www.buildfire.com

Information Security Policies

Mobile Computing Security Policy

Policy #	IS-12	Effective Date	03/01/2017	Email	policy@buildfire.com
Version	1.0	Contact	Daniel Hindi	Phone	(949) 899-8204

Table of Contents

Purpose 1
Scope 1
Policy 1
  Issuing of Mobile Devices 1
  Configuration and Access Management 2
  Sensitive Information Storage 2
  Remote Access 2
  Physical Security Protection 2
Violations 2
Definitions 3
References 3
Approval and Revision History 3

PURPOSE

This policy defines the information security requirements for the protection of sensitive information on all BuildFire mobile and portable computing devices.

SCOPE

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

POLICY

Issuing of Mobile Devices

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

Approved Configuration of Mobile Computing Devices – Mobile computing devices must not be used to store BuildFire business information unless they have been configured with the necessary controls and approved for such use by the Information Security Manager.

Writable Media – All portable storage media (USB, CD/DVD-RW) used to store or process sensitive BuildFire information must be issued by the Information Technology Department.

Configuration and Access Management

Mobile Device Encryption - All mobile computing devices containing sensitive BuildFire information must consistently employ both hard-disk encryption for all such files, and wherever possible, startup and screen-saver-based password\boot protection.

Changes to Configurations And Software -, Employees must not change the operating system configuration or install new software On BuildFire-supplied mobile devices unless this software has been approved by the Information Technology group..

Sensitive Information Storage

Approval for Storage of Sensitive Data - All mobile computing devices used to conduct any BuildFire business must be approved by the Information Security Department for use with the information appropriate for the normal business activities of the individual user.

Ownership of Information - The information stored in BuildFire portable computer equipment is BuildFire property, can be inspected or used in any manner at any time by BuildFire and, like the equipment, it must be returned to BuildFire or wiped clean at the time Employees are no longer employed by BuildFire.

Remote Access

Authorized Access Points – Al remote access into BuildFire networks by mobile devices must pass through a central access point authorized and controlled by the Information Security Department.

Physical Security Protection

Locking Personal Offices - All Employees with separate personal offices that handle sensitive information should lock the doors when these offices are not in use or otherwise unattended.

Leaving Mobile Devices Unattended - Employees must keep BuildFire portable computers containing BuildFire information in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.

Mobile Devices Stored Out of Site – All portable devices in the possession of BuildFire personnel must be stored in a secure location, such as a locked file cabinet or drawer, when not in use. Under no circumstances should portable devices be left in open view on desks or in public areas.

Checked Luggage - Employees in the possession of portable computers containing sensitive BuildFire information must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage.

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.

Mobile Computing Devices - Mobile computing assets include, but are not limited to: laptop, notebook, tablet, desktop computers, all personal wireless-enabled devices, including smart phones, cellular phones, mobile email devices, PDAs and other hybrid devices, and all portable storage media, including flash drives, smart cards, tokens, etc.

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: 4.8 Mobile Computing
ISO 27002 - 6.2 Mobile devices and teleworking

APPROVAL AND REVISION HISTORY

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