WordFly Security Statement

We take security and privacy seriously at WordFly. Every step of the way, our team prioritizes the protection and care of your data. We work diligently to exceed international policy standards, and we go the extra mile to care for the information contained in your WordFly account. Creating a secure and innovative product is an ongoing effort. Our team of security specialists make regular updates to our infrastructure and applications to create a safe, reliable, and redundant environment for our customers. In addition, we routinely review our practices and undergo a rigorous annual third-party audit of our approach. To help create transparency around the subject of data security and privacy, we've created a brief overview to explain how WordFly manages your data and the steps we've taken to protect it. Do you have security-related questions? Please reach out to us at infosec@wordfly.com.

WordFly Data Center

- WordFly's infrastructure is housed in a Tier 5 Platinum Elite data center that meets or exceeds the standards of IEEE, ANSI, ASHRAE, 24/7, ISO 9001, SAS 70/SSAE-16, BICSI, the Green Grid Association, and more.
- DDOS mitigation tools are in place with extensive logging, analysis, and monitoring.
- All data center resources are monitored and secured 24x7x364.

WordFly Physical Security

Physical access to our machines is restricted to specific individuals and uses multiple levels of security, including:

- The equipment hosting WordFly services is located in physically secure facilities. Access to these facilities is limited to authorized personnel. Badge access and biometric authentication (hand scanners and fingerprint IDs) are required in order to access the facilities.
- WordFly equipment is isolated and secured in spaces reserved for WordFly equipment only. Spaces are not shared with third parties.
- Access to hosting environments is regularly reviewed to ensure authorization
- WordFly offices are secured by keycard access and are monitored with CCTV cameras throughout.
- Both physical and wireless networks are segmented to provide network layer isolation between services.

WordFly Application Security

- The WordFly application security team is embedded within the development team and follows a secure by design methodology, serving as a dedicated resource to the application development team and is led by CISSP certified professionals.
- Our servers are monitored 24x7 for integrity, availability and malicious activity.
- The entire WordFly application is encrypted with TLS.

- WordFly has brute force detection monitoring and automatic remediation.
- We regularly perform external security penetration tests using multiple vendors. Testing involves high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.
- WordFly hosting environment is protected from the public Internet via multiple firewalls and active monitors which alert WordFly administrators of any suspicious traffic.
- All account, credit card, and subscriber information and content are encrypted via industry-standard Secure Sockets Layer (SSL) connections over HTTPS.
- WordFly uses industry-standard security hardening techniques on all systems. In accordance with our security and change management policies, unused services are disabled and software updates are applied on a regular basis.
- WordFly regularly reviews information on current potential security vulnerabilities, including vendor announcements and other industry sources. If security updates are determined to be critical to the WordFly environment, they are thoroughly tested and deployed in a timely manner.

WordFly Application Development

- All internally developed code is subject to a strict Quality Assurance program, including extensive testing of functionality and business logic.
- Change management processes are in place to ensure that all code deployed to the production environment has been appropriately reviewed and approved by QA for release.
- WordFly performs regular security reviews, including external and internal scanning for vulnerabilities on an ongoing basis by a third-party vendor. All vulnerabilities discovered are reviewed and responded to by WordFly engineers.

WordFly Client Access

- WordFly account passwords are hashed. Nobody—not even our own staff—can view passwords. If you lose your password, we cannot retrieve it. It must be reset.
- All login pages pass data via TLS.
- User-level access to WordFly services is provided via a username and password selected by the end user.
- Passwords and all user data is encrypted, hashed, and seeded using industry-standard encryption algorithms.
- Strong password creation and verification routines are used throughout WordFly.
- User account setup, maintenance, and termination are under the control of the end user.

WordFly Data Loss and Protection

- All client databases are dedicated to each client. This isolation provides more security for our clients while allowing our engineers to compartmentalize each client's data.
- All Account data is stored redundantly both onsite and via offsite physical backup media that is stored in a vault.

- WordFly uses an extensive backup process to ensure all client data is backed up and to confirm the reliability and operation of all systems involved in backup and restoration of client data.
- All backup data stored in encrypted format on LTO media.
- Backup and restore operations are tested regularly to ensure consistent operation.

WordFly Security Education and Training

- WordFly requires annual training for all employees on best security practices, including how to identify social engineering, phishing scams, and hackers.
- All employees undergo criminal history and credit background checks prior to employment.
- All employees sign a Privacy and Security Agreement outlining their responsibility in the protection, handling, and use of customer data.
- To protect WordFly from losses, we carry comprehensive insurance coverage that includes, but is not limited to: general liability, data loss, data privacy incidents, regulatory, general errors and omission liability coverage, property, as well as international commercial general liability coverage.

WordFly Protocols Privacy Law, Standards, and Process

- Our product development and legal teams work closely to ensure our products and features comply with all applicable international spam and privacy laws.
- We undergo annual verification with a U.S.-based third-party outside compliance reviewer under the Privacy Shield verification program, and we have certified our compliance with the EU-U.S./Swiss-U.S. Privacy Shield Frameworks.
- Our corporate attorneys and Legal Compliance Manager are active members of the International Association of Privacy Professionals (IAPP) and collectively hold the certifications of CIPP/US, CIPP/G, and CIPP/E.