www.buildfire.com

Information Security Policies

Information Storage and Retention Policy

Policy #	IS-05	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 for the inventory, retention and disposal of BuildFire information assets.

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

Information Collection

Pretext Data Collection – BuildFire staff or authorized third parties must not at any time gather personal information using misrepresentations or pretext statements about its right to receive such information.

Information Inventory

Asset Inventory - Information - The Information Security Department must compile and annually update a corporate-wide data dictionary and other high-level descriptions of the major BuildFire information assets.

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.

Information Retention

Information Retention Periods - A retention period must be assigned to all sensitive information, regardless of the form it takes (paper documents, computer files, etc.).

Customer Data Retention – Customer data are retained and protected as long as each Customer continues to do business with BuildFire and for 90 days thereafter. At that point BuildFire may declassify or destroy customer data.

Record Destruction - Employees must not destroy BuildFire sensitive information records unless these records appear on a list of records authorized for destruction.

Litigation Hold

Destroying Documents Relevant To Litigation - If there is credible reason to believe that certain BuildFire internal documents may be needed as evidence in upcoming litigation, these documents must not be destroyed by the ongoing BuildFire document destruction process. They must instead be brought to the attention of internal legal counsel and then properly secured.

Information Disposal Standards

Data Sanitization Standards – The Information Security group is responsible for establishing standards for the proper sanitization of all computer equipment and media storage scheduled for destruction. These same standards must be used by any third-party vendor contracted to dispose of BuildFire equipment.

Disposal of Hardcopy Records

Hardcopy Disposal - When disposed of all confidential or private information in hardcopy form must be either shredded or incinerated. To ensure that documents are properly destroyed, only shredders approved by BuildFire will be used to shred hardcopy records containing sensitive information.

Secure Information Containers – Sensitive information that is no longer needed must be placed in a designated locked destruction container within BuildFire offices and never placed in trash bins, recycle bins, or other publicly-accessible locations.

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: 5.4 Information Storage and Retention
ISO/IEC 27002 - 18.1.3 Protection of records

APPROVAL AND REVISION HISTORY

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