www.buildfire.com

Information Security Policies

Access Control Policy

Policy #	IS-10	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 access to BuildFire production computer and communications systems, including those managed by third-parties. Note: BuildFire exclusively uses third-party ("cloud") service providers to support the IT infrastructure.

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

Access Restrictions

Access Control - All BuildFire technology platforms (i.e. network, operating system, application, and database) must authenticate the identity of users using unique user IDs and passwords.

Privilege Restriction - Need To Know - The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know and based on the users role within the organization.

Access Authorization

Access Control Authorization - Requests for the addition, deletion, and modification of all user IDs, credentials, and other identifier objects on BuildFire computer and communications systems must be authorized by the worker's immediate supervisor or manager.

Account Categorization

Account Categorization – All accounts created on BuildFire systems must fall into one of two categories, each designed for different levels of control and security. Accounts and corresponding passwords must fall into the following two categories:

- **User Account (Identity)** – This account may represent a human being and therefore that password determines identity e.g. an active directory user account – the password on the account is the secret known by the human that identifies that human to the system. An identity password should not be associated with a privileged account but rather a regular user account.
- **Privileged (Non-Identity) Account** – Non-identity accounts are not associated with a specific human being, but a system or service (for example system account like UNIX root or a service account) The passwords on these accounts do not provide for any identity of a human and therefore do not need to be memorized. These passwords can be set to very large values and stored in the privileged account

User ID and Account Management

Unique User IDs - Each computer and communication system User ID must uniquely identify only one user. Shared or group user IDs must not be created or used.

Reuse Of User IDs - Each BuildFire computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with BuildFire.

User ID Standard – When a user creates a BuildFire-specific business account on any third party business application (“application”) they must follow the BuildFire user account standard.

Password Requirements

Minimum Password Length - All passwords for User accounts must have at least 8 characters and this length must always be checked automatically at the time that users construct or select their password.

Password Complexity - All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character.

Password Change Requirements – All users must change their passwords according to the change requirements of each third-party business application. All users must change their passwords at least once every 90 days, if this same requirement is not automatically enforced.

Privileged Account Passwords – Fixed passwords for privileges accounts must be at least 23 characters long and contain and at least 2 special characters and 2 numbers.

Privileged User Accounts

Number Of Privileged User IDs - The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

Inventory of Privileged Accounts – BuildFire must maintain an inventory of all privileged accounts and their associated permissions and access and update this inventory at least once annually.

Session Controls

Maximum Logon Attempts – Access control systems must be configured to automatically disable User IDs after four unsuccessful logon attempts.

Account Lockout Duration – All user IDs that have been locked out or disabled must remain locked for a period of at least 30 minutes.

Session Timeout – Access control systems must be configured to automatically logoff users after a period of inactivity of 15 minutes.

Access Records

Access Control System Logging – Production application access control systems must be configured to capture and maintain the following:

- The creation date for every user ID.
- Date and time of the last logon for every user ID.
- Date and time of the last logoff for every user ID.
- Date and time of the last password change for every user ID.
- An expiration date or every user ID that represents the last date that the user ID is active for use.
- Details of addition and changes to the privileges of user IDs.

Access Review

Review Of User Access Privileges - The system access privileges granted to every user must be reevaluated by the user's immediate manager annually to determine whether currently-enabled system privileges are needed to perform the user's current job duties.

Inactive Account Maintenance - All User IDs for employees that are inactive accounts over 90 days old must be either removed or disabled.

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