Information Security Policies

Information Exchange Security Policy

Policy #	IS-06	Effective Date	03/01/2017	Email	policy@buildfire.com
Version	1.0	Contact	Daniel Hindi	Phone	(949) 899-8204

Table of Contents

Purpose 1
Scope 1
Policy 1
  Disclosure Restrictions 1
  Exchange Agreements 1
  Physical Transit Controls 2
  Electronic Transmission 2
  Web Site Security 2
Violations 2
Definitions 2
References 3
Approval and Revision History 3

PURPOSE

This policy defines controls for the proper exchange and transfer of all BuildFire sensitive information assets, either in paper or electronic format.

SCOPE

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

POLICY

Disclosure Restrictions

External Information Requests - All requests from a third party for internal information that is not classified as PUBLIC must be approved by both the Information Owner and the BuildFire Chief Security Officer.

Information Transfer To Third Parties - BuildFire software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-BuildFire party for any purposes other than those expressly authorized by management.

Exchange Agreements

Information Exchange Agreements - Exchanges of internal confidential information between BuildFire and any third party must be accompanied by a written agreement that

specifies the terms of the exchange, and the manner in which the software or information is to be handled and protected.

Physical Transit Controls

Sending Confidential Hardcopy Information - Confidential information in hardcopy or electronic form must be sent by trusted courier or registered mail, must always be tracked with a bill number and must always be marked recipient “signature required.”

Sending Confidential Information – Packaging - If confidential information is sent through internal mail, external mail, or by courier, it must be enclosed in two envelopes or containers with the outside envelope or container providing no indication of the sensitivity of the information contained therein and the inside sealed and opaque envelope or container labeled “Private” or “Confidential.”

Sending Electronic Confidential Information – All electronic media containing confidential information sent to third parties must be encrypted during transit.

Electronic Transmission

Confidential Data Electronic Transmission - All BuildFire confidential data transmitted over any external communication network must be encrypted using technology and protocols (Such as SSL/TLS or IPSEC) approved by the Information Security Department.

Wireless Transmissions Of Confidential Information - Wireless technology must never be used for the transmission of unencrypted confidential information.

Electronic Mail Encryption - All sensitive information must be encrypted when transmitted through electronic mail.

Web Site Security

Confidential Information On Web – BuildFire Confidential information must not be resident on Internet web servers.

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.

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

REFERENCES

CPL: 5.3. Information Exchange and Transit
ISO/IEC 27002 - 13.2 Information transfer

APPROVAL AND REVISION HISTORY

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