Flux

Flux Fact Sheet

Security

We understand that clients care deeply about information security. We do too. That's why we take significant measures to protect your information and the information of your customers. How do we do that? Read on.

PROTECTING YOUR DATA

We're committed to the security of our customers' data and provide multiple layers of protection for the personal and financial information you trust to Flux.

Controls around our people

Our hiring criteria are stringent, and we hire only competent and experienced professionals, with a passion for excellence in their work. We vet and background-check our employees prior to employment. Our crew sign confidentiality agreements which endure long after they move onto new pastures. Our off-boarding and access management processes are designed to ensure that crew access is restricted only to systems and data they need in order to provide you with the excellent service you expect from us. Access is secured using 2 factor authentication (2FA).

We utilise the principles of 'least privilege', allowing access to privileged accounts only for the duration of the task requiring it, and 'segregation of duties' whereby no individual is able to complete a critical transaction end-to-end on their own. Crew activity on systems is monitored and logged, and we alert on anomalous behaviours.

Controls available to your staff

We offer the ability to grant your staff access appropriate to their role (RBAC). Client logins are protected by 2 factor authentication (2FA) to make their access more secure. All staff activity on the platform is logged.

Data encryption

All web, API and mobile traffic data is encrypted in transit using industry-standard protocol Transport Layer Security (TLS) at a minimum version of 1.2, protecting your personal and financial data. Your data is also encrypted at rest when it is stored on our servers, and encrypted when we transfer it between data centres for backup and replication. We support a number of backend third party integrations all of which support encryption. We apply disk level encryption for all our data.

Infrastructure protection

Flux takes a “defence in depth” approach to protecting our systems and your data. Multiple layers of security controls protect access to and within our environment, including firewalls and network segregation. Flux's security services are configured, monitored and maintained according to industry best practice. We partner with industry-leading security vendors to leverage their expertise and global threat intelligence to protect our systems. We tightly control all outbound connectivity and alert on any anomalies.

Secure infrastructure

Flux runs in Amazon Web Services (AWS) making full use of the AWS Shared Responsibility Model for security. AWS provides excellent best-in-class security from their data centres, through to their services. Providing a strong foundation on which to build secure applications.

Security monitoring

Flux's Security team continuously monitors security systems, event logs, notifications and alerts from all systems to identify and manage threats. We have regular vulnerability scanning in place alongside regular patching. In addition we perform regular penetration tests of our website, Admin App and Mobile Applications. We utilise static and dynamic vulnerability scanning technology to regularly scan our environments. We regularly perform penetration testing of our solution, covering all external facing solutions.

Email Security

Outgoing emails are verified via use of SPF and DKIM and are sent via Send Grid.

Secure development

We utilise the principles of Security by Design, with security considerations at every gateway in the development process. We utilise code reviews, dependency version scanning and regular patching to ensure our code stays up to date. All changes go through a rigorous Change Management process.

Passwords

Passwords stored in our database are salted and hashed using the BCrypt function. Our public facing website enforces a password of 8-72 characters, with passwords screened against a known compromised password database. Accounts are locked after 5 invalid attempts. The Mobile App hands off to the public site for credentials creation. Changing a password can only be done via the public facing website; the mobile app does not support this. Mobile App users can create a 4 digit pin to allow opening of the App. Fingerprint authentication is also supported if a pin has been set up by the App User. Operator users can set up MFA in addition to the password criteria above.

DDOS protection

Flux regularly reviews its DDOS protection and processes to ensure that we remain secure from attack. We have an established relationship with CERT NZ, the government funded Computer Emergency Response Team, set up to help Businesses and Organisations to help combat Cyber Security Incidents. Flux is undertaking work this calendar year to improve its DDoS protection but in place today is AWS Shield - Advanced.

GDPR Compliance

Flux meets the GDPR regulations for all of the countries we operate in and ensures changes are made to the product as any policy is changed.

ALWAYS READY

We know the importance of keeping your platform running smoothly at all times so we build our technology to enable this continuity.

Best in class availability

Flux delivers best-in-class availability. We use multiple redundancy technologies for our hardware, networks, data centres and infrastructure. These ensure that if any component fails, Flux will keep on running – with little or no disruption to your service.

Built to perform at scale

Flux has been designed to grow with your business. Our high performance servers, networks and infrastructure ensure we can deliver quality service to you and our hundreds of thousands of other users.

Disaster recovery and readiness

Flux performs real-time data replication between our geographically diverse, protected facilities, to ensure your data is available and safely stored. This means that even should an unlikely event occur, such as an entire hosting facility failure, we can switch over quickly to a backup site to keep Flux and your business running. We transmit data securely, across encrypted links. We have robust Incident Management and Business Continuity processes in place, which we periodically test. In addition to our systems being geographically diverse, we also make sure that we have skilled staff operating from geographically diverse locations at all times.

Constant updates and innovation

We're constantly enhancing Flux, delivering new features and performance improvements. Updates are delivered frequently, with the majority of them being delivered without interrupting our service nor disrupting users.

SECURITY ASSURANCE

Flux Federation is certified as compliant with ISO/IEC 27001:2013 which is globally recognized as the premier Information Security Management System (ISMS) standard. We achieved certification by developing and implementing a robust security management programme, and demonstrating that effective security controls and policies are in place.

Flux complies with the Payment Card Industry Data Security Standard: PCI DSS v3.2, SAQ D.