery or implementation. It is impossible to perform full validation prior to delivery or implementation; partial validation is performed to the extent applicable.

IT Application Management looks at our projects / products objectively, ensuring a confident rollout. With exclusive testing engagements, our skills, tools, processes & infrastructure - tuned to address unique nuances of every stage at product life cycle. We are fully adept working in a dynamic environment and take ownership of code quality.

Final deployment of the site includes setup and testing on the customer's systems. We actively participate with the customer in the beta releases of the system, and our detailed logging mechanisms ensure that any bugs that have passed the earlier phases unnoticed are efficiently located and fixed. This phase also includes any necessary knowledge transfer of working principals through presentation.

Security in development and support processes:

Please refer to the IRIS KPO Statement of Applicability (SoA) for further details on our Security in development and support process controls.

IRIS KPO staff specialise in the development and support of software systems for accounting services and is privy to confidential information, not least to personal data, which is subject to the General Data Protection Regulation we ensure that our software and services are designed with robust information security at their core. This includes coding for security for both desktop and cloud services and in particular with reference to OWASP guidelines.

The IRIS KPO Job portal cloud service is subject to annual third-party security penetration testing and monthly vulnerability scanning to ensure it remains secure and we act on the findings within pre-determined time-scales to remediate any issues.

All IRIS KPO developed software must incorporate appropriate controls and audit trails or activity log and validation of input data, internal processing and output data.

All source code for IRIS KPO products must be treated as highly confidential and all personnel with authorised access must strictly adhere to the use of the appropriate IRIS KPO development tooling for the purposes of checking code in and out. The Development managers are responsible for controlling access to the respective department's development and support environments.

All versions due for release to any customer must have prior undergone IRIS KPO Product manager, risk owner and release management process to ensure that changes to issued software are controlled, have been thoroughly tested and are to a high quality.

Test data is based on sample test data as a rule. Occasionally, production derived data may be used but its use is carefully protected and controlled and any such data is destroyed once testing is completed.

Customers must always be advised to maintain suitable facilities for testing and training purposes separately from their live environment. System changes must be reviewed and tested as agreed between IRIS KPO and Customer. All development testing will be done in IRIS KPO testing servers.

IRIS KPO's servers and all other equipment containing confidential information, personal data or source code must be ring fenced. All source code must be stored in central repositories to which physical and logical access is closely monitored. All desktops and laptops, whether static or mobile, shall be fully encrypted.

Database Creation and Maintenance:

SQL (Structured Query Language) is a standardized language for defining and manipulating data in a relational database. In accordance with the relational model of data, the database is treated as a set of tables, relationships are represented by values in tables, and data is retrieved by specifying a result table that can be derived from one or more master tables. SQL statements are executed by IT Application Management.

Schedule Backup and Maintenance:

Code and Database backups will place in the appropriate location mentioned by IT Systems. For database-driven software applications such as these, it is important to have established procedures to assure that proper database maintenance and backup activities are being performed.

Application user login creation:

Relevant department (CRO/HR) sends the request form via Helpdesk for the new users to create the applications login id. The login id will be created with base privileges for those employees' / customer users. For internal users, once the production / job training is completed, account managers shall raise a request with required access privileges and will be activated accordingly.

Supplier relationships:

Information security in supplier relationships policy:

As part of IRIS KPO, all support services abide by the Information security in supplier relationships 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 organization, or who do handle/manage the information on behalf of the organization at IRIS KPO Resourcing (India) Private Limited facility. All of the above are supposed to read this policy. This policy shall comply with the laws and regulations of the land where the organization is functioning.

Review:

Review of this policy shall be every year or whenever there is change in the business environment or technology or whenever there is a change /transition of any of the suppliers, whichever is earlier.

IRIS KPO shall ensure that the Suppliers shall be aware of all the local and regulatory laws applicable to the organization and be compliant to them. Additionally, supplier shall be aware of all the contractual requirements and the standard requirements of the organization, which it shall abide.

Information security incident management

The IRIS KPO have documented procedures in place to handle information security support cases.

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 format. This includes electronic data held within IRIS KPO systems and physically held information.

Procedure for Dealing with Information Security Incidents:

<u>Reporting an Information Security Incident:</u>

- All information security incidents should be reported immediately on being identified to the Data Protection officer via dpodesk@iriskpo.in or Helpdesk portal. The sooner an incident is reported the sooner the risks can be assessed and managed. Lost IT equipment should also be reported to the dpodesk@iriskpo.in or IT desk at extension 212 or IT Helpdesk portal or it_systems@iriskpo.in.

- If an information security incident is caused by an external contractor, this should be reported through their IRIS KPO contact. The team responsible for the external contract should check whether contract terms were appropriate in respect of information security and had been complied with mandatory documents. Seek legal advice from the IRIS KPO legal adviser if required.

- The IRIS KPO Data Protection Officer will report a summary of all data protection incidents to the IRIS Group DPO and maintain a list of learning outcomes and actions arising from incidents with the aim of ensuring Information Asset Owners follow through on those actions.

Organizational Management of Information Security Incidents:

- If the Incident requires the invocation of BCP plan, Incident Management & Governance Team will proceed with the Critical Incident Management Process with the guidance of Data Protection Officer.

- In line with the IRIS KPO Risk Management Policy, the IMG team will conduct a risk assessment for each critical incident, to gauge the impact and likelihood of realization, in relation to data subjects, customers and IRIS KPO.

- All critical incidents will be reported to the Director – Operations / Sr. Management of Division after the risk assessment is complete to address with the employee(s) involved and when the mitigated risk is rated at medium or above, to Human Resources.

- A significant security breach, or repeated security breaches, by the same individual will result in disciplinary action by the HR dept. Breaches of a criminal or illegal nature will be, where appropriate, reported to the relevant authorities.

Business continuity – Information security aspects:

Business Continuity/DR Policy:

The purpose of the IT Business Continuity/DR Policy is to ensure that IRIS has the appropriate resources available for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a Business Continuity/DR capability that will enable the organisations to prepare for, respond to and recover from disruptive incidents when they arise. The scale of events covered by this Policy ranges from minor or partial system unavailability (business continuity) through to total system loss (disaster recovery).

Business Continuity Management:

The organization has established a process to ensure the business continuity. Identifying business continuity needs, producing and implementing continuity plans and testing are carried out as per Business Continuity Process.

Purpose and Scope – Business Continuity Plan:

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

This Plan is aimed at an incident in IRIS KPO Chennai or dealing with the wider issues of an incident at the geographical location.

This document covers method of invoking the plan in a disaster recovery situation, detailed responsibilities and timelines for recovery and a process to bring the operations to BAU (Business as Usual) mode.

Role	Name	Contact Details
Plan Director	Venkata Ramana Talapalli	Primary Mobile: +919380872021

Information Security Risk Assessment:

The major business process of the organization is related to operations & support services. Operational processes are supported by internal processes of the organization such as Information Technology processes, Administration Processes and HR processes as illustrated and records in documented control.

Risk assessment has been carried out based on Risk Management Process. List of security controls listed in ISO 27001:2013 standard is used to implement security controls at IRIS KPO.

Information Security Risk Treatment:

Risk Assessment and Risk Treatment Plan Document presents details of Risk Matrix used to quantify risk, Risk Assessment and Risk Treatment as applicable to IRIS.

The control objectives and controls selected based on risk analysis and as required by ISO 27001:2013 is documented in Statement of Applicability with justification for exclusions.

Compliance:

Compliance with legal and contractual requirements:

Senior management or Legal department will identify the possible legislations/ regulations local and foreign that the company shall comply with.

When required, a professional consultant may be identified to conduct, a detailed legal review of the Company in order to determine the level of statutory and to make suggestions regarding areas in which IRIS could implement a change or make further improvements.

Compliance statement will be reviewed by senior management as a part of security control effectiveness review.

Applicable Legislations/Regulations:

A. Labour and Employment:

Compliance with labour law requirements, with reference to the relevant statutes and rules framed there under. Important provisions of the applicable labour enactments:

Statutory Compliance

Legal, regulatory and statutory requirements with respect to State & Central Government as listed in Information security supplier relationships policy.

B. Other Domestic Legislations:

- Intellectual Property Rights
- Reserve Bank of India
- I.T. Act
- Data Privacy

C. Foreign Acts:

- UK Data Protection Act
- General Data Protection Regulation (GDPR)

Policy on IPR compliance:

To ensure 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 shall be complied with.
- Ownership of materials governed by Intellectual Property Rights shall be honoured.
- Employees shall not be allowed to bring in any software or download any software without approval.

Compliance with security policies and standards:

DPO or ISSO shall 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.

Information security reviews

ISO27001 certification is audited annually by an external assessor. Internal compliance with Group ISMS is also annually reviewed. Annual external third-Party Penetration testing is carried out for cloud services with monthly vulnerability scanning.

Data Protection – quick reference

IRIS KPO Data Protection Officer – dpodesk@iriskpo.in

Data protection owner for IRIS KPO – Venkata Ramana T - venkataramana.t@iriskpo.in

Location of personal data processing:

Personal data is accessed by customer in Microsoft Azure portal located in UK south data centre and customer's own infrastructure. The data is downloaded in KPO data centre in Chennai, India, processed and posted back to UK data centre. EU contract clauses are in place with customer and IRIS KPO

Data subject rights:

IRIS KPO processes the personal data lawfully and for the purposes of accounting services and to allow our customers to provide various accounts statements relating to their employees or individuals according to UK legislation.

The IRIS KPO Customer Relations Department and IT Support team can be contacted with regard to data subject information requests.