www.buildfire.com

Information Security Policies

Physical Security Policy

Policy #	IS-13	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 establishing physical access controls at BuildFire locations and for establishing physical and environmental security protection for buildings that house production information systems.

SCOPE

This policy applies to all BuildFire employees and third-parties with access to BuildFire information assets from mobile devices.

POLICY

Access Control

Security Perimeter - Access to every BuildFire area that contains sensitive information must be controlled by a clearly defined security perimeter.

Physical Access Control Approval - Only approved BuildFire personnel must be granted a key that allows physical access to the building and secure areas.

Physical Access Control To Sensitive Information - Access to every office and work area containing sensitive information must be physically restricted to limit access to those with a need to know.

Guarded Access - All third party access to BuildFire offices containing sensitive information must be controlled by guards, receptionists, or other staff.

Access Control Monitoring

Access Control System Records - The Security Department must maintain records of the persons currently and previously inside BuildFire buildings and securely retain this information for at least three months.

Keys and Access Badges

Badge-Controlled Access - Each person must present his or her key before entering every controlled door within BuildFire premises.

(This would be a good idea for the future. This is best practice)

Identification Badges - When in BuildFire secure buildings or facilities, all persons must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible to all people with whom the wearer converses.

Visitors

Visitor Badge - Identification - All visitors must be provided with a badge that clearly identifies them as a non-employee.

Escorting Visitors - Visitors to BuildFire offices must be escorted at all times by an authorized worker.

Unescorted Visitors - Whenever a worker notices an unescorted visitor inside BuildFire restricted areas, the visitor must be questioned about the purpose for being in restricted areas, then be accompanied to a reception desk, a guard station, or the person they came to see.

Data Center Access Control

Computers and Communications Systems Access – Data Centers or other buildings that house BuildFire computers or communications systems must be protected with physical security measures that prevent unauthorized persons from gaining access.

Facility Location Monitoring - Video cameras or other access control mechanisms that monitor the entry and exit points to secure areas must be in place.

Intrusion Protection

Intrusion Alarms - All BuildFire computer data centers must be equipped with physical intrusion alarm systems that automatically alert those who can take immediate action.

Doors – Data center rooms must be equipped with riot doors, fire doors, and other doors resistant to forcible entry.

Environmental Controls

Alarm Systems - All BuildFire computer data centers must be equipped with fire, water, and physical intrusion alarm systems that automatically alert those who can take immediate action.

Fire Protection - Local management must provide and adequately maintain fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environment protection systems in every BuildFire computer data center.

Water and Flood Protection - All BuildFire data center locations that house computer and communications equipment must meet minimum water damage prevention requirements and minimum water damage alarm precautions established by the Director if IT Services. These include being above ground level and above flood levels of nearby rivers and sewers, having adequate drainage, and not being situated immediately below water tanks or water pipes.

Surge Protection - If weather and building conditions pose a significant risk of static electricity discharge, all personal computers and workstations must be outfitted with static protection equipment that has been approved by the Information Technology Department.

Backup Power Utilities - All new BuildFire computer or communications centers must be located and provisioned such that they have ready access to two electrical power substations and two telephone central offices and two Internet providers. Unless cost prohibitive, the redundant paths for each respective utility should be across separate areas of the campus.

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.

Data Center – Any physical room or building that houses computer or communications equipment. This includes any third party facilities that host BuildFire systems.

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.

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: 10.01 Physical Access Control
ISO/IEC 27002: 11.1 Secure Areas

APPROVAL AND REVISION HISTORY

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