www.buildfire.com

# Information Security Policies

## Third Party Security Management Policy

| | | | | | |
|---|---|---|---|---|---|
| Policy # | IS-14 | Effective Date | 03/01/2017 | Email | policy@buildfire.com |
| Version | 1.0 | Contact | Daniel Hindi | Phone | (949) 899-8204 |

### Table of Contents



## PURPOSE

This policy defines the requirements for the management of third-party organizations and services that handle sensitive information for BuildFire.

## SCOPE

This policy applies to all BuildFire employees responsible for managing controls with third-parties.

## POLICY

### Third Party Service Providers

**Third-Party Risk Assessment** – The Information Security Department or an approved delegate must conduct an annual review of the information security risks of all third-parties with access to BuildFire sensitive information.

### Third-Party Security Requirements

**Third-Party Security Policy Acknowledge** - All BuildFire third parties with access to sensitive information must be made aware of the BuildFire security policies and agree to follow BuildFire information security policies.

### Third-Party Access Control

**Third-Party Access Approval** - Third-party access to any BuildFire internal computer systems that are not clearly public must be approved in advance by BuildFire management.

### Third-Party Contracts

**Third-Party Contracts - Information Security Responsibilities** - All BuildFire business partners, suppliers, and other business associates must be made aware of their information security responsibilities through specific language appearing in contracts that define their relationship with BuildFire.

**Reporting Third-Party Security Violations** - All Information Technology outsourcing contracts must stipulate that the third parties must notify BuildFire immediately of any security incident likely to impact sensitive BuildFire information under their control.

### Contingency Plans

**Continuity Service Level Agreements with Third Parties** - All agreements with third-parties which could negatively impact the business processes of BuildFire must define service level agreements and require minimum standards of contingency planning and preparation on the part of these third parties.

## VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. BuildFire reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. BuildFire does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, BuildFire reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

## DEFINITIONS

**Confidential Information (Sensitive Information)** – Any BuildFire information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by BuildFire from a third party under a non-disclosure agreement.

**Data Center –** Any physical room or building that houses computer or communications equipment. This includes any third party facilities that host BuildFire systems.

**Information Asset –** Any BuildFire data in any form, and the equipment used to manage, process, or store BuildFire data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Password –** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**Third Party –** Any non-employee of BuildFire who is contractually bound to provide some form of service to BuildFire.

**User -** Any BuildFire employee or partner who has been authorized to access any BuildFire electronic information resource.

## REFERENCES

CPL: 6.0 Third Party Security
ISO/IEC 27002: 15. Supplier relationships

## APPROVAL AND REVISION HISTORY

| Version | Description | Revision Date | Approved By: | Title |
|---|---|---|---|---|
| 1.0 | Initial Version | 03/01/2017 | Daniel Hindi | CTO |
| | | | | |