Vivial Media LLC Platforms Trusted Services

The Vivial Media platforms are critical to our customer's digital marketing and business success. That is why we design our systems and processes to be highly available and performant to avoid outages, errors, data corruption, or nefarious activity.

vivial™

SECURITY

Strict Standards for Top-to-Bottom Security

Vivial's approach to security is to implement protection at all layers of our environment. These include firewalls, strong passwords, VPN, and encryption.

Vivial applies the following National Institute of Standards and Technology (NIST) principles to protect the Vivial Media platforms including:

Simplicity — We design security mechanisms (and information systems in general) to be as simple as possible.

Fail-Safe — If a failure occurs, the Vivial Media platforms are designed to fail in a secure manner, i.e., security controls and settings remain in effect and are enforced.

Complete Mediation — Rather than providing direct access to information, mediators that enforce access policy are employed (interfaces, file system permissions, proxies, firewalls, and mail gateways).

Open Design — Our system security does not depend on the secrecy of the implementation or its components.

Separation of Privilege — Functions, to the degree possible, are separate and provide as much granularity as possible. The concept can apply to both systems and users. In the case of systems, functions such as read, edit, write, and execute should be separate. In the case of system users, roles should be as separate as possible.

Least Privilege — Each task, process, or user is granted the minimum rights required to perform its job. We apply this principle consistently so that if a task, process, or user is compromised, the scope of damage is constrained to the limited resources available to the compromised entity.

Design Acceptability — Users are trained to understand the necessity of security. In addition, the security mechanisms in place present users with sensible options that give them the usability they require on a daily basis. If users find the security mechanisms too cumbersome, they may devise ways to work around or compromise them. The objective is not to weaken security so it is understandable and acceptable, but to train and educate users and to design security mechanisms and policies that are usable and effective.

Least Common Mechanism — When providing a feature for the system, it is best to have a single process or service gain some function without granting that same function to other parts of the system. The ability for the Web server process to access a back-end database, for instance, should not also enable other applications on the system to access the back-end database.

Defense-in-Depth — Vivial understands that a single security mechanism is generally insufficient. Our security mechanisms (defenses) are layered so that a compromise of a single security mechanism is insufficient to compromise a host or network.

Work Factor — Our security services are designed so the amount of work necessary for an attacker to break the system or network should exceed the value that the attacker would gain from a successful compromise.

Frequent and Rigorous Testing

To assure the security of the Vivial Media platforms, frequent testing is performed.

In addition to ongoing application regression testing, Vivial contracts with an independent third party, Coalfire, to perform annual application vulnerability assessments and penetration testing.

Data Security Across All Layers

Data on our systems is protected. We use a layered approach to security implementing firewalls, encryption, private networks, monitoring, alerting and access controls. This keeps customer data secure through all stages of transit and storage.

- Keeping data transmitted between Vivial and the Customer secure. Data is encrypted while being transmitted over the public Internet. We use Secure Sockets Layer (SSL) to provide security and data integrity over the Internet.

Reliable Network and Physical Security of Servers and Datacenters

The Vivial Media platforms are hosted at Amazon Web Services (AWS). By using AWS, Vivial inherits the many security controls of AWS. For more information, please refer to AWS Security and Compliance Quick Reference Guide.

Secure Change Management

Vivial's change management procedures assure implementations of new hardware, software or cloud technology can occur without creating security problems. Our assessment, monitoring and advanced planning assures we are prepared to execute any changes to our infrastructure and applications in a secure manner.

Availability

Redundant Systems to Minimize Catastrophic Losses

We believe our systems and infrastructure should have no single points of failure and that data should be as redundant as possible. To this end we implement dynamic DNS, load balancers, clustered databases, backups and redundant network connections to minimize loss due to human error, data corruption and/or system failure.

Privacy and Compliance

We Keep Private Data Private

We are committed to protecting the security of your information. We have adopted commercially reasonable security measures consistent with industry practice that are designed to assist in protecting against the loss, misuse and alteration of your Personal Information and Personal Health Information which is under our control. As you know, no security system or system of transmitting data over the Internet can be guaranteed to be 100% secure. Accordingly, you should not expect that any information provided to us or to any third party will always remain private. Please review our privacy policy at http://www.vivial.net/privacy-policy for more information.