www.buildfire.com

Information Security Policies

Network Security Management Policy

Policy #	IS-11	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 secure networks that connect to BuildFire production computer and communications systems, including those managed by third-parties.

SCOPE

This policy applies to all BuildFire production information systems. This policy applies to all employees and third-parties with access to BuildFire information assets.

POLICY

Firewalls and Internet Access

Internet Access - All Internet access using BuildFire computers must be routed through a firewall or similar device that provide firewall functionality.

Firewalls and Intrusion Prevention

Network Firewalls – All networks which provide access to BuildFire production applications must be protected by a firewall or similar device that provide firewall functionality.

Intrusion Detection – All networks which provide access to BuildFire production applications must be protected by an intrusion detection system (IDS) that is periodically updated to detect the latest threats.

Wireless Networks

Approved Wireless Access Points - Only those wireless networks that have been issued by the Information Technology Department or otherwise approved by management will be used to access BuildFire information and system assets.

Secure Network Access Points - To prevent tampering, reconfiguration, theft, and other unauthorized activity, all wireless network access points must be physically secured in areas accessible only by authorized personnel.

Vendor Defaults - Wireless - All vendor default settings on wireless equipment must be changed.

Wireless Default Service Set Identifiers - All default service set identifiers (SSIDs) on wireless networks must be changed.

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.

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.

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: 9.0 Access Control
ISO/IEC 27002 – 11 Access Control

APPROVAL AND REVISION HISTORY

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