Information Security Policies

Security Incident Management Policy

Policy #	IS-15	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 reporting and responding to incidents related to BuildFire information systems and operations.

SCOPE

This policy applies to all BuildFire production information systems. This policy applies to all employees and third-parties with access to BuildFire information assets.

POLICY

Computer Emergency Response Team (CERT)

Computer Emergency Response Team - Information Technology Department management must organize and maintain an in-house computer emergency response team (CERT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies.

Testing The Computer Emergency Response Team - At least once every three months, the Information Security Department must utilize simulated incidents to mobilize and test the adequacy of the BuildFire Computer Emergency Response Team.

Incident Response and Recovery

Intrusion Response Procedures - The Information Technology Department must document and periodically revise intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

Reporting Information Security Events

Incident Reporting - All suspected information security incidents must be reported as quickly as possible through the approved BuildFire internal channels.

Information Security Alert System - Information Systems Department management must establish and maintain a communications system permitting employees to promptly notify appropriate staff about suspected information security problems.

Investigation and Forensics

Computer Crime Investigation - Whenever evidence clearly shows that BuildFire has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Information Security Investigations - All BuildFire internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Manager.

Reporting to Third Parties

External Violation Reporting - Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with representatives from the Legal Department and the Information Security Department must weigh the pros and cons of external disclosure before reporting these violations.

Contacting Law Enforcement - Every decision about the involvement of law enforcement with information security incidents or problems must be approved by a senior BuildFire executive and be initiated by the Information Security Manager.

Incident Review

Violation And Problem Analysis - An annual analysis of reported information security problems and violations must be prepared by the Information Security Department.

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.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

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: 13 Incident Detection & Management
ISO/IEC 27002: 16.0 Information Security Incident Management

APPROVAL AND REVISION HISTORY

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