www.buildfire.com

Information Security Policies

Data Privacy Program Policy

Policy #	IS-21	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 implementation and maintenance of a customer data privacy program at Buildfire.

SCOPE

This policy applies to employees and third parties with access to Buildfire data and application development services.

POLICY

Programs

Information Privacy Program - Buildfire must implement a comprehensive, written information privacy program that will secure Buildfire employee and customer personally identifiable information (PII) against unauthorized use or disclosure.

Formal Privacy Governance Program - Buildfire will establish a formally documented privacy governance program. Buildfire will assign roles and responsibilities to support the program, and communicate the program goals and activities to all personnel.

Roles and Responsibilities

Assign Privacy Roles and Responsibilities - Buildfire must assign privacy responsibilities to personnel and incorporate privacy responsibilities into all positions that handle PII.

Designated Privacy Officer - Buildfire will appoint a Chief Privacy Officer to oversee and be responsible for all Buildfire information privacy initiatives, activities and incidents.

Privacy Assessments

Privacy risk assessment required - The Buildfire Chief Privacy Officer, or an authorized delegate, must analyze the threats to PII and determine what the potential impact to the company in the event a related incident occurred. The Chief Privacy Officer must then calculate the actions and related costs to help prevent such incidents.

Monitoring of security and privacy laws - Buildfire must continuously monitor corporate information security and privacy legal compliance, new security and privacy laws and regulations, and update programs as necessary to help ensure compliance.

Policy and Procedures Requirements

Data Privacy Policies - Policies must be written, implemented and enforced to assure the security, reliability, integrity, and availability of sensitive personal information (PII).

Data Privacy Security Procedures - Procedures must be implemented and enforced to enforce security policies and assure the security, reliability, integrity, and availability of sensitive personal information (PII).

Personal Information Inventory

Comprehensive PII inventory required - Buildfire must define and document the PII Buildfire handles and communicate this information to personnel to ensure they know and understand what PII Buildfire is responsible for protecting.

PII Data Flow Assessment - Buildfire must map the data flows and identify points during the flows where PII is most vulnerable, then create controls and protections as appropriate.

Third Party Privacy Requirements

Third Party Privacy Impact Assessment - Satisfactory Privacy Impact Assessments (PIAs) must be performed for third parties, and the results approved by the CPO, before giving the third party access to Buildfire PII to manage, process, transfer, or otherwise handle in any other way.

Privacy Training Requirements

Annual privacy training required - All Buildfire personnel must complete annual privacy training and participate in targeted privacy training as requested.

Documented privacy education program - The Buildfire Chief Privacy Officer must ensure the corporate personnel and business partner privacy education program is documented and authorized by the Privacy Oversight Council.

Targeted privacy training for personnel handling PII - Buildfire must provide targeted privacy training to groups handling or using PII and provide ongoing awareness messages communicating how to protect PII.

Regular training of privacy team personnel - All privacy team members and privacy advocates must participate in regular training, including training for privacy incident response procedures.

Internal System Development

Privacy requirements included in systems development - Buildfire must incorporate privacy requirements into the Buildfire systems and applications development life cycle and systems and applications update procedures.

Limited Use of PII - Buildfire must limit the use of PII to only those purposes for which it was collected.

Limit Personnel Access to PII - Buildfire must limit the number of people who have access to PII to only those who need it to perform business activities.

Program Communication

External privacy policy required - Buildfire must post a website privacy policy, approved by the Chief Privacy Officer, on the corporate websites. Each page on each website must provide an easy-to-find link to the privacy policy.

Employee Notice of Privacy Policies – All Buildfire personnel who handle PII in any manor must be made aware of the privacy policies that apply to them, as well as the sanctions for not complying with policies.

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.

Opt-Out Notice - Notification to customers that they may choose not to permit their information shared with nonaffiliated third parties.

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.

Personally Identifiable Information (PII) – Information that alone, or when combined with other personal or identifying information can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

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: 16.2 Customer Privacy Management
ISO 27002: 18.1.4 Privacy and protection of personally identifiable information

APPROVAL AND REVISION HISTORY

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