www.buildfire.com

Information Security Policies

Information Classification Policy

Policy #	IS-04	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 requirements assigning and maintaining classification settings for all 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

Asset Ownership

Information Ownership - All production information possessed by or used by BuildFire must have a designated Information Owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

Information Classification

Three-Category Data Classification - All BuildFire data must be broken into the following three sensitivity classifications: CONFIDENTIAL, PRIVATE, and PUBLIC. Distinct handling, labeling, and review procedures must be established for each classification.

Data Classification Descriptions - The following descriptions are used for identifying and labeling each sensitivity classification for all BuildFire information.

CONFIDENTIAL - This classification label applies to the most sensitive business information that is intended for use within BuildFire. Its unauthorized disclosure could adversely impact BuildFire or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification.

PRIVATE - FOR INTERNAL USE ONLY - This classification label applies to less-sensitive business information that is intended for use within BuildFire. Its unauthorized disclosure could adversely impact BuildFire or its employees, suppliers, business partners, or its customers.

PUBLIC - This classification applies to information that has been approved by BuildFire management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

Default Classification - Information without a label is by default classified as Internal Use Only.

Asset Labeling

Data Classification Labeling - All printed or portable electronic copies of confidential information must be labeled according to policies and standards issued by the Information Security Department, while information not falling into one or more of these categories need not be labeled.

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: 5.2. Information Classification
ISO/IEC 27002: 7.2.1 Classification Guidelines

APPROVAL AND REVISION HISTORY

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