FLUXX

SECURITY PROGRAM

FLUXX.IO

The information contained in this document reflects our current security practices and controls at the time of publication. Because our systems and processes evolve in response to changing technologies, threats, and customer needs, this document should not be interpreted as a binding commitment or guarantee.

This white paper is provided for informational purposes only and does not constitute legal, contractual, or security advice.

While Fluxx is responsible for securing the underlying platform and infrastructure, customers retain responsibility for configuring and using the platform in a secure manner, including managing user access, authentication settings, and data handling practices within their environments.

Nothing in this document grants any license or right to Fluxx's intellectual property.

Overview

Your data is sensitive—and your trust matters.
That's why we've built Fluxx as a security-first platform, combining strong technical controls, responsible innovation, and continuous oversight to protect the information entrusted to us.

Our approach to security is grounded in proven frameworks, integrated into every layer of our systems, and reinforced through ongoing monitoring and independent validation. From infrastructure to application design—and across both our Grantmaker and Grantseeker platforms—we apply consistent, risk-based controls to safeguard data and ensure reliability.

At the same time, we recognize that innovation must be handled thoughtfully. Whether introducing new capabilities like artificial intelligence or expanding across cloud environments, we prioritize transparency, customer control, and strict data boundaries.

This commitment enables us to deliver modern, flexible solutions while maintaining the highest standards of security, privacy, and trust.

Fluxx delivers our services through two complementary platforms:

- **Grantmaker**, hosted in Amazon Web Services (AWS); and
- **Grantseeker**, hosted in Google Cloud Platform (GCP).

This multi-cloud architecture enables flexibility and resilience while maintaining consistent security standards across environments. Regardless of hosting platform, Fluxx applies a unified set of security principles, controls, and monitoring practices to ensure a consistent and secure customer experience.

Security Organization and Program

Security at Fluxx is managed through a centralized Information Security program that is aligned with industry standards and best practices, including NIST 800-53 and SOC 2.

While responsibility for security is shared across the organization, a dedicated security function oversees the design, implementation, and continuous improvement of the program.

The security program is supported by a comprehensive set of policies governing access control, data protection, encryption, change management, vendor risk management, incident response, and system monitoring. These policies are reviewed regularly and are designed to evolve alongside the organization's risk profile and technology landscape.

Security leadership collaborates closely with engineering and executive teams to assess emerging risks, prioritize mitigation efforts, and ensure that security remains embedded in both operational processes and product development. This integrated approach allows us to maintain a strong security posture while continuing to innovate and scale.

Personnel Security

We recognize that our employees play a critical role in maintaining the security of our systems and data. As such, the organization has implemented structured processes to ensure that personnel are onboarded, managed, and offboarded in a secure and controlled manner.

Access to systems is provisioned based on role and business need through a formalized request and approval process. The principle of least privilege is enforced, ensuring that individuals have only the access necessary to perform their responsibilities. Access rights are reviewed on a quarterly basis to validate their continued appropriateness.

When an employee or contractor departs the organization, access to all systems is revoked promptly, and in all cases within 24 hours. This helps minimize the risk of unauthorized access following termination.

Fluxx also invests in ongoing security awareness and training, ensuring that our employees understand their responsibilities and remain informed about evolving threats. This continuous education supports a culture of security awareness across the organization.

Product Security

Security is integrated into every phase of the software development lifecycle. Engineering teams follow secure development practices aligned with recognized standards such as the OWASP Top 10, and systems are configured to meet NIST 800-53 moderate control requirements.

All changes to production systems are governed by a formal change management process that includes documentation, testing, approval, and post-deployment validation. This ensures that modifications are introduced in a controlled manner and do not negatively impact system stability or security.

To proactively identify vulnerabilities, we employ automated tools to continuously scan application code, dependencies, and containerized environments. Identified issues are tracked through a centralized system and remediated according to their severity and potential impact.

Customer data is protected through strong encryption practices. Data transmitted to and from Fluxx systems is encrypted using industry-standard protocols, while data at rest is secured using robust encryption mechanisms. Within the application, data is logically segregated by tenant, ensuring that customer environments remain isolated and secure.

Authentication, Access Controls, and Enterprise Integration

Strong authentication and access controls are foundational to how we protect customer data within the Fluxx platform. We provide flexible, administrator-controlled security capabilities across both Grantmaker and Grantseeker, tailored to the distinct architectures and use cases of each product.

Within **Grantmaker**, authentication is managed through a combination of configurable password policies and multi-factor authentication (MFA). Administrators can enforce password complexity requirements aligned with organizational standards, ensuring that user credentials meet defined security thresholds. In addition, MFA can be enabled to require a second layer of verification for all users, including both internal staff and

external collaborators. Users may authenticate using one-time passwords (OTPs) delivered via phone or through trusted authenticator applications such as Google Authenticator and Microsoft Authenticator, significantly reducing the risk of unauthorized access due to compromised credentials.

For organizations requiring centralized identity management within Grantmaker, Fluxx supports SAML 2.0 Single Sign-On (SSO) as an add-on enterprise feature. This allows integration with leading identity providers such as Okta, Microsoft Azure AD, and Ping Identity, enabling customers to enforce authentication policies through their existing identity infrastructure. Customers interested in purchasing and enabling SSO should coordinate with their Customer Success Manager or sales representative.

In contrast, **Grantseeker** is designed as a modern, passwordless platform that leverages OpenID Connect (OIDC) for authentication. This approach eliminates the need for locally managed passwords and instead relies on trusted identity providers to securely authenticate users. By delegating authentication to external identity providers, Grantseeker reduces credential management risk while enabling a streamlined and secure user experience.

Data Protection and Encryption

Customer data is stored within cloud-native managed services in AWS (Grantmaker) and GCP (Grantseeker), where it is logically segmented and associated with specific customer tenants. Although the platforms operate on a multi-tenant architecture, strict logical separation is enforced through tenant-specific identifiers and access boundaries, preventing unauthorized cross-tenant access.

Encryption is applied to safeguard data both in transit and at rest. All data transmitted to and from the platform is encrypted using industry-standard protocols (TLS 1.2 or higher). Data at rest is encrypted using strong encryption standards such as AES-256, with encryption keys managed through cloud-native key management services and rotated in accordance with established security practices.

To support data durability, Fluxx performs regular backups of critical customer data and maintains the ability to restore data to prior states when needed. Backup data is securely stored and retained according to defined policies, after which it is permanently deleted.

Customer data is retained only for the duration necessary to provide the service. Following the termination of a customer relationship, data is securely deleted in accordance with our data retention and disposal policies.

Cloud and Infrastructure Security

Fluxx operates a defense-in-depth security model across our multi-cloud infrastructure, leveraging both AWS and GCP native capabilities alongside internally managed controls.

Access to production environments is tightly controlled through role-based access mechanisms and multi-factor authentication. Administrative access is restricted to authorized personnel and is subject to monitoring and audit logging.

Network architectures are designed to limit exposure by segmenting critical systems and restricting unnecessary communication pathways. Only essential services are exposed externally, while sensitive components such as databases and internal services remain isolated within private networks.

For the Grantmaker platform, AWS-native services such as GuardDuty, CloudWatch, and CloudTrail are used to provide continuous monitoring, threat detection, and audit logging. The Grantseeker platform leverages comparable GCP-native capabilities to achieve similar visibility and control.

Across both environments, assets are inventoried and tracked, with defined ownership and security classification. Configuration management practices ensure that systems remain aligned with established security baselines.

Vulnerability Management

Fluxx maintains a structured vulnerability management program designed to identify, assess, and remediate security weaknesses in a timely manner. This program is integrated into both the software development lifecycle and ongoing operational processes, ensuring that vulnerabilities are continuously identified and addressed.

The program incorporates automated and continuous scanning of application code, infrastructure, and third-party dependencies. Vulnerabilities identified through internal tooling, independent security assessments, or operational monitoring are evaluated and

prioritized based on severity and potential impact. Findings are tracked through a centralized workflow, providing visibility and accountability across engineering and security teams. Remediation timelines are defined according to risk level to ensure that critical issues are addressed promptly.

In addition to internal processes, we also maintain a **Vulnerability Disclosure Program (VDP)** to support responsible external reporting. Security researchers and members of the broader community are encouraged to report potential vulnerabilities through designated channels. All submissions are reviewed, validated, and triaged in accordance with the same risk-based prioritization framework used for internally identified issues.

Security Monitoring and Incident Response

Continuous monitoring is a foundational component of our security program. Logs are collected from applications, infrastructure, and supporting systems to provide comprehensive visibility into system activity and potential threats. These logs are retained for audit and forensic purposes, supporting both operational monitoring and incident investigations.

Automated alerting mechanisms are in place to identify anomalous behavior, unauthorized access attempts, and potential security events. Alerts are reviewed and triaged by appropriate personnel to determine required actions.

Fluxx maintains a formal incident response program that defines roles, responsibilities, and procedures for responding to security incidents. This includes processes for detection, containment, remediation, and post-incident analysis. The program is designed to ensure that incidents are handled efficiently and that lessons learned are incorporated into ongoing security improvements.

Physical Security

As a remote-first organization, Fluxx does not operate our own data centers and instead relies on its cloud service providers, AWS and GCP, for physical and environmental security controls.

Both providers maintain highly secure facilities with robust access controls, surveillance systems, and environmental protections. These controls are designed to prevent unauthorized physical access and to ensure the reliability and safety of the infrastructure supporting Fluxx services.

We perform due diligence on our cloud providers and rely on their independently audited security controls as part of our overall security framework.

Business Continuity and Disaster Recovery

Fluxx has designed our systems to support high availability and resilience in the face of disruptions. Infrastructure is deployed across multiple availability zones, enabling continued operation even in the event of localized failures.

Data is backed up regularly, and recovery mechanisms support restoration to specific points in time. These capabilities help ensure that customer data can be recovered in the event of data loss or system failure.

A formal disaster recovery plan defines the procedures for restoring services following a major disruption. This plan is tested periodically to validate its effectiveness and to ensure that recovery objectives can be met.

Security Risk Management

Fluxx employs an ongoing risk management process to identify, evaluate, and mitigate risks to its systems and data. Risks are documented in a centralized register and are reviewed regularly to ensure appropriate prioritization and treatment.

This process considers threats from both internal and external sources, including cybersecurity risks, operational risks, and third-party dependencies. Mitigation strategies are implemented based on the likelihood and potential impact of each risk.

Third-party vendors are subject to security assessments prior to onboarding and are monitored periodically to ensure continued compliance with our security requirements.

Security Compliance

We align our security program with recognized industry standards and regulatory frameworks to ensure that our controls are both effective and independently validated. Our approach to compliance is designed not only to meet requirements, but to continuously strengthen our overall security posture.

Fluxx maintains a **SOC 2 Type II** attestation, which provides independent verification of the design and operating effectiveness of our security controls over time. This audit evaluates our controls across key trust service criteria, including security, availability, and confidentiality.

We are also compliant with **TX-RAMP (Texas Risk and Authorization Management Program)** Level 2 requirements, demonstrating our ability to meet the security standards required for serving public sector organizations and handling sensitive government data.

Our security program is further informed by **NIST-based frameworks**, including alignment with NIST CSF and NIST 800-53 controls. These standards guide the design and implementation of our policies, procedures, and technical safeguards across our environments.

We regularly review and update our controls to ensure ongoing alignment with evolving regulatory expectations, industry best practices, and customer requirements. Through this structured and proactive approach, we provide our customers with confidence that their data is protected within a secure, compliant, and well-governed environment.

Artificial Intelligence and Responsible Use

Fluxx incorporates artificial intelligence (AI) capabilities into both our Grantmaker and Grantseeker platforms to enhance user productivity and streamline workflows. These capabilities are designed with a strong emphasis on security, privacy, and customer control.

All AI-driven features within our platforms are **strictly opt-in**, ensuring customers retain full control over whether and how these capabilities are used within their environments. AI functionality is never enabled by default, and customers may disable these features at any time.

We utilize pre-trained AI models and do not train our own models on customer data. **Customer data is never used to train AI models.** Instead, Fluxx's implementation focuses on controlled prompt engineering and application-layer logic to deliver AI-powered functionality while maintaining strict data boundaries.

The development and deployment of AI features are governed by Fluxx's secure software development lifecycle (SDLC) and Responsible AI Policy. AI capabilities are subject to the same rigorous controls as all other product features, including design review, security assessment, and testing prior to release. This includes evaluation of how data is processed, how outputs are generated, and how access is controlled.

We implement safeguards to ensure that customer data remains protected when interacting with AI systems. These safeguards enforce existing data classification, access control, and tenant isolation standards, ensuring that AI functionality operates within the same security boundaries as the core platform.

In addition, we maintain internal governance processes to evaluate AI use cases and ensure alignment with ethical standards, regulatory expectations, and customer trust. AI features are monitored and periodically reviewed to assess performance, accuracy, and potential risk.

Through this controlled and transparent approach, Fluxx enables customers to benefit from AI-driven capabilities while maintaining strict data privacy and security guarantees.

We recognize that every organization has unique security requirements. If you have questions, would like to review additional materials, or want to connect directly with our security team, please reach out to us at:

security@fluxxlabs.com