www.buildfire.com

Information Security Policies

Information Security Program Policy

Policy #	IS-02	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 establishes the minimum requirements and responsibilities for the protection of BuildFire information assets, preventing the misuse and loss of information assets, establishing the basis for audits and self-assessments, and preserving management options and legal remedies in the event of asset loss or misuse.

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

Programs

Information Security Program - BuildFire must implement a comprehensive, written information security and data privacy program that will secure BuildFire information assets in a manner commensurate with each asset's value and sensitivity.

Policy and Procedures Requirements

Information Asset Security Policies - Policies must be implemented and enforced to assure the security, reliability, integrity, and availability of BuildFire information assets.

Information Asset Security Procedures - Procedures must be implemented and enforced to enforce security policies and assure the security, reliability, integrity, and availability of BuildFire information assets.

Policy Sanctions

Policy Sanctions – BuildFire must implement sanctions against employees and third parties who violate the written policies.

Exceptions

Exceptions to Policies - All BuildFire employees responsible for information security must submit a written request for exceptions to conform to information security policies. Such exceptions must be approved by a member of the information security department.

Policy Distribution

Security Policy Document Distribution - BuildFire management must publish written information security policies and make them available to all employees and relevant external parties.

Acknowledgement of Security Policies — All BuildFire employees and contractors must review and acknowledge acceptance of the information security policies which apply to them at least on an annual basis.

Policy Document Classification – All BuildFire security policy documents must be labeled as CONFIDENTIAL – Internal Use Only and revealed only to BuildFire workers and selected outsiders (such as auditors) who have a legitimate business need for this information.

Policy Review

Annual Review of Information Security Policy Documents - All BuildFire written information security policy documents must be reviewed on an annual basis by a team consisting (at a minimum) of members from the information security, legal and human resources departments.

Program Review and Maintenance

Annual Program Updates - The information security program must be updated and re-approved by BuildFire management annually or whenever there is a material change in the organization or infrastructure.

Security Program Compliance

Laws, Regulations And Contractual Requirements – The control requirements for the BuildFire information security program must include an analysis and definition of all relevant statutory, regulatory, and contractual requirements.

Information System Control Reviews — Independent - An independent and externally-provided review of information systems security must be periodically obtained to determine both the adequacy of and compliance with controls.

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 - Security Program Management
ISO 27002: 5.1 Management direction for information security

APPROVAL AND REVISION HISTORY

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