www.buildfire.com

Information Security Policies

Asset and Media Management Policy

Policy #	IS-07	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 and responsibilities for the protection of BuildFire equipment and media assets throughout the asset lifecycle.

SCOPE

This policy applies to all BuildFire information and system assets, including those managed for BuildFire by third-parties. This policy applies to all employees and third-parties with access to BuildFire information assets.

POLICY

Asset Inventory

Asset Inventory - Technology - The Information Systems Department must prepare an annual inventory of production information systems detailing all existing production hardware, software, and communications links.

Asset Inventory Contents – Every asset recorded in the Asset inventory must include the following information:

- Asset Name
- Asset Owner

- Asset Location
- Security Classification

Ownership and Classification

Asset Ownership - All production information technology assets used by BuildFire must have a designated owner with ownership responsibilities clearly documented.

Security Classification - Every BuildFire production system asset must be assigned a security classification.

Equipment Authorization

Only Company Owned Devices - Employees must not use personal computing devices to store or process BuildFire information. All mobile devices used for BuildFire business purposes must be issued by the Information Technology department.

Issuing Electronic Media – All electronic media used to store confidential BuildFire information must be issued by the Information Technology Department.

Equipment Configuration

Approved Security Configuration – All computer and communication equipment issued to users, including personal computers, mobile devices, and smart phones, must be configured according to standards approved by the Information Security Department if these devices store or process sensitive information.

Malware Scanning Enabled – As part of the standard configuration, all BuildFire computers issued to a user must have an approved anti-virus/anti-malware software system continuously running.

Property Removal and Return

Mobile Devices Returned - All BuildFire issued storage media, including mobile devices, must be returned to BuildFire when no longer in use by employees or contractors.

Disposal of Electronic Media

Media Disposal – All BuildFire electronic media must have the hard drives properly sanitized of all data before disposal or release to a third party.

Storage Media Destruction - Destruction of sensitive information captured on computer storage media must only be performed with approved destruction methods including shredders or other equipment approved by the Information Security Department.

Release of Computer Equipment and Media

Devices Must Not Be Resold - BuildFire storage devices such as hard-drives, PDA's, electronic cameras and cell phones which store Sensitive data must not be resold or recycled. These devices must be destroyed using sensitive information destruction procedures established 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.

Production Information System – Any computer or communication system that is used to support day-to-day operations, including any systems used to support customer or store sensitive data in any way.

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: 04.01 Asset Management
ISO/IEC 27002: 8.1 Responsibility for Assets

APPROVAL AND REVISION HISTORY

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