IRIS Payroll Professional's myePayWindow and ePayslips Service

IRIS Payroll Professional's myePayWindow and ePayslips service provides a self-service payslip and payroll collaboration facility that enables Employees and Employers to access their payslips, P60's or P11Ds directly from a secure web site, thereby reducing costs and offering the highest level of service 24 hours a day, 365 days a year.

myePayWindow offers a significant upgrade and extension to the existing ePayslips service, which we originally pioneered over 11 years ago. All existing ePayslips users are expected progressively to migrate to the myePayWindow service and so take advantage of the new features available. It is intended that myePayWindow will effectively supercede the ePayslips Service once that migration has been completed.

As before, the ePayslips data is transmitted from the IRIS Payroll Professional software up to a single secure ePayslips database over SSL (both services share the same ePayslips database). From there it can be accessed via the ePayslips and/or the myePayWindow sites.

In addition, however, the myePayWindow service and site allows the Service Provider and Employer securely to exchange various payroll documentation and to notify one another when this happens.

The Service Provider is able to publish and notify when IRIS Payroll Professional Software generated reports (including P60's, P11d's and Auto-Enrolment letters) are sent directly to the Employer user's myePayWindow account and respectively also to their Employees. Employers are able to upload various documents and notify the Service Provider when such documents are waiting for their attention. All traffic, to and from, myePayWindow is transmitted via HTTPS using SSL certified by DigiCert in accordance with Advanced Encryption Standard AES_128/256 and all data and documents are encrypted at rest using Transport Data Encryption AES_128.

All posted documentation will be automatically deleted after 3 months but Auto Enrolment letters, ePayslips, P60's and P11d's will be held for at least 12 months and thereafter may only be deleted by IRIS on expiry of reasonable prior notice given to the Service Provider or Employer as appropriate.

Hosting for both IRIS Payroll Professional's myePayWindow and ePayslips services is exclusively UK based, and managed by Rackspace Limited. Their certifications include ISO27001, AICPA-SOC (formerly known as SAS70) and PCI-DSS. For the avoidance of doubt, IRIS has ensured that its engagement of Rackspace as a sub-processor fully conforms to the provisions contained in Article 28 of the GDPR.

Once they have created a myePayWindow account, Employer users and Employees can self-administer password and username resets. Assistance with account resets can be provided by the Service Provider as required, and this assistance is facilitated either via the

IRIS Payroll Professional Software or the Employer's own myePayWindow account. Each Employee during registration on myePayWindow will be required to confirm Consent online for its use and will also have the option to withdraw Consent at any time whereupon the Employee's account will immediately be closed.

The myePayWindow and ePayslips Service only use session cookies. These are not persistent, are used for security purposes and do not cross between sessions.

IRIS Payroll Professional's own internal processes and procedures are also certified to ISO27001 and access to the ePayslips and myePayWindow servers and applications for administration and support is limited by IP address and to two named individuals, one each at Star's Brighton and Leeds offices, such access is over a VPN, controlled and audited by Rackspace Limited.

PCI accredited vulnerability testing is run on a regular weekly basis and penetration testing on a yearly basis, conducted by Netcraft Ltd of the world's leading Web Application Testing specialist organisations.

Availability

IRIS does not guarantee that access will be available to the myePayWindow and ePayslips Services at all times owing to Internet service interruptions and the need to maintain and upgrade software. However, IRIS will use best endeavours to ensure that the services will be available at least 98% of the time within each calendar month between the hours of 8.00 am and 8.00 pm (''the myePayWindow and ePayslips Service Hours''). It can be anticipated that the period of greatest use of the Services is between the 21st of the month and the 5th of the following month. IRIS therefore ensures that routine maintenance and, wherever practicable, upgrades avoid this critical period so that such work is undertaken between 6th and 20th of any month and also conducted outside the myePayWindow and ePayslips Service Hours.

Continuity

IRIS has in place appropriate business continuity procedures (including daily backups) and provides for disaster recovery facilities in respect of separate physical servers using virtual server technology to be able to failover in the event of an individual virtual machine or hardware failure. This involves the use of VMWare Clustering and SAN technology. IRIS hereby confirms that the availability contained in the service level agreement terms provided by Rackspace Limited includes 100% availability of the network and repair of any problem hardware component within one hour of identification, additional time may be required to rebuild a RAID array or to reload operating systems and or applications.

Rackspace Managed Hosting

Physical Security

Physical Security includes locking down and logging all physical access to the Rackspace data centre.

- Data centre access is limited to only authorised personnel
- Badges and biometric scanning for controlled data centre access 24x7 security camera monitoring at all data centre locations Access and video surveillance log retention
- 24x7 onsite staff provides additional protection against unauthorised entry
- Unmarked facilities to help maintain low profile
- Physical security audited by independent firms annually

Network Infrastructure

Network Infrastructure provides the availability guarantees backed by aggressive SLAs.

- High-performance bandwidth provided by multiple network providers Elimination of single points of failure throughout shared network infrastructure
- Cables properly trunked and secured
- Proactive network management methodology monitors network route efficiency
- Real-time topology and configuration improvements to adjust for anomalies
- Network uptime backed by Service Level Agreements
- Network management performed by only authorised personnel
- Virus and Malware protection provided by Sophos
- Cisco firewall technology provides protection from Internet and Rackspace public network

Human Resources

Human Resources provides Rackspace employees with an education curriculum to help ensure that they understand their roles and responsibilities related to information security.

- Reference checks taken for employees with access to customer accounts
- Employees are required to sign non-disclosure and confidentiality agreements
- Employees undergo mandatory security awareness training upon employment and annually thereafter

Operations Security

Operational Security involves creating business processes and policies that follow security best practices to limit access to confidential information and maintain tight security over time.

- ISO 27001/2 based policies, reviewed at least annually
- Documented infrastructure change management procedures
- Secure document and media destruction
- Incident management function
- Business continuity plan focused on availability of infrastructure
- Independent reviews performed by third parties
- Continuous monitoring and improvement of security program

Environmental Controls

Environmental Controls implemented to help mitigate against the risk of service interruption caused by fires, floods and other forms of natural disasters.

- Dual power paths into facilities
- Uninterruptable power supplies (minimum N+1)
- Diesel generators (minimum N+1)
- Service agreements with fuel suppliers in place
- HVAC (minimum N+1)
- Smoke detectors
- Flood detection
- Continuous facility monitoring

Security Organisation

Security Organisation includes establishing a global security services team tasked with managing operational risk, by executing an information management framework based on the ISO 27001 standard.

- Security management responsibilities assigned to Global Security Services
- Chief Security Officer oversight of Security Operations and Governance,
- Risk, and Compliance activities
- Direct involvement with Incident Management, Change Management, and Business Continuity.