www.buildfire.com

Information Security Policies

IT Business Continuity Policy

Policy #	IS-17	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 developing, testing, and maintaining the BuildFire business continuity plan.

SCOPE

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

POLICY

Business Impact Analysis

Business Impact Analysis - The Information Security Department or its designee must perform a business impact analysis (BIA) each year as part of the annual organization-wide risk assessment.

System Criticality Rating

Multi-User Application Criticality Rating - In conjunction with the Information Owners, Information Systems Department managers must periodically prepare or revise an assessment of the degree of criticality of all production multi-user computer applications.

Four Category Rating System - All production computer applications must be placed into one of five criticality classifications, each with separate handling requirements: critical,

priority, required, and deferrable. This criticality classification system must be used throughout BuildFire, and must form an integral part of the system contingency planning process.

System Recovery Times – The mean Recovery Time Objectives (RTO) and recovery point objectives (RPO) for each system type must be defined according to the system criticality rating.

Plan Development

Business Contingency Plans - Management must prepare, periodically update, and regularly test a business continuity and recovery plan (BCP) that specifies how BuildFire can continue operation after a disruptive event.

Alternative Facilities – The BCP must identify alternative facilities (offices, telephones, systems, etc.) that will be provided so workers can continue operations in the event of a business interruption.

Recovery Procedures - Procedures for restoring systems and services must be documented in formal contingency plans.

Plan Communication

Plan Availability - Business and information systems contingency plans must be continuously accessible through at least two separate Internet addresses, at least one of which is not supported by systems at the primary location.

Plan Testing

Contingency Plan Testing - To the extent practical and feasible, computer and communication system contingency plans must be tested annually to assure that they are still relevant and effective.

Recovery Personnel

Recovery Personnel Notifications – Every worker who has responsibility for business recovery must be notified of his/her responsibilities and corresponding work requirements.

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.

Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Business Impact Analysis (BIA) - A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

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: 14.03 Business Continuity Planning
ISO/IEC 27002: 17.1 Information security continuity

APPROVAL AND REVISION HISTORY

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