Star's ePayslips Service

Star's ePayslips service provides a self-service payslip facility that enables employees 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. Payslip, P60 and P11D information is automatically uploaded to the secure website from Star's Payroll Professional software run either by the employees' Employer or its Payroll Service Provider ("the Client"), and once there, employees are able to access their own payslips (both current and historic) without the need to revert to the payroll department. Employees without a PC or Smartphone and internet access or otherwise preferring traditional payslips, can continue to have paper ones produced by the system in the normal manner.

Rackspace Limited provides dedicated UK based hosting for Star's ePayslips service and certifications include ISO27001, AICPA-SOC (formerly known as SAS70) and PCI-DSS. The ePayslips data is transmitted from the Star Payroll software over SSL up to the secure ePayslips site where the ePayslips SQL database is encrypted using Transparent Data Encryption with Advanced Encryption Standard AES_128.

The Client is advised that on first publishing an ePayslip for an Employee, the software generates and assigns a unique 12 digit Employee ID and 8 character Password for such Employee to access the ePayslips Software (the "Login Identifiers"). It is the Client's responsibility to distribute the Login Identifiers to the relevant Employers and Employees and to manage any administration necessitated by any Employer or Employee losing or forgetting any Login Identifier(s). Subject to matching key private information an employee has previously entered, the employee can obtain a replacement temporary PIN directly from ePayslips which they will be forced to change on first use. The ePayslips service does use cookies but only session ones to maintain security settings whilst the user is in a session. These do not cross between sessions.

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

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

Availability

Star does not guarantee that access will be available to the ePayslips Service at all times owing to Internet service interruptions and the need to maintain and upgrade ePayslips software. However, Star will use best endeavours to ensure that the service 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 ePayslips Service Hours"). It can be anticipated that the period of greatest use of the ePayslips Service is between the 21st of the month and the 5th of the following month. Star 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 ePayslips Service Hours.

Continuity

Star 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.

Star 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.

Data

Star is a registered data controller under the Data Protection Act 1998 and will retain data hosted upon the website in the UK for a period of twelve months after the date of upload. After this period Star reserves the right to delete all such data upon expiry of reasonable prior notice being given by Star to the Client. Brexit notwithstanding, Star intends also to comply with the EU GDPR regulations prior to their coming into force in May 2018.

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.