FLUXX

SECURITY CONTROLS AND INFRASTRUCTURE MANAGEMENT

FLUXX.IO

Infrastructure and Access Management

Fluxx's commitment to security is demonstrated through comprehensive controls and practices that protect both our Grantmaker platform and corporate infrastructure. Our asset management strategy provides complete visibility across our technology landscape, with endpoint assets monitored through an enterprise Mobile Device Management (MDM) system that tracks asset location, patch levels, and system utilization. In our cloud infrastructure, we leverage AWS's native management console to maintain oversight of all systems and services within the Grantmaker production environment.

Our security framework begins with stringent access control measures that combine managerial oversight with information security team governance. User access is carefully managed throughout the employee lifecycle, beginning with a structured onboarding process where appropriate role-based access is allocated through our ticketing system. Access termination is equally rigorous, with complete access removal executed within 24 hours of employee departure. To maintain access hygiene, we conduct quarterly access reviews to validate all user permissions.

Threat Protection and Monitoring

Protection against malware and other security threats is achieved through a multi-layered approach. All endpoint devices are secured with SentinelOne anti-malware solution, with mandatory installation enforced through MDM and daily signature updates. The Grantmaker production environment benefits from comprehensive security measures including virus scanning for all file uploads, AWS Intrusion Detection System, and AWS GuardDuty for rapid threat detection and response. Our vulnerability management program leverages GitHub's Dependabot for daily vulnerability assessments of both application code and containers, with findings tracked and managed through Jira tickets. Production environment security is continuously monitored through AWS GuardDuty, with all identified issues tracked to resolution.

Security event logging and retention is implemented through AWS CloudWatch and CloudTrail, with logs retained for a minimum of one year. Our Global administrator support tool maintains indefinite log retention, ensuring comprehensive audit capabilities. Endpoint management is streamlined through Rippling MDM, enabling centralized control over endpoint tracking, patching, and software deployment across our corporate environment. All patches undergo pre-deployment validation before distribution to production endpoints.

Engineering Standards and Customer Security

Our commitment to security extends to our vendor relationships, with all tools and vendors undergoing thorough security assessment prior to adoption. Annual reassessments ensure continued compliance with our security requirements. Through this comprehensive vendor management process, we maintain consistent security standards across our entire technology stack.

System deployments follow rigorous engineering standards, with all systems configured to meet NIST 800-53 moderate controls and OWASP Top 10 security requirements. Server deployments are governed by standardized baseline configurations maintained in Terraform, ensuring consistent security controls across the Grantmaker environment. Customer security is paramount, with access to Grantmaker environments strictly controlled through role-based access control (RBAC) mechanisms within designated tenants. This granular access control is managed by primary privileged accounts within each customer tenant, ensuring appropriate separation and security of customer environments. Through these comprehensive security measures, we maintain the integrity and security of both our corporate infrastructure and the Grantmaker platform, providing our customers with a secure and reliable service.

Cloud Security Controls

Security & Compliance Measures

Fluxx operates as a remote-first company, relying on Amazon Web Services (AWS) for physical security and environmental controls. AWS facilities are designed with security in mind, featuring fortified structures, strict access controls, and advanced surveillance systems. The infrastructure is monitored around the clock, with intrusion detection and access management systems ensuring unauthorized personnel cannot gain entry. Further details on AWS's security measures can be found on their official site.

To protect against cyber threats, Fluxx utilizes AWS GuardDuty, an intelligent threat detection service that continuously monitors AWS accounts, workloads, and data. If malicious activity is detected, GuardDuty generates real-time alerts for rapid response. Additionally, AWS Shield provides protection against Distributed Denial of Service (DDoS) attacks, ensuring continuous application availability.

Fluxx's application environment follows best practices for vulnerability management. The system undergoes continuous scanning, and Kubernetes-based infrastructure ensures that containers remain ephemeral, reducing the risk of persistent threats. User-uploaded f iles are scanned for malware to provide an added layer of security. In the event of an incident, Fluxx employs a comprehensive set of management tools, including AWS GuardDuty, AWS CloudTrail, PagerDuty, Jira, Slack, and Statuspage.io, ensuring a streamlined and efficient response.

Reliability & Data Protection

Fluxx has engineered its infrastructure for high availability and disaster resilience. AWS's Multi-AZ architecture ensures that production databases remain available even in the event of an outage, with automatic failover configurations in place. Load balancers distribute traffic efficiently, rerouting requests to healthy instances when failures are detected. Additionally, weekly global data backups are stored in AWS S3, allowing for full recovery even in the unlikely event of a regional failure.

To further enhance reliability, all static media, generated reports, and attached documents are stored securely and automatically replicated across multiple failover locations. Systems are regularly tested through annual disaster recovery exercises to ensure operational continuity. Customer data stored in AWS RDS can be restored to a prior point in time, allowing rollbacks in five-minute increments for up to 30 days.

Infrastructure & Data Handling

Fluxx's cloud infrastructure is fully hosted on AWS, utilizing a robust technology stack that includes AWS Route 53 for DNS management, AWS S3 for document storage, AWS EKS for container orchestration, and AWS RDS for database management. The search functionality is powered by AWS OpenSearch, while secrets and sensitive credentials are securely stored in AWS Secrets Manager. The application runs on Ubuntu, with Apache and Puma serving as the web servers. The development framework of choice is Ruby on Rails, ensuring a scalable and maintainable architecture.

Fluxx follows strict data destruction policies, aligning with AWS's high-security standards. Media storage devices containing customer data are classified as critical and securely decommissioned following NIST 800-88 guidelines. No storage media leaves AWS's control until it has been securely wiped or physically destroyed. Additionally, for customers using US-based infrastructure, all physical access to customer data is managed exclusively by AWS, with data centers located in North Virginia.

At Fluxx, we remain committed to maintaining the highest standards of security, reliability, and resilience for our customers. By leveraging AWS's advanced infrastructure, continuous monitoring, and stringent data protection measures, we ensure that customer data remains secure while delivering a seamless application experience.

Application Security and Release Practices

At Fluxx, safeguarding our customers' data and ensuring the reliability of our platform is at the core of our development and operations practices. Security is never an afterthought — it is built into every phase of our Software Development Life Cycle (SDLC), release management processes, and ongoing monitoring activities. Our goal is to provide customers with a platform that doesn't just meet their functional needs, but also delivers the confidence that their data is protected by mature, industry-aligned security practices every step of the way.

Secure Development, Structured Releases, and Responsible Patching

Fluxx's development process follows a Scrum-based SDLC, incorporating acceptance criteria and definition of done checklists to ensure each feature or enhancement is fully validated for functionality, performance, and security before deployment. All code is managed through Git, hosted securely on GitHub, where every change undergoes peer review, automated testing, manual quality assurance, and continuous integration checks. This disciplined process ensures not only the delivery of high-quality software, but also maintains a strong security baseline that evolves with each release.

To balance the delivery of new capabilities with the need for stability, Fluxx follows a predictable release cadence. Customers on our Standard Cloud Offering can expect updates every two weeks, while those on the Enterprise Cloud Offering receive new releases on an eight-week schedule designed to better support complex environments. These scheduled releases occur Wednesdays, outside core business hours, helping customers plan with confidence and minimizing any potential impact on their users.

Fluxx employs zero-downtime deployments by default, ensuring that enhancements, fixes, and new features become available seamlessly. On rare occasions, when maintenance requires temporary downtime, customers are given ample advance notice through in-application messaging and updates to our knowledge base. This transparent approach ensures that customers always feel informed and in control.

While regular releases follow a well-structured process, Fluxx also recognizes the need to move swiftly when urgent issues arise. Out-of-cycle patches may be deployed to address critical security vulnerabilities, support urgent troubleshooting efforts, or resolve regressions where previously functioning features are affected. Even with accelerated timelines, these patches follow the same rigorous quality and security processes as regular releases, ensuring they are thoroughly reviewed, tested, and validated before deployment. To maintain transparency, all patches are documented in our release notes once they are live. For security patches, Fluxx follows responsible disclosure best practices, ensuring that details are only published once all affected environments are secured and the issue fully mitigated. This approach protects our customers while maintaining the transparency and trust they deserve.

Proactive Monitoring, Data Protection, and Secure Testing Practices

Fluxx's commitment to security doesn't end when a release goes live. Our platform is continuously monitored using Intrusion Detection Systems (IDS) and real-time logging alerts, providing immediate visibility into potential threats so they can be investigated and addressed before they impact customers. This proactive stance reflects our belief that security is not just about defense, but about constant vigilance and continuous improvement.

We also recognize that many customers want to test upcoming releases or configuration changes in a controlled environment. That's why Fluxx offers a pre-production environment, empowering customers to preview new functionality in a secure, isolated space. Most customers trust our rigorous quality assurance and security processes, but for those with heavily customized configurations, this added flexibility ensures they can test with confidence.

To further safeguard customer data, Fluxx follows industry best practices regarding the use of real data in test environments. For new customers and prospects, storing real customer data in pre-production is strictly prohibited. For existing customers who have already established test environments with real data, Fluxx supports this use case within the scope of our SOC 2-audited controls — though we strongly encourage the use of anonymized or synthetic data instead.

To help customers anonymize data, we recommend tools such as Mockaroo, Tonic.ai, and ARX to de-identify structured datasets before importing them into pre-production. Alternatively, customers can generate entirely synthetic datasets, which offers a fast, secure way to populate a test environment without any risk to live data. For customers seeking hands-on support with data anonymization or environment setup, Fluxx's Advanced Services Team is available to help, ensuring a smooth and secure transition to safer testing practices.

Authentication, Access Controls, and Enterprise Integration

Strong authentication and access controls are foundational to Fluxx's commitment to customer data protection. The platform provides flexible, administrator-controlled Multi-Factor Authentication (MFA), allowing customers to require a second layer of verification for all users — whether internal staff or external collaborators. Users can choose to authenticate using one-time passwords (OTPs) via phone or through trusted third-party authenticator apps, such as Google Authenticator and Microsoft Authenticator.

For organizations seeking seamless identity management, Fluxx supports SAML 2.0 Single Sign-On (SSO), enabling integration with industry-leading identity providers such as Okta, Azure AD, and Ping Identity. This allows organizations to enforce centralized identity policies, requiring that users authenticate through their existing enterprise directories rather than managing credentials directly in Fluxx. Fluxx's SAML integration only requires the NameID attribute, mapped directly to the user's sso_uid in the platform, ensuring simple configuration with robust security outcomes.

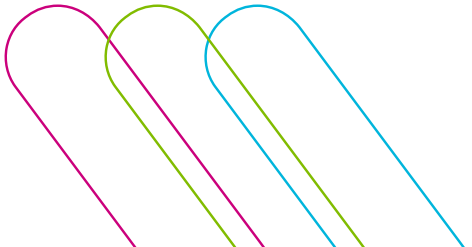
To further protect sessions, Fluxx allows administrators to configure session timeout policies tailored to their organization's security needs, automatically logging users out after a defined period of inactivity. Whether using native authentication or SAML SSO, all authentication traffic is encrypted using TLS 1.2, ensuring credentials are fully protected in transit.

Fluxx also takes great care to ensure that authentication processes fail securely, meaning that in the event of an incorrect login attempt, no sensitive account information is revealed. In addition, authentication credentials and personally identifiable information (PII) are never stored in cookies, eliminating the risk of credential leakage through common web storage mechanisms.

By combining robust development practices, responsible release processes, proactive security monitoring, and strong identity and access controls, Fluxx delivers a secure and reliable platform that customers can depend on with confidence. Our goal is to offer not just a feature-rich solution, but also the peace of mind that comes from knowing your data is protected by mature, well-audited security processes that evolve alongside emerging threats and customer needs.

Data Protections

In an era where data security is paramount, Fluxx remains dedicated to safeguarding the sensitive information entrusted to its grant management platform, Grantmaker. By leveraging Amazon Web Services (AWS) infrastructure and adhering to stringent security protocols, Fluxx ensures the confidentiality, integrity, and availability of customer data. From encryption to backup management, every facet of Fluxx's data protection framework is meticulously designed to meet the needs of grantmakers and their grantees while complying with global regulations.



Fluxx's data storage practices form the foundation of its security model. Customer data is housed within AWS's Relational Database Service (RDS), where environments are carefully segregated to accommodate regional compliance requirements. For example, European customers benefit from GDPR-compliant storage in EU-based environments, while U.S. operations adhere to TX-RAMP Level 2 standards. Access is tightly restricted, with only authorized personnel permitted to interact with production data, further reducing risks of exposure.

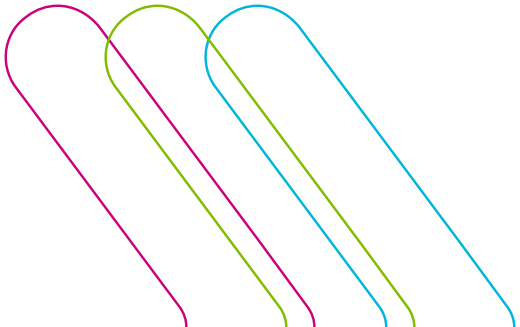
To protect the sensitive information handled within the Grantmaker application, Fluxx employs rigorous data classification and logical separation practices. Personally identifiable information (PII), such as names, organizational details, and email addresses, is managed with care. Although the system operates on a multi-tenant architecture, Fluxx ensures privacy by logically isolating customer data using tenant-specific identifiers. This approach prevents unauthorized cross-tenant access and enhances security, while any data remaining after a service agreement concludes is fully deleted within 30 days.

Encryption lies at the heart of Fluxx's efforts to maintain secure data environments. During transmission, all communications are encrypted using TLS 1.2+, while data at rest is secured through AES-256 encryption. Sensitive credentials are hashed with unique salts to prevent compromise, and all encryption keys are managed through AWS's Key Management Service (KMS), with frequent rotations to further enhance protection. These measures ensure that data remains protected both in transit and at rest.

Access controls are implemented on a global scale to provide secure, region-specific operations while adhering to international and local regulations. Fluxx authorizes personnel in approved locations, including the United States, Canada, Europe, and Latin America, to access data, ensuring compliance without sacrificing functionality. Customers are further protected by the Grantmaker platform's secure, tenant-specific login credentials, allowing only authorized individuals to interact with the application.

Resilience and availability are additional pillars of Fluxx's approach to data protection. Daily backups of production data are securely stored in AWS S3 buckets with strong encryption. These backups are retained for 30 days, after which they are permanently deleted to prevent unauthorized access. In the unlikely event of an incident, these backups enable quick recovery and restoration of customer operations.

By combining these comprehensive practices—secure storage, advanced encryption, region-specific access, and robust backups—Fluxx provides its customers with a reliable and trustworthy grant management platform. Through its dedication to compliance and innovation, Fluxx stands as a trusted partner for grantmakers worldwide, ensuring that sensitive information is protected at every stage of the process.



Artificial Intelligence at Fluxx: Responsible Innovation and Customer Trust

At Fluxx, we embrace the potential of Artificial Intelligence (AI) as a tool to enhance operational efficiency, streamline workflows, and foster innovation. As a trusted SaaS provider, our approach to AI is guided by a deep commitment to responsibility, transparency, and data security. We recognize that AI adoption must align with the highest ethical standards, ensuring that every step forward strengthens the trust our customers place in us.

Currently, Fluxx leverages AI tools such as ChatGPT Team and GitHub Copilot for internal purposes, including process optimization and software development. These tools enhance productivity within our teams, but they are not integrated into Fluxx's customer-facing application, nor do they play a role in how our platform functions. we continually evaluate emerging technologies and, should AI-based enhancements be considered in the future, they will undergo rigorous review to ensure they meet our stringent standards for security, privacy, and ethical use.

Fluxx upholds a customer-first approach to data protection, and this extends to our AI use. We do not use customer data to train AI models, and no identifiable customer data is processed through AI systems. In the limited cases where anonymized data is used within ChatGPT Team for internal functions, strict safeguards ensure privacy and security remain uncompromised. While Fluxx reserves the right to use anonymized, aggregated data for potential AI training in the future, this will always be done in accordance with our Master Services Agreement (MSA) and with a commitment to transparency.

Commitment to Responsible AI Governance

As AI capabilities evolve, we believe that responsible adoption is not just a best practice—it is essential. Fluxx's AI governance framework ensures that every tool we use, whether internally or in the future for customer-facing applications, aligns with industry-leading security and privacy standards. Today, Fluxx relies on commercial AI solutions rather than developing proprietary AI models. To ensure the integrity of these tools, we subject all AI vendors to Fluxx's Vendor Security Review process, which verifies that our partners uphold security and privacy protections comparable to our own.

Looking ahead, if Fluxx develops proprietary AI or machine learning models, we will implement a secure development lifecycle (SDLC) designed to address the unique challenges and risks associated with AI. This process will ensure that AI-driven solutions meet the same rigorous security, privacy, and ethical requirements that define all of Fluxx's technology practices.

To reinforce our commitment to trustworthy AI, Fluxx references well-regarded industry frameworks, including the Technology Association for Grantmaker's Responsible AI Adoption for Philanthropy framework and the Foundation Model Transparency Index (FMTI) from Stanford University's Center for Research on Foundation Models. These resources guide our approach to AI transparency, risk management, and ethical decision-making, ensuring we remain aligned with evolving best practices.

Security, Incident Preparedness, and the Future of AI at Fluxx

Security and resilience are central to Fluxx's approach, and AI-related risks are treated with the same diligence as any other area of our operations. AI-related incidents fall under Fluxx's comprehensive Incident Response Plan, ensuring that any security or operational concerns are addressed swiftly and transparently. Whether related to data protection, AI model behavior, or vendor security, our incident response framework provides a clear path for investigation, mitigation, and resolution.

While Fluxx has not yet engaged external experts specifically to review AI governance, we remain open to collaborating with leading security, legal, and technology experts as our use of AI evolves. This openness to external validation reflects our broader commitment: innovation must be balanced with responsibility, and security must always come first.

As we look to the future, Fluxx remains excited about the potential of AI to enhance the way we work and support our customers. Our approach will always be guided by integrity, security, and a commitment to ethical innovation, ensuring that as AI technologies evolve, Fluxx remains a trusted and responsible leader in the SaaS industry.

For more details on Fluxx's information security practices or compliance certifications, contact us at

security@fluxxlabs.com

or visit our Trust Portal.