Information Security Assurance Statement for Direct PSI Clients

PSI Payroll Services Inc. by IRIS

INFORMATION SECURITY ASSURANCE STATEMENT OF
PSI PAYROLL SERVICES INC

Document Control	
Version number	1
Owner	Juliana Borges (Head of Operations)
Date of last update	September 1, 2022
Document type	Assurance Statement
Replaces	New Release
Approved by	Adrian Demkiw (Managing Director)
Approval date	September 2, 2022
Data protection impact screening	Completed/ Approved
Date of next formal review	September 2, 2023

CONTENTS

1.0 OBJECTIVE OF THIS DOCUMENT

The purpose of this Information Security Assurance Statement is to provide clients of PSI Payroll Services Inc. by IRIS with transparency as to the security and personal data compliance of this service 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 PSI Payroll Services Inc. by IRIS as a thoroughly secure service provider.

1.1 Description of the data processing carried out by PSI Payroll Services Inc. by IRIS.

PSI Payroll Service Inc. by IRIS provides payroll outsourcing services in Canada. We offer end-to-end payroll processing functions. The objective of the service is to reduce cost and increase profit of our clients. PSI provides various types of payroll related services such as payroll calculations, payroll queries, payroll reporting , government (Provincial and Federal, garnishments, Workers Compensation) and 3 rd party vendors (RRSP, DPSP) remittances, processing Record of Employments (ROEs), payslip distribution and Year-End Processing (T4, T4A, RL1).

2.0 STATEMENT OF ASSURANCE

PSI Payroll Service Inc. by IRIS 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 and maintain 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.

PSI Payroll Service Inc. by 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.

3.0 PSI PAYROLL SERVICES INC. by IRIS ORGANISATIONAL SECURITY

PSI Payroll Services Inc by IRIS is committed to fulfilling its obligations under The Personal Information Protection and Electronic Document Act (PIPEDA) and The Privacy Act that is relevant to its service . PSI Payroll Services Inc. by IRIS observes the IRIS Group Data Protection Policy to give this assurance to our clients and staff.

In addition to the IRIS 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.

PSI Payroll Service Inc by IRIS 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.

PSI Payroll Service Inc. by IRIS 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 PSI Payroll Services Inc. by IRIS respects privacy and treats personal data lawfully and correctly.

Supporting accreditations held by PSI Payroll Services Inc. by IRIS are:

- ISO9001
- ISO27001

We employ the use of WinLedge Payroll System technology that houses personal data in Canada.

Employees are only granted access to view this data through the use of an internal group VPN.

PSI Payroll Services Inc is part of the **IRIS Software Group**.

3.1 Organizational security at PSI Service Inc. by IRIS:

Data protection and information security at PSI Payroll Service Inc. by IRIS is controlled by the IRIS Information Security and Governance Forum. This forum 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
- Other key security leads within the company

The Information Security and Governance Forum approves IRIS Group level policies relating to information security and data protection, which PSI Payroll Services In.c by IRIS products must comply with. There are three group policies and a detailed Information Security Management System (ISMS). The three group level policies are:

1. **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.

2. **Information Security and Acceptable Use Policy Summary**
   This sets out the basic information security and acceptable use standards that all staff within the PSI Payroll Service Inc. by IRIS are required to adhere to.

3. **IRIS Group 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 PSI payroll Services Inc. by IRIS organization.

The above policies are communicated to all staff and relevant external staff within the IRIS Software Group at least annually, using a dedicated training and policy management platform.

- **IRIS ISMS**
  This is the default security system for the IRIS Group. All PSI Payroll Services Inc. by 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.

3.2 Organizational security for PSI Payroll Services Inc. by IRIS

At PSI Payroll Services Inc. by 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 payroll services to ensure PSI Payroll Services Inc. by IRIS complies with the IRIS Software Group policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

For PSI Payroll Services Inc by IRIS, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

Employee Name	Department	Designation
Adrian Demkiw	Senoir Management	General Manager PSI
Juliana Borges	Senior Management	Head of Operations
Cindy Positano	Implementation Team	Head of Implementation
Monika Migdal	Payroll Managed Service	Payroll Team Lead
Mary Brown-Reym	Finance and Accounts	Finance Manager
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group

The PSI Payroll Services Inc by IRIS 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 PSI Payroll Services Inc. by IRIS.

The PSI Payroll Services Inc. by IRIS 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 PSI Payroll Services Inc by IRIS 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.

IRIS Group IT are responsible for the operation and integrity of PSI Payroll Services Inc. by IRIS's IT systems and for keeping systems reasonably up to date.

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

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

3.3 PSI will have access to your data to fulfil the Payroll Services

Prior to employment

PSI Payroll Service Inc. by IRIS Employees 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 and Information Security & Acceptable Use Policy.

During employment

The responsibility for ensuring that processes and procedures are both established and maintained are held with PSI Payroll Services Inc. by IRIS Managers. In the event of the use of an external party, controls are put in place to restrict the level of data they have access to in line with group policy and this activity is supervised and relevant risk assessments have taken place.

In addition to local procedure, the IRIS Software Group also requires the completion of corporate policy training and the subsequent testing of this knowledge through the MetaCompliance portal. This testing is repeated as frequently as is reasonable for all IRIS Group employees.

In the unlikely event of a security breach, the governing policy or procedure would be re-reviewed and amended to ensure stricter compliance moving forwards. PSI Payroll Services Inc by IRIS places the onus on the employee for their adherence to security protocols and a disciplinary procedure is enforced for non-compliance. If no improvement is found to employee performance under the afore mentioned disciplinary, employment is terminated as set out in the terms of the procedure.

Termination and change of employment

In the event of an employee terminating their employment contract with PSI, the following departments are notified and the following actions take place:

Department	Action
Managed Services Management	To notify IRIS Software Group HR revoke log in credentials from internal systems required for role.
IRIS Software Group HR	Notify's IT to revoke access to internal systems and HR systems.
IRIS Software Group IT	To close off network access, organise recovery of assets, revoke other access (Office 365 account and VPN access).

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

- Full removal of access to any part of the corporate network prior to departure.
- All corporate assets in that person's possession having been returned and or been collected by the relevant Department manager or the Information asset Owner as appropriate.
- In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

Employees have been contracted to a non-disclosure clause in their contracts that remains applicable after termination.

Payroll managing services tasks may be processed by our India outsourcing function.

4.0 PSI PAYROLL SERVICES INC. by IRIS ACCESS CONTROL

Access is granted on the least privileged rule basis consistent with an individual's job/role responsibilities. For PSI Payroll Services Inc. by IRIS 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 SoftwareGroup's Acceptable usage policy. Passwords must not be disclosed to colleagues or any third parties. As set out in the IRIS Software Group'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 Group's IT Department and PSI Payroll Services Inc by IRIS' users are 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 IRIS Software Group IT team in conjunction with the Infrastructure 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.

4.1 Password and Authentication Policy

This policy describes the authentication requirements for accessing internal computers and 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 PSI Payroll Services Inc. by IRIS's computer systems, networks, and information resources.

4.2 How we transmit confidential information to clients

Dependent on the service provided, PSI Payroll Services Inc by IRIS utilises several proprietary secure document sharing portals (Citrix Content Collaborator and/or DocuSign) to transmit client personal data between the client and PSI Payroll Services Inc by IRIS, we also send password protected documents issued by email.

4.3 Media Handling

Media Handling	Description
Management of removable media	PSI Payroll Services Inc by IRIS sets out the acceptable usage of removable media in Information security and acceptable use summary Policy. It is not permitted to create a copy of protected data on unauthorised devices.
Disposal of media	PSI Payroll Services Inc by IRIS sets out responsible use of data in our IRIS Software Group Data Protection Policy, including secure disposal and audit of media.

5.0 OPERATION SECURITY

Operations Security	Description
Change management	Change management controls have been implemented to ensure satisfactory control of all changes. Major architectural changes are reviewed by an architecture review board (ARB) to discuss security, service level and complexity issues.
Capacity management	Resources are monitored, tuned and protections made of future capacity requirements to ensure systems continue to perform at optimum levels.
Protection from malware	PSI Payroll Services Inc. by IRIS utilises Defender and Carbon Black, to protect against malicious software and this is centrally monitored. All Employees machines are auto updated on connection to the network or via internet. Firewalls are in place. Mimecast is used to provide comprehensive email filtering (not only to preclude spam but also to scan attachments more effectively to counteract viruses and other malware).
Back-ups	All data is backed up nightly in the Microsoft Azure environment for the Canada East Region.
Clock synchronisation	IRIS Software Group IT controls clock settings, ensuring that synchronisation is enabled to a real time clock set at local standard time.

Restrictions on software installations	IRIS Software Group IT regularly review acceptable use and monitor or restrict installations that have not yet been deemed safe. Requests to install new software must be authorised by IRIS Software Group IT if not already placed on a safe list.

6.0 COMMUNCIATION SECURITY

Communications Security	Description
Network security	All integrated web-applications are maintained and tested to a high standard of security. The integrity of client data is ensured through a quality hosted environment that holds more than appropriate accreditation outlined within this document.
Security of network services	We employ the use of Cloud-Based Technology that houses personal data in Canadian Data Centres hosted by Microsoft Azure, that uses world class security protocols to ensure security compliance (accreditation details in 'Organisational Security' section). As an additional layer of complexity, only employees granted access to view this data can only do so through the use of an internal group VPN. These controls are reviewed annually.
Segregation of networks	PSI Payroll Services Inc. by IRIS has its own subscription in Microsoft Azure which separates itself from other areas of the IRIS Group's wider network . In addition, controls are in place to ensure that only authorised persons have access to these drives.
Electronic messaging	PSI Payroll Services Inc. by IRIS employees are subject to audited training on appropriate use of electronic communication, particularly with sensitive and/or personal information

7.0 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Security in Development and Support Processes	Description
System change control procedures	Major system changes are reviewed by the Architectural Review Board (ARB).

Technical review of applications after operating platform changes	IRIS Software Group tests all product updates against a range of supported environments and software. Regression testing is completed to review the overall product impact of any system changes.
Restrictions on changes to software packages	Changes to software development inhouse is subject to change control procedures.
Secure system engineering principles	Principles for engineering secure systems have been established, documented, and maintained by the IRIS Software Group's architecture team and are used as part of an internal training plan for all developers (Architecture Corpus).

8.0 SUPPLIER RELATIONSHIPS

8.1 IRIS Software Group Entities

PSI Payroll Service Inc. by IRIS	Description:
IRIS KPO India	Payroll managing services tasks may be processed by our India outsourcing function. IRIS KPO use our internal secure IRIS VPN connection. The same VPN connection as our Employees in Canada. A detail risk assessment is carried out annually to ensure continue process review of security requirements.
WinLedge	Payroll Software used to process the clients' payrolls.
Microsoft Azure	Payroll Software and client data is held in a Microsoft Azure hosted environment in Canada East Region.

9.0 INFORMATION SECURITY INCIDENT MANAGEMENT

9.1 Management of information security incidents and improvements

In all instances, any information or payroll critical incidents (whether relating to information security or not) are managed through the "Critical Incident Management Process", handled and coordinated by the IRIS Critical Incident Manager. Incidents are prioritised and classified as part of this process. The process outlines stakeholder communication with a focus on customer communication during an incident resolution. A post incident review is then drawn up by the software manager and / or product manager and corrective actions are logged and tracked to execution.

Information security incidents must follow this process, but in addition will be triggered by the Group Data Protection Officer. The IRIS Group Data Protection Officer will report a summary of all data protection incidents to the IRIS Information & Security Governance Group 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. This process will also be used internally for any issues discovered during development, and training is provided for staff to promote awareness of this process.

10.0 BUSINESS CONTINUITY – INFORMATION SECURITY ASPECTS

10.1 Information security continuity

Information Security Continuity	Description
Planning information security continuity	During adverse situations, PSI Payroll Services Inc. by IRIS has a number of secure ways to ensure the continuity work carried out. All processors and managers are laptop users with access to the IRIS Software Group's secure VPN. The installation of 3rd party software is strictly controlled with appropriate auditing in place detailed throughout this document.
Implementing information security	We also utilise the Working From Home Procedures policy and Acceptable Usage policy.
Verify, review and evaluate information security continuity	PSI Payroll Services Inc.by IRIS review all policies as often as required but no less than once per year.

10.2 Redundancies

Redundancies	Description
Availability of information processing facilities	All systems and data have been loaded into secure cloud based desktop environments (Microsoft Azure) to ensure continuity. We are able to move instances with ease using backups of the environment and a final redundancy available on the internal network accessible only through the IRIS Software Group's VPN.

11.0 COMPLIANCE

11.1 Compliance with legal and contractual requirements

Legal and Contractual Requirements	Description
Identification of legislation and contractual requirements applicable to PSI Payroll Services Inc. by IRIS	Within the scope of the role performed, processors, managers and software provisions will defer to Federal and Provincial regulations. PSI Payroll Services Inc. by IRIS makes every effort reasonable to inform its clients of any major changes to legislation within these areas.

Privacy and protection of personally identifiable information	Covered within PSI Payroll Services Inc. by IRIS' Data Protection Policy both at local and group level.

Categories of personal data processed as part of the PSI Payroll Services Inc. by IRIS provision:

- **Trade Union Membership** – identifiable through deductions made to employees.
- **Information relating to criminal convictions and offences** – identifiable though court order fines processed through payroll.

Categories of data subjects under the PSI Payroll Services Inc. by IRIS provision:

- **Employees** – identifiable through payroll processing.
- **Trainees** – identifiable through payroll processing (apprenticeships) .
- **Next of Kin** – identifiable on rare occasion where beneficiary payment needs to be made through payroll.
-

13.4 Location of personal data processing

All personal data is held within payroll software databases and on electronic documents from client communicating this data to PSI Payroll Services Inc. by IRIS. In all instances, information is held on secured network drives held in the Canada and only accessible by those authorized to process it.

PSI Payroll Service Inc by IRIS may use IRIS Software Group Employees in India as processors of this data. All relevant security requirements have been addressed and further information may be requested. A full risk assessment is carried out annually to ensure that client data is always protected.

12.0 AVAILABLE APPENDICES

Details	
Microsoft Azure	https://docs.microsoft.com/en-us/azure/compliance/
IRIS KPO Assurance Statement	Available on Request
IRIS KPO Risk Assessment	Available on Request
IRIS Group Data Protection Statement	Available on Request
IRIS Group Working from Home Policy	Available on Request
IRIS Group Acceptable Use Policy	Available on Request
IRIS Group Personal Data Incident Reporting and Investigation Procedure	Available on Request