www.buildfire.com

Information Security Policies

Information Security Organization Policy

Policy #	IS-03	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 specific information security roles required to implement the BuildFire information security program and applicable policies and controls.

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

Security Planning

Centralized Information Security - Guidance, direction, and authority for all information security activities are centralized for the entire organization in the Information Security Department.

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."

Worker Information Security Roles

Three Categories Of Responsibilities - To coordinate a team effort, BuildFire has established three categories, at least one of which applies to each employee or third-party with access to sensitive information. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

Owner Responsibilities - Information Owners are the department managers, members of the top management team, or their delegates within BuildFire who bear responsibility for the acquisition, development, and maintenance of production applications that process BuildFire information. Production applications are computer programs that regularly provide reports in support of decision making and other business activities. All production application system information must have a designated Owner. For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

Custodian Responsibilities - Custodians are in physical or logical possession of either BuildFire information or information that has been entrusted to BuildFire. While Information Technology department staff members clearly are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

User Responsibilities - Users are responsible for familiarizing themselves with and complying with all BuildFire policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information.

Contact with Authorities

Contacting Law Enforcement - Every decision about the involvement of law enforcement with information security incidents or problems must be made by a BuildFire corporate officer in conjunction with the Information Security Manager.

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.

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

CPL: 3.0 – Information Security Organization
ISO 27002: 6. Organization of information security

APPROVAL AND REVISION HISTORY

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