# FLYWHEEL | *Security*

## *How we handle security at Flywheel*

Flywheel was founded in 2012 on a mission to create an exceptional platform to help creatives do their best work. As the leading WordPress hosting provider for thousands of the world's top creative businesses, we strive to exceed every security standard in order to keep your site secure, your data safe, and your mind at ease.

# A company built on security

We built Flywheel from the ground up with security as a core pillar of not only our platform, but our entire organizational culture. We assess how security affects code we're pushing at a micro-level, and how it affects what we're building at a macro-level. To accomplish this, we have a variety of teams and individuals dedicated to reviewing, updating, and developing industry-leading security practices across every aspect of the company.

### SECURITY AND PRIVACY TRAINING

Whether you're a summer intern or a new director of security, every single employee goes through security training during their first week at Flywheel. This training educates employees about Flywheel's security practices, covers all procedural policies that we follow, and ensures employees are held to the highest standard of professional privacy and security. We also review our internal processes so that every member of Flywheel feels confident in reporting vulnerabilities or bugs to the appropriate team or individual to address the concern as quickly as possible.

Beyond the first training, every employee is required to annually review Flywheel's security practices to ensure understanding and compliance. They're also required to acknowledge that they understand these practices and will be held accountable to the standards we've set in place.

## EMPLOYEE ACCESS LEVELS

Flywheel employees are granted access to varying internal information systems depending upon their role within the company and the training they've completed. Once granted, we use unique access identifiers in order to review who does what for maximum accountability. This allows for a level of control over Flywheel's most advanced and impactful functions and reduces the chance of internal error.

Before accessing these systems, all employees must sign a confidentiality agreement, acknowledge their understanding of Flywheel's security practices, and demonstrate compliance with the policies we've set in place. All access is removed immediately upon termination of employment at Flywheel.

## THE ROLES AND TEAMS CENTERED AROUND SECURITY

Our CTO, Tony Noecker, manages our product and engineering teams and teaches every employee in the company how to execute industry-leading practices to provide an exceptional experience for our customers. He is also a member of our cross-departmental Security Team, which consists of our CEO, CTO, COO, Customer Security Manager, and IT Specialist. The Security Team is also supported by a number of other teams centered around security solutions, including Software Engineering, Infrastructure Engineering, and Hosting Operations.

These teams work together to ensure Flywheel's security standards are upheld during every phase of development and throughout every internal process.

### SECURITY TEAM

The Flywheel Security Team is a cross-departmental effort focused on maintaining top-to-bottom security standards throughout the company. Their responsibilities include:

- **Establishing internal security and privacy standards**
- **Creating and maintaining company-wide security policies**
- **Providing ongoing security training for Flywheel employees**
- **Identifying and implementing new security strategies**
- **Monitoring security publications, news, and best practices**

## SOFTWARE ENGINEERING

The Software Engineering Team is dedicated to maintaining development standards for every line of code we push to production. They're responsible for:

- **Establishing secure development practices and standards**
- **Creating and maintaining software documentation**
- **Training engineers on industry-leading security practices**
- **Reviewing new code to ensure security and standards compliance**
- **Implementing secure technologies within all new software solutions**

## INFRASTRUCTURE ENGINEERING

The Infrastructure Engineering Team is invested in ensuring the security of code installed on our customers' sites. They're in charge of:

- **Establishing secure infrastructure practices and standards**
- **Creating and maintaining documentation about third-party vulnerabilities**
- **Training engineers on industry-leading WordPress practices**
- **Creating systems that are secure from malware**

## HOSTING OPERATIONS

The Hosting Operations Team is responsible for patching and resolving security vulnerabilities identified on customer sites. Their priorities include:

- **Patching software vulnerabilities to exceed security standards**
- **Creating and maintaining documentation around malware patterns and protection efforts**
- **Scanning for, identifying, and cleaning up malware**
- **Ensuring operational security during every update, patch, and process**
- **Notifying customers of identified vulnerabilities and necessary updates**
- **Detecting outdated WordPress themes, plugins, or other services with vulnerabilities**

## POLICIES AND STANDARDS

Flywheel upholds a number of internal policies, procedures, standards, and guidelines to ensure the highest level of security and privacy protection. These rules and trainings help employees maintain our excellent standards in both our work and organization. These security and privacy policies include (but are not limited to):

- **Acceptable uses of information systems**
- **Classification and management of security incidents**
- **Code review process for infrastructure and software engineers**
- **Documentation and records outlining security standards and policies**
- **Documentation guidelines for informational assets**
- **Encryption of application and user data at rest and in transit**
- **Fair, ethical, and legal standards of business conduct**
- **Identification, authentication, and authorization practices for system data access**
- **Organizational requirements for onboarding, transitions, training, and advancement**
- **Regular vulnerability and penetration testing**
- **Secure login credentials management**
- **Secure development, configuration, and maintenance of infrastructure systems**
- **Standardized software and hardware maintenance process**
- **Use of risk assessments, audits, and penetration tests to assess and improve upon security**

These policies are maintained and updated by the Flywheel Security Team and are available for all employees.

## SECURITY COMPLIANCE AND ASSESSMENTS

Flywheel uses a variety of internal tests to assess security during every stage of development and throughout the organization. We also adhere to the security expectations set forth by a number of organizations to meet and exceed industry standards.

### CERTIFICATIONS

Due to our dedication and transparency around security, we're proud to share that Flywheel has received the following certifications:

**SOC2**

*Cloud Security Alliance*

**EU PRIVACY SHIELD**

*Data Privacy Practices*

**GDPR**

*General Data Protection Regulation*

### AUDITS

Flywheel performs internal audits of all systems and software to ensure privacy and security standards are met and exceeded. We also work with credentialed assessors to perform external audits and determine compliance of industry security regulations.

### DATA REQUESTS

We provide certain levels of data to users that pertain to their particular WordPress sites hosted on our platform. This includes information such as site backup data and log activity (including access logs, error logs, and slow error logs). Beyond standard data requests, users may contact their Account Manager or our support team for additional information, at which point we'll determine any privacy concerns with the request and act accordingly.

### LEGAL COMPLIANCE

Flywheel works with legal professionals to review all security and privacy standards set forth by our organization. These professionals collaborate with the Flywheel Security Team to ensure all policies comply with legal and regulatory requirements while upholding Flywheels' mission and values.

### PENETRATION TESTING

Our security and development teams partner with third party security providers to conduct regular penetration and vulnerability testing on both our application and infrastructure to identify potential security or privacy concerns. Any reported incidents are then prioritized and patched by the relevant security team, engineers, and/or management. Any concerns reported by customers are evaluated and prioritized by the same standards to quickly resolve all incidents.

# Our update procedure

To ensure consistency and quality across security teams, we've established standard procedures to follow when pushing any line of code to production.

## SECURITY PATCHING

### MONITORING

We proactively monitor the Flywheel network, servers, and customer sites for malware infections, security breaches, and potential vulnerabilities. This monitoring includes (but is not limited to):

- **Nightly scans of Flywheel's network to identify known or spot potential vulnerabilities.**
- **Identifying and communicating identified vulnerabilities and/or security breaches to Flywheel's leadership and the relevant security teams.**
- **Individual monitoring of each website operating on Flywheel's network.**

## REVIEW AND EVALUATION

Once we have identified a vulnerability, members of the appropriate security team will review the incident within hours of the notice. We will then categorize the threat and impact of the vulnerability to prioritize the patch. Levels of security assessment include:

- **Emergency: An immediate threat to Flywheel's application, infrastructure, or sites hosted within.**
- **Critical: A security vulnerability that could have high impact but has not yet.**
- **Not Critical: A standard security release update that's necessary, but not urgent.**
- **Not Applicable: A security vulnerability that's helpful to be aware of, but not relevant to Flywheel's environment and systems.**

Regardless of the assigned classification, all security patch releases will follow a defined process for deployment that includes assessing the risk, testing the patch, scheduling the update, installing the repair, and verifying the solution.

## RISK ASSESSMENT AND TESTING

We will assess the effect of a patch to the Flywheel infrastructure prior to its deployment. The Flywheel Security Team will also assess the affected patch for impact to each component of the Flywheel platform, including servers, sites, software, and more.

If we categorize a vulnerability as an Emergency, the security team overseeing the patch considers it an imminent threat to our network. In these scenarios, we may deploy the patch before waiting to test its effect on our platform.

Vulnerabilities deemed Critical or Not Critical will undergo testing for each affected component of our infrastructure before implementing the patch. For Critical updates, we may expedite the testing process to address time-sensitive critical concerns.

## NOTIFICATION AND SCHEDULING

Before we proceed with a large-scale patch, the Flywheel Security team must approve the schedule as it affects Flywheel's platform and customer sites. Regardless of criticality, each patch release requires the creation and approval of a Request for Technical Change (RTC) prior to implementation. The Flywheel Security Team and leadership will determine when notifying customers is necessary.

### IMPLEMENTATION

Flywheel will deploy Emergency patches as soon as possible. As Emergency patches pose an imminent threat to the network, the release may precede testing. In all instances, Flywheel will perform testing (either pre- or post-implementation) and document it for auditing and tracking purposes.

Security teams must obtain authorization for implementing Critical patches via an emergency RTC. The department overseeing the patch will implement Not Critical updates during regularly scheduled preventative maintenance. Each patch must have an approved RTC.

### AUDITING, ASSESSMENT, AND VERIFICATION

Following the release of all patches to Flywheel's platform, members of the security team overseeing the update will verify the successful installation of the patch and confirm there have been no adverse effects on varying systems.

## SOFTWARE UPDATES

### SCHEDULED MAINTENANCE

Flywheel will provide scheduled maintenance for the purpose of general upkeep of systems, including (but not limited to) general adjustments, the installation of bug fixes and patches, and the implementation of updates, upgrades, revisions, and new versions of Flywheel software and hardware.

### REMEDIAL MAINTENANCE

Flywheel will also provide remedial maintenance, including responding to problems encountered by customers and end users of our product and services.

### NOTIFICATION OF SCHEDULED AND REMEDIAL MAINTENANCE

Flywheel will give customers at least 72 hours notice of any scheduled maintenance plans and will provide customers with sufficient advance notice whenever maintenance might have a material impact on our services or the availability of our services. We reserve the right to conduct maintenance as deemed necessary to ensure the safety and security of all customer data.

Scheduled maintenance will not affect the availability of hosted sites on Flywheel's platform, unless customers request additional Scheduled Maintenance or the parties otherwise agree additional updates are appropriate. Scheduled Maintenance and Remedial Maintenance will be conducted during non-peak usage times, when practical.

# Protecting customer data

Flywheel is centered around building an exceptional platform and providing peace of mind to our customers (and their customers). Therefore, we follow a number of practices to prevent unauthorized access to systems and data, identify risks, execute industry-leading best practices, and evaluate ways to continue improving our platform.

## AUTHENTICATION

Flywheel employees are required to use a password manager to create, manage, and share complex credentials for the software and tools we use on a daily basis. They are required to be cryptographically strong in order to reduce the risk of an employee's account being compromised and unauthorized contacts gaining access to our systems.

We also use two-factor authentication when appropriate to access systems with classified data, such as the Flywheel admin application. Temporary SSH keys, device-specific tokens, and rotating passwords are all ways in which we ensure authorized users are the only ones accessing data related to Flywheel and our customers.

## CLASSIFYING AND INVENTORYING DATA

All data is assessed and categorized based on the sensitivity of the information and the access to it that different Flywheel employees may need. This allows us to control access and guarantee that only employees with the necessary permissions are able to access certain levels of user data.

## COMPANY HARDWARE PROTECTION

Flywheel's hardware runs a variety of monitoring tools that may detect suspicious code, configurations, and user behavior. Our IT specialist is responsible for installing, monitoring, and escalating any incidents that may occur to the Flywheel Security Team. Together, they'll determine the best course of action to quickly remedy the situation.

To protect the hardware itself, we have security cameras installed throughout our office space that monitor who's coming and going 24/7/365. Additionally, we have a key inventory to track who has access to our building at any given time.

## DATA AND MEDIA DISPOSAL

Depending on the sensitivity of information, we may store customer information for a variety of time. Site backups, for example, may be stored for up to 30 days, whereas site log information is only held for seven.

For questions or requests related to data or media disposal, customers are encouraged to contact their Account Manager or the Flywheel support team.

## DATA ENCRYPTION AT REST AND IN TRANSIT

We use encryption to transmit data over public networks. This includes all data shared between Flywheel systems, clients, and employees, both at rest and in transit. We support the latest techniques to securely encrypt communication and constantly monitor best practices to best serve our customers.

## NETWORK SECURITY

We use a secure VPN to allow employees to connect to the Flywheel network from anywhere in the world. This ensures all data is transmitted securely whether we're working from our Omaha headquarters or a coffee shop in Australia.

## PROTECTING SECRETS

We've created a variety of automated processes that protect the creation, storage, retrieval, and destruction of sensitive information, such as encryption keys or login credentials.

## THIRD-PARTY SUPPLIERS

Flywheel works with a number of third-party suppliers to create our exceptional hosting platform, systems, and processes. When choosing another company to partner with, we assess the impact upon Flywheel's production environment and take the appropriate steps to ensure our own security standards are maintained at every level. We are constantly evaluating our third-party suppliers to ensure we're providing the most secure solution for our customers.

# Still have questions?

Flywheel thinks a lot about security so you can think about it less. We're constantly evaluating our processes, building new partnerships, and updating our systems to execute industry-leading security solutions.

If you would like to request more information about Flywheel's security, feel free to reach out to your Account Manager or email one of our experts! They'd be happy to provide additional details or reports so you can feel confident in our security systems and policies.

**CONTACT**

sales@getflywheel.com | 402-223-6105

Or, sign up at getflywheel.com

FLYWHEEL