www.buildfire.com

Information Security Policies

Personnel Security Management Policy

Policy #	IS-09	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 information security-related requirements that impact the hiring, ongoing management and termination of personnel at BuildFire.

SCOPE

This policy applies to all employees and third-parties with access to BuildFire information assets.

POLICY

Roles and Responsibilities

Job Descriptions - Specific information security responsibilities must be incorporated into all formal job descriptions if such employees have access to sensitive information.

Pre-Employment Screening

Background Checks - All employees to be placed in computer-related positions of trust must pass a background check. This process shall include examination of criminal conviction records, lawsuit records, credit bureau records, driver's license records, and verification of previous employment.

Terms and Conditions of Employment

Policy Compliance Agreement - As a condition of continued employment, employees, consultants, and contractors must annually sign an information security compliance agreement.

Non-Disclosure Agreements - All employees must personally sign a BuildFire non-disclosure agreement before work begins. If an Employee has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

Intellectual Property Rights Agreement - While employees of BuildFire, all staff members must agree to grant to BuildFire exclusive rights to patents, copyrights, inventions, and all other intellectual property they originate or develop.

Code Of Conduct Acknowledgement - All Employees must indicate their understanding of the code of conduct by annually signing a form acknowledging that they agree to subscribe to the code.

Security Awareness and Training

Security Violations and Reporting - Users must be clearly informed about the actions that constitute security violations as well as informed that all such violations will be logged and how to properly report possible security incidents.

Information Security Policy Distribution - On or before their first day of work, all new BuildFire Employees must be made aware (or receive a copy) of the information security policy (policies) and be notified that they must comply with the requirements described in these policies as a condition of continued employment.

Annual Information Security Class - All employees and partners must complete an information security training course and pass a corresponding test on an annual basis. New Employees must attend and pass the course within 15 days of the date when they begin employment with BuildFire.

Training Records List - Management must maintain a listing of the training provided to all users of BuildFire information assets.

Personnel Transfers and Changes

Reporting Status Changes - When an employee changes job duties, including termination, transfer, promotion and leave of absence, his or her supervisor must immediately notify the System Admin department.

Personnel Terminations

Employee Termination Procedure - In the event that an employee, consultant, or contractor is terminating his or her relationship with BuildFire, the employee's immediate manager must ensure that all property in the custody of the employee is returned before the employee leaves BuildFire, notify all administrators handling the computer and communications accounts used by the employee as soon as the termination is known, and terminate all other work-related privileges of the individual at the time that the termination takes place.

Involuntary Terminations - In all cases where information technology employees are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all BuildFire equipment and information, and escorted while they pack their belongings and walk out of BuildFire facilities.

Recovery Of Organization Property - Employees, temporaries, contractors, and consultants must not receive their final paycheck unless they have returned all hardware, software, working materials, confidential information, and other property belonging to BuildFire.

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.

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: 7.1. Personnel Security Management
ISO/IEC 27002: 7. Human Resources Security

APPROVAL AND REVISION HISTORY

Version	Description	Revision Date	Approved By:	Title

1.0	Initial Version	03/01/2017	Daniel Hindi	CTO