www.buildfire.com

Information Security Policies

IT Risk Management Policy

Policy #	IS-01	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 identification and treatment of information security risks for all BuildFire information and system assets.

SCOPE

This policy applies to all BuildFire computer systems and facilities, including those managed for BuildFire by third-parties. This policy applies to all employees and third-parties with access to BuildFire information assets.

POLICY

Risk Management Process

Enterprise Security Risk Assessment - Each year the Information Security Department in conjunction with Information Technology (IT) must conduct, or manage an independent party who conducts, an organization-wide security risk assessment. The report resulting from this project must include a detailed description of the information security risks currently facing the organization, and specific recommendations for preventing or mitigating these risks.

Control Framework - BuildFire will adopt and information security control framework designed to mitigate information security risks and comply with regulatory and contract requirements for information security.

Risk Mitigation - Insurance

BCP and Insurance - BuildFire will maintain insurance commensurate with those residual risks which pose potential for financial loss or other disastrous consequences, as well as the expenses related to recovering from a disaster.

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.

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.

Risk - The result of a threat acting on a vulnerability, expressed as a product of likelihood (probability) and severity (of impact.)

Risk Assessment - The determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat or hazard. The result of a risk assessment is typically a report that shows assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.

Residual Risk – The risk that remains after a control is applied to an identified risk, and that control does not eliminate the risk.

Risk Mitigation – The process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process.

Threat - Any person, object or event that, if realized, could potentially cause damage to an information resource or the data processed on those resources. This includes damage to the **availability, integrity**, and/or **confidentiality** of resources or information.

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

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.

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

REFERENCES

ISO/IEC 27002: 4.0 Risk Management
CPL: 1.0 IT Risk Management

APPROVAL AND REVISION HISTORY

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