www.buildfire.com

Information Security Policies

Application Development Policy

Policy #	IS-18	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 for the secure development, testing and deployment of BuildFire applications developed in-house or by third parties that process or store sensitive information.

Scope

This policy applies to all BuildFire production application systems. This policy applies to all employees and third-parties responsible for managing BuildFire systems.

Policy

Application Development Specification

Information Security Requirements – Each development specification document produced for BuildFire applications that are developed or purchased must include information security and data privacy requirements. Security and data privacy requirements must be identified as such within the specification document.

Initial Application Criticality Classification – Each application built or acquired by BuildFire must have an initial application criticality classification. This rating will specify the overall level of security of the system, as well as the required recovery time for any system disruption.

Secure Application Coding

Code Reviews – BuildFire application development teams must perform periodic reviews of source code for possible security and privacy flaws. Reviewers must possess special training in application security techniques or use a third-party authorized to review application security.

Secure Code Training Required - All employees involved in the coding of BuildFire business applications must receive training on secure coding principles.

Secure Coding Methods – All source code created by BuildFire developers must use secure coding methods approved by the development team and the Information Security Department.

Source Code Management - All program source code used for BuildFire production systems must be stored in a secure source code management system with access controls approved by the Information Security Department.

Application Security Requirements

(Note: You can roll these and other controls into a specific Application Security Standard. You can then include one of these for your clients)

Application Development Standard - All BuildFire applications must be developed according to security requirements developed by the Information Security Department. The standard includes a list security requirement for each type of system. (For example, Passwords must never be hardcoded into software, and developers must not build in secret or back-door accounts.)

Open Source Software

Conditions for Use of Open Source - BuildFire production computers must not employ open source software unless this software is known to have passed a rigorous security testing process undertaken by an independent and reputable third party. Additionally, this same software is known to be readily supported by a wide variety of technical consultants from different organizations.

Application Testing

Testing Data Sets – To maintain the security and privacy of its customers, BuildFire must limit the amount of sensitive data that gets duplicated, stored and transmitted. Applications that process sensitive BuildFire data (such as customer medical data, financial data, credit cards, etc.) testing must not use real customer data for testing purposes.

Third-Party Testing – BuildFire must not employ any third party to test applications which process sensitive data unless test data has been sanitized to mask the true customer data.

Test Data and Account Removal - Test data and accounts must be removed before a development system is moved into production.

Vulnerability Analysis and Testing

Vulnerability Analysis before Release – Before being released into production, all BuildFire business applications must undergo a vulnerability analysis and penetration test by either (1) a member of BuildFire staff trained under this discipline, or (2) a trusted third-party.

Vulnerability analysis must be based on, at a minimum, the most recent list of common vulnerabilities available from Open Web Application Security Project (OWASP).

Documentation and Source Code

Documentation Confidentiality - All BuildFire computer related documentation is confidential, and must not be taken elsewhere when a worker leaves the employ of BuildFire.

Open Source and Third-Party Library Inventory – Part of the required documentation for each BuildFire application is a list of all third-party software packages used within the application. These include but are not limited to linked libraries, database applications, and encryption packages.

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.

Production Application – Production Applications are those applications created and maintained by BuildFire for their customers. These do not include third-party application such as Office 365.

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: 12.1.2. Application Development Security

APPROVAL AND REVISION HISTORY

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