www.buildfire.com

# Information Security Policies

## Policy Exception - Risk Acceptance Memo

| | | | | | |
|---|---|---|---|---|---|
| Policy # | IF-02 | Effective Date | 03/01/2017 | Email | policy@buildfire.com |
| Version | 1.0 | Contact | Daniel Hindi | Phone | (949) 899-8204 |

## INSTRUCTIONS – WHEN TO USE THIS FORM

This form must be employed when:

- An information system, a communications system, or an organizational unit is known to be out of compliance with BuildFire information security policies or standards, and
- The responsible manager does not intend to come into full compliance within a three-month period.

If this out-of-compliance situation is to continue, the brief risk assessment regarding the out of compliance situation must be updated annually, the approvals must be obtained annually, and this form must be signed by the responsible manager annually. Each year the responsible manager must return a signed copy of this form to the manager of the Information Security Department who will keep it on file.

## RISK ACCEPTANCE MEMO

__ Regarding BuildFire policy or standard no.: _____

__ Dealing with the topic of:

_____

_____

I understand that compliance with BuildFire information security policies and standards is expected for all organizational units, information systems, and communication systems. I have read the above-named policy or standard and I believe that the control(s) described therein should not be required for the following:

__ Information system __ Communication system

(Check the relevant choice among the above options and describe below):

_____

_____

_____

_____

I furthermore understand that a control deficiency in one network-connected system can jeopardize other information systems because erroneous data may be inherited, or because a conduit for a intruder to enter BuildFire systems may be created. I also understand that non-compliance in this instance may adversely affect the morale or willingness of staff associated with other systems to comply with information security policies and standards.

I understand that an exception to information security policies and standards is appropriate only when it would:

__ Adversely affect the accomplishment of BuildFire business, or

__ Cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance. I believe that an exception to this policy or standard is warranted because:

_____

_____

_____

I have prepared, or have had a staff member reporting to me prepare, a written assessment of the risks associated with being out of compliance with the above-mentioned policy or standard. This risk assessment has been reviewed and approved by the manager of the Information Security Department and the manager of the Internal Audit Department.

I accept personal responsibility for this situation to be out of compliance with information security policies and/or standards. Personal responsibility does not mean that I am financially responsible for losses that may take place as a result of this out of compliance situation. Personal responsibility does mean that my job performance evaluation, my salary and bonus, and my continued employment status at BuildFire can be jeopardized or damaged if a major loss takes place because this out of compliance situation existed.

I also understand that this exception will expire one year from the date the approvals are obtained.

_____
Signature of Responsible Manager

_____
Printed Name of Responsible Manager

_____
Date Signed

## REFERENCES

ISO/IEC 27002: 4.0 Risk Management
CPL: 2.0 – Information Security Policies

## APPROVAL AND REVISION HISTORY

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