www.buildfire.com

Information Security Policies

Remediation Plan Policy

Policy #	IS-17	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 developing, testing, and maintaining the BuildFire remediation plan.

SCOPE

This policy applies to all BuildFire production information systems. This policy applies to all employees and third-parties responsible for managing BuildFire systems.

POLICY

Enterprise Security Risk Assessment

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.

Information Security Responsibility Assignment

Defining Specific Security Roles - BuildFire must define specific job roles required for the effective implementation of the BuildFire information security program. Each role must include a specific description of the information security-related duties performed by each team member performing those job functions.

Assigning Specific Security Roles - BuildFire must explicitly define at least one individual

responsible for the duties of the information security specific roles

Assigning Security Officer - BuildFire must explicitly define at least one individual responsible for the duties of the information security function. This role will be entitled “Information Security Manager.”

Data Storage Restrictions

Storage Restrictions - Sensitive data must always be encrypted during storage on electronic media if it is taken outside of BuildFire premises.

Encryption Standards - All sensitive data encryption must follow standards established by the Information Security Department.

System Administration Remote Management

Remote Access Encryption - All non-local access to Buildfire systems must be encrypted using methods approved by the Information Security Department. All web-based access must use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Secure Application Coding

Code Reviews - BuildFire application development teams must perform periodic reviews of source code for possible security and privacy flaws. Reviewers must possess special training in application security techniques or use a third-party authorized to review application security.

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.

APPROVAL AND REVISION HISTORY

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