www.buildfire.com

Information Security Policies

Encryption and Key Management Policy

Policy #	IS-20	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 managing encryption technology used to protect Buildfire applications developed in-house or by third parties.

SCOPE

This policy applies to all Buildfire production application systems. This policy applies to all employees and third-parties responsible for managing Buildfire systems.

POLICY

Authorization

Encryption Process Approval — Systems – All Encryption processes and algorithms used for Buildfire information must be approved by the Information Security Manager.

Algorithms

Standard Encryption Algorithm And Implementation - If encryption is used, government-approved standard algorithms and standard implementations must be consistently employed.

Publicly-Evaluated Encryption Algorithms - Every general purpose encryption algorithm used to protect Buildfire production information and information systems must be open (that

is, the specific mechanisms are publicly disclosed) and must have been evaluated by cryptography experts.

Requirements

Encryption Keys Not Resident In Main Memory - Encryption keys must never be resident in main memory, buffers, or registers on the production computers where they are employed for security processes. Instead they must be resident in peripheral hardware devices known as security modules, key loaders, or other dedicated purpose devices.

User-Chosen Encryption Key Length - Whenever user-chosen encryption keys are employed, the encryption system must prevent users from employing keys made-up of less than 10 characters.

Systems Design Encryption Key Length - Buildfire production system encryption systems employing symmetric algorithms must have a key length of at least 256 bits. Asymmetric algorithms must employ a key length which, in the estimation of the Information Security Department, provides a comparable level of security.

Encryption And Digital Signature Key Separation - If both encryption and digital signatures are used, separate keys must be used for each of these two control measures.

Only Approved Cryptographic Libraries Used in Development - All in-house or third-party developed applications must only use cryptographic controls documented and approved by the Information security department.

Key Management

Encryption Key Management Systems - Buildfire encryption systems must be designed such that no single person has full knowledge of any single encryption key.

Management Responsibility Delegation - Key management responsibility must be delegated only to a party who has passed a background check, passed an operational security audit, and signed a confidentiality agreement.

Data And Encryption Key Transmission - If encryption is used, and if keys are transmitted to a remote party in a readable form, then the information protected with encryption must be transmitted over a different communication channel than the keys used to govern the encryption process.

At Least Two People With Access To Master Keys - At all times, at least two trusted and authorized people must have access to the encryption master keys used to protect production information.

Key Exchange Material Destruction - Custodians of key exchange material must destroy this material according to approved procedures within a reasonable time, not to exceed 10 business days, following the successful verification of a key exchange process.

Private Encryption Key Transmission - If private encryption keys are transmitted over communication lines, they must be encrypted with a stronger algorithm than is used to encrypt other sensitive data protected by encryption.

Public Key Changes - If a public encryption key has been posted on a web server or in another publicly accessible location, all regular correspondents with whom this key has been used must be notified whenever there is a change in this public key.

Compromised Keys - Encryption keys that have been compromised, or revealed to third parties under a key escrow arrangement, must immediately be revoked retroactively to the last time and date when the keys were known to be safe.

Key Management Responsibility - Whenever encryption is used to protect sensitive data, the relevant Owner of the data must explicitly assign responsibility for encryption key management.

Unauthorized Key Substitution - Key management procedures must be implemented to prevent the unauthorized substitution of encryption keys.

Key Custodian Acknowledgement - Encryption key custodians must sign a form specifying that they understand and accept their key custodian responsibilities.

Key Generation

Encryption Key Life - Keys used for encrypting Buildfire data must be changed at least every 90 days.

Encryption Key Expiration - All encryption keys must have a stated life and must be changed on or before the stated expiration date.

Encryption Key Generation - Whenever encryption is used, the keys employed must be generated by means that are not practically discernible by an adversary, and that will yield keys that are difficult-to-guess.

Encryption Key Change Interval - Keys used for encrypting Buildfire data must be changed at least once every year.

Key Security

Encryption Key Disclosure — Approval - Encryption keys are a most sensitive type of information, and access to such keys must be strictly limited to those who have a need-to-know.

Encryption And Digital Signature Key Storage - Keys employed by end users for encryption and digital signatures must always be stored in a tamper-resistant hardware device, such as a smart card.

Backup Encryption Keys - If a Buildfire worker is going to employ encryption for production business information processing activities, the worker must securely deposit backup copies of all keys with the Information Security Department.

Encryption Key Storage Media - If encryption is used to protect sensitive data resident on computer storage media, the encryption keys and related encryption keying materials used in the encryption process must not be stored anywhere on this storage media in unencrypted form.

Encryption Key Duplication - Encryption keys used to conceal backup data must themselves be backed-up and must be stored with security measures comparable to or more stringent than measures applied to the involved backed-up data.

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.

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: 12.1.2. Application Development Security
ISO/IEC 27002: 14.0 Information Systems Acquisition, Development and Maintenance

APPROVAL AND REVISION HISTORY

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