www.buildfire.com

Information Security Policies

Security Incident Reporting Form

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

DESCRIPTION

[This section describes the overall objectives and purpose of this policy document.]

This Sample Incident Reporting Form can be used as a template for your organization. The form is designed to either be printed (on a single sheet) or for easy posting via the intranet or other central document repository. Organizations may wish to refer employees to related documents such as a Data Classification Policy (which defines "sensitive" information) or to remind the employee that they will not be reprimanded for reporting such incidents.

INSTRUCTIONS

Use this form to report any suspected disclosure of sensitive company information to parties not authorized to view the information. Completed forms are classified as confidential information.

Section I – Incident Description (To be completed by the Employee Reporting the Incident)

1. To provide an accurate picture of the organization's privacy commitment, report all incidents, even if they are of a questionable or limited nature. You must notify the Information Security Department.
2. Print (or Type) clearly. Omit your name in item 2 if you wish to remain anonymous.
3. Email, Hand carry (or mail under confidential cover) the completed Form to the following appropriate official:
    a. Mailing Address: 1760 The Alameda Ste 300, San Jose, CA 95126.

Section II – Additional Comments (To be completed by the Incident Response Team responding to the Report)

1. Use Section II to note if local/division management corrected the incident. Explain what action was taken, by whom, and when, if known. Also, use the "Additional Comments" block to add any relevant or pertinent remarks regarding the incident.
2. Forward the Form to the Chief Security Officer. Keep a copy of the form for your internal files. Incident reports with confidential information must be handled according to privacy and security policies and not transmitted electronically without the approved encryption method to secure confidential and other sensitive information.

Section III – Security Officer Comments (To be completed by the Security Officer)

1. Provide comments in Section III describing the type of action taken in this particular incident.
2. Distribute copies of the completed form to the Human Resources Division, the Security Incident File, and other officials involved in the incident.

REFERENCES

CPL: 13 Incident Detection & Management
ISO/IEC 27002: 16.0 Information Security Incident Management
NIST: Incident Response (IR)
HIPAA: Security Incident Procedures 164.308(a)(6)
PCI-DSS: 12.10 Incident Response Plan

APPROVAL AND REVISION HISTORY

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

Section I – Incident Description (To be Completed by Employee Reporting Incident)			
1. Category of Incident or Responsible Parties		2. Name of Person Reporting Incident (Optional)	
3. Location of incident		4. Telephone Number	5. Office
		6. Date of Incident	7. Time of incident
8. Detailed Description of Incident (Include as many details as possible, including which systems were used or compromised.)			

8. Individual(s) Notified (*Check all that apply*)	9. Time & Date Notified	10. Name/Title/Ph No/Address of Person(s)
☐ Information Security Representative		
☐ Information Technology Representative		
☐ Information Security/Privacy Officer		
☐ Manager/Director		
☐ Human Resources		
☐ Other (describe):		

Section II – Additional Comments (To Be Completed by Security Personnel Receiving the Report)
11. Explain Action Taken, By Whom, and When, If Incident Was Corrected by Management. Add Any Other Pertinent or Relevant Remarks.

Section III – Security Officer Comments (To Be Completed by Security Officer)
12. Explain Type of Action Taken in This Incident