www.buildfire.com

Information Security Policies

Acceptable Use of Assets Policy

Policy #	IS-08	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 acceptable use of all BuildFire computer and communication system assets.

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

System Usage

Reasonable Personal Use Of Systems - BuildFire allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use must be consistent with conventional standards of ethical and polite conduct.

Use at Your Own Risk - Users access the Internet with BuildFire systems at their own risk. BuildFire is not responsible for material viewed, downloaded, or received by users through the Internet.

Activity Monitoring – Users must be aware that their internet activity while using BuildFire systems is monitored and recorded. This information may include web sites visited, files downloaded, time spent on the Internet, and related information.

No Guarantee of Message Privacy - BuildFire cannot guarantee that electronic communications will be private. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others.

User IDs and Passwords

Personal User IDs Responsibility - Users must be responsible for all activity performed with their personal user IDs. They must not permit others to perform any activity with their user IDs, and they must not perform any activity with IDs belonging to other users.

Access Code Sharing Prohibited - BuildFire computer accounts, user IDs, network passwords, voice mail box personal identification numbers, credit card numbers, and other access codes must not be used by anyone other than the person to whom they were originally issued.

Strong Passwords – When creating accounts on any third-party web site (for example Office 365) users must choose strong passwords that conform to the BuildFire password standard. Exceptions can be made for sites that do not support the current Password Complexity Standard.

Password Complexity Standard - Each password must contain at least one number, one special character and be at least eight characters long. Passwords must also be difficult to guess. For example, users must not choose a dictionary word, derivatives of user IDs, or details of their personal history, a common name, or a word that is easily guessed.

Voicemail Passwords – Users must change the default passwords on any voicemail system used to store messages containing BuildFire information.

Electronic Messaging

Identity Misrepresentation - Users must not misrepresent, obscure, suppress, or replace their own or another person's identity on any BuildFire electronic communications.

Handling Attachments - All electronic mail attachment files from third parties must be scanned with an authorized virus detection software package before opening or execution.

Responding to Personal Information Requests – BuildFire workers must never respond to electronic mail messages that request personal or sensitive company information, even from internal sources. The BuildFire Information Systems (IS) department will never request that you perform security duties, such as changing your password, via electronic mail. Any such requests will be confirmed with separate communication from management.

Harassing Of Offensive Materials - BuildFire computer and communications systems are not intended to be used for, and must not be used for the exercise of the workers' right to free speech. These systems must not be used as an open forum to discuss BuildFire organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited.

Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.

Internet and Web Usage

Disclosing Internal Information - Employees must not publicly disclose internal BuildFire information by posting to any web site, including blogs, newsgroups, chat groups, photo sharing or social networking sites.

Blocking Sites and Content Types - The ability to connect with a specific web site does not in itself imply that users of BuildFire systems are permitted to visit that site. BuildFire may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include graphic and music files.

Approved Business Sites – User must only use third-party web sites and applications for BuildFire business if these same sites have been approved by management.

****Note**: You can include a specific list here or refer to another list.

Data Storage

Establishing Third-Party Networks - Users must not establish any third-party information storage network that will handle BuildFire information (file sharing, blogs, cloud storage) without the specific approval of the Information Security department.

External Storage Checking - Externally-supplied CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses.

Prohibition Against All Forms Of Adult Content - All forms of adult content (pornography or what some would consider to be pornography) are prohibited on BuildFire computers and networks. This includes content obtained via web sites, email attachments, CD-ROMs, and file sharing networks.

Copyright Protection

Trusted Software Scanning - Employees must not use any externally-provided software from a person or organization other than a known and trusted supplier unless the software has been scanned for malicious code and approved by the Information Security Department or a local information security coordinator.

Unauthorized Software And Data Copies - BuildFire strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet users or other system users make unauthorized copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by BuildFire. Likewise, BuildFire allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

Personal Equipment

Current Virus Software- Every BuildFire employee who processes or stores BuildFire information must install and regularly run the most current version of a virus detection (malware detection) software package approved by the Information Security Department.

Installation Of Software - Users must not install software on their personal computers, network servers, or other machines without receiving advance authorization to do so from the Information Security Manager.

Sharing Systems Prohibited - Employees must not share their personal computer, if it is used for BuildFire business, with any other person.

Unattended Active Sessions - If the computer system to which they are connected or which they are using contains sensitive information, users must not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

Physical Security

Locking Sensitive Information - When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

Security Incident Reporting

Reporting Security Events – Any suspected events that may compromise information security or are known to violate an existing security policy must be immediately reported to the Information Security Manager or the Help Desk. Examples of these events include:

- Any unauthorized use of BuildFire information systems;
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed;
- All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages;
- Suspected or actual disclosure of Sensitive BuildFire information to unauthorized third parties.

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.

Third Party – Any non-employee of BuildFire who is contractually bound to provide some form of service to BuildFire.

Third Party Web Sites – Any web site or application not owned or operated by BuildFire, but used to perform day-to-day business. Examples including cloud storage and email systems such as Office 365.

User - Any BuildFire employee or partner who has been authorized to access any BuildFire electronic information resource.

REFERENCES

CPL: 4.5 Acceptable Use of Assets
ISO/IEC 27002: 8.1.3 Acceptable Use of Assets

APPROVAL AND REVISION HISTORY

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