www.buildfire.com

Information Security Policies

Security Operations Management Policy

Policy #	IS-16	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 covers the requirements for ongoing operations and management of all information technology hardware, software, and computer-related components that are managed by BuildFire or third-parties.

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

Documented Operating Procedures

Standard Operating Procedures - Operating procedures for the ongoing maintenance and operation of the IT systems of BuildFire must be maintained and made available to all users who need them.

System Planning and Acceptance

New System Approval - Prior to being placed into production use, each new, or significantly modified production business system must be approved in advance.

Operational Software Installation

Security Impact Statements - Prior to being placed into production use, each new, or significantly modified, or enhanced business application system must include a brief security impact statement that has been prepared according to standard procedures.

Segregation of Duties

Separation of Request and Approval - Whenever a BuildFire computer-based process involves sensitive information, the system must include controls so that the person requesting a change is separate from the person approving the change.

Systems Administrators Don`t Handle Security Administration - To achieve proper separation of duties, for all BuildFire production systems, Systems Administrators must not attend to, or otherwise be responsible for, information systems security administration. Security administration must instead be handled by Information Systems Security Administrators.

Systems Administrators Install/Update Server Software - Only authorized Systems Administrators are permitted to install and/or update software on BuildFire servers. These installations must be documented in a separate log according to the BuildFire Change Control Procedures.

Change Management

Change Control Procedure - All production information systems used for BuildFire must employ a formal change control procedure to authorize all significant changes to software, hardware, communications networks, and related procedures.

Change Control Documentation - Production information system change control documentation must be maintained so that management can readily determine exactly what changed and allow any and all prior versions of production applications to be readily recreated and pressed into service if necessary.

Malicious Software Management

Antivirus Software Deployment – Antivirus/antimalware software must be deployed and executing on all BuildFire computer and communications systems commonly affected by malicious software, e.g., personal computers and servers, where applicable anti-virus technology exists.

Antivirus Software Updates - All antivirus programs deployed on BuildFire computer and communications systems must be configured to accept automatic updates of the software.

Antivirus Software Scans - All antivirus programs deployed on BuildFire computer and communications systems must be configured to periodically scan all systems for malware.

Audit Logging and Monitoring

Computer and Communication System Logs - All BuildFire production information systems must have computer logs that record security-related events according the standards developed by the Information Security Department..

Production System Logs Standard - All computer systems running BuildFire production application systems must include logs that record, at a minimum, user session activity including user IDs, logon date and time, logoff date and time, as well as applications invoked, changes to critical application system files, changes to the privileges of users, and system start-ups and shut-downs.

Clock Synchronization - All production systems used for BuildFire must always have the current time accurately reflected in their internal clocks.

Log Management and Retention

Log Retention Period - Every log and audit trail produced by a BuildFire computer or communication system must be retained for at least one year.

System Log Rotation And Archival - To prevent the overwriting of system logs or the expansion of these logs to the point where they consume all available disk space, a formal log rotation and archival storage process must be employed for all network periphery security systems and all multi-user production servers.

System Log Integrity Check - All BuildFire production information systems must employ cryptographic checksums to protect system logs.

Limited Log Access – Only system administrators with approved access will be allowed to access, modify or archive log data.

Event Monitoring

Security Event Monitoring (SEM) – BuildFire must employ security event monitoring software to facilitate the collection, storage and analysis of system audit logs

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.

Emergency Change - When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

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.

Security Impact Analysis - The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

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: 11.0 Operations Management
ISO 27002: 12.0 Operations Security

APPROVAL AND REVISION HISTORY

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