Information Security Schedule

Direct customers · Version 2.1 · Effective 6 November 2026

Flow Payroll (AIPayroll Limited) — security controls and incident response

1) Overview

This Schedule sets out the technical and organisational security measures operated by the Supplier in respect of the Services. The Supplier's infrastructure is hosted on Amazon Web Services (AWS), which maintains recognised, independently audited security certifications for the underlying infrastructure. The Supplier may update, replace or enhance these measures from time to time, provided that the overall level of security is not materially reduced.

2) Definitions

In this Schedule, capitalised terms not defined below have the meanings given in the MSA or the DPA. The following definitions apply in this Schedule and wherever these terms are used elsewhere in the Agreement:

a) **Disaster:** an event that makes the Services unavailable from the primary hosting region and which the Supplier declares to be a disaster for the purposes of its disaster-recovery arrangements.

b) **Good Industry Practice:** the degree of skill, care, prudence and foresight reasonably expected of a skilled and experienced provider of similar software-as-a-service payroll services in the United Kingdom.

c) **Incident:** any actual or reasonably suspected unauthorised access to, or loss, disclosure or corruption of, Client Data, or any event that materially compromises the security or availability of the Services.

d) **Mitigate:** to take reasonable steps to prevent, reduce the likelihood of, or limit the impact of an Incident, and "Mitigation" shall be construed accordingly.

e) **Recovery Point Objective (RPO):** the targeted maximum period of data loss, measured back from the time of a Disaster.

f) **Recovery Time Objective (RTO):** the targeted period within which the Services are restored following a Disaster.

g) **UK Business Hours:** has the meaning given in the Service Level & Support Schedule.

3) Hosting and infrastructure

a) Services are hosted on AWS, with personal data primarily stored and backed up in the AWS Ireland (eu-west-1) region, and a disaster-recovery environment in the AWS London (eu-west-2) region.

b) AWS provides physical and environmental security for the underlying data centres under its own certifications; the Supplier does not operate its own data centres.

c) Infrastructure is provisioned and managed as code, with segregation between production and non-production environments.

4) Access control

a) Access to production systems and personal data is restricted to authorised personnel on a least privileged, role-based basis.

b) Multi-factor authentication (MFA) is enforced for access to production systems and administrative interfaces.

c) Access is provisioned on joining, reviewed periodically, and revoked promptly on role change or departure.

d) Individual named accounts are used; shared credentials are avoided.

5) Encryption

a) Personal data is encrypted in transit using TLS, and at rest using AES-256 or stronger encryption.

b) Encryption keys are managed through AWS Key Management Service (KMS).

6) Backups and recovery

a) Encrypted backups of production data are taken on a regular automated schedule and retained for 35 days.

b) A disaster-recovery environment is maintained in a separate AWS region (London), enabling recovery in the event of a primary-region failure.

c) Recovery objectives and procedures are documented; backup restoration is tested.

7) Vulnerability and patch management

a) The Supplier monitors security vulnerabilities and applies critical security patches within 30 days of release (and more urgently for actively exploited critical issues).

b) Dependency and infrastructure vulnerability scanning is performed on a regular basis.

c) Anti-malware protection is applied to relevant systems.

8) Secure development and change management

a) Security is considered in design and development (security-by-design); changes are peer-reviewed and subject to automated testing before deployment.

b) An iterative release process with rollback capability and production monitoring is operated.

9) Logging and monitoring

a) Security-relevant events are logged, and infrastructure is monitored with alerting for anomalies and availability.

b) An audit log of security-relevant actions is also maintained.

10) Incident response

a) The Supplier operates an incident management process covering identification, containment, remediation and communication.

b) Personal data breaches are handled in accordance with the DPA, including notification to the Client without undue delay and in any event within 24 hours as set out in the DPA, to enable the Client to meet its own obligations.

c) A root-cause analysis is provided for material incidents.

11) Business continuity

a) The Supplier maintains business continuity and disaster-recovery arrangements appropriate to a payroll service, including the cross-region DR environment described above, to maintain continuity of statutory payroll processing.

b) The Supplier targets a Recovery Time Objective (RTO) of 24 hours during UK Business Hours and a Recovery Point Objective (RPO) of 1 hour following a Disaster. These are targets, not guarantees.

12) Sub-processors and supplier security

a) The Supplier's sub-processors are set out in the DPA. Material sub-processors (including AWS) are subject to their own security certifications and contractual data-protection obligations.

13) AI and machine-learning security

a) The Supplier applies data minimisation to inputs to AI and machine-learning tooling so that identifiable Payee Data is not deliberately provided to third-party AI providers.

b) AI and machine-learning providers are treated as sub-processors under the DPA, and the Supplier will give the Client notice of any material change to its AI sub-processors in accordance with the DPA.

c) These measures are designed to accommodate the ongoing development of the Supplier's products and do not limit the Supplier's ability to improve or change its AI tooling, provided the protections in this section are maintained and subject to the notice and objection provisions of the DPA.