



community<sup>TM</sup>force

INFORMATION SECURITY

## Organizational Policy Review Process

**Origin Date:**

January 12, 2008

**Last Revised Date:**

January 10, 2011

**Version: 1.2**

**Owner:**

Muneer A. Baig  
VP Information Security Services

**Contact:**

CommunityForce Information Security

**Executive Sponsor:**

Khaja Syed  
President

## Table of Contents



1. Introduction .....	2
2. Purpose.....	2
3. Scope.....	2
4. Process.....	2
4.1. Development:.....	2
4.2. Publishing:.....	3
4.3. Training and Awareness:.....	3
5. Enforcement:.....	3



## 1. Introduction

IT security policies and guidelines are implemented at CommunityForce in the interests of the entire company – to communicate to all users the kinds of actions that can help or hinder the availability and reliability of IT resources supporting CommunityForce’s mission. To ensure that CommunityForce’s IT security policies and guidelines are fair and reasonable for all staff, employees, contractors, management, clients, suppliers following review process has been put in place.

## 2. Purpose

The purpose of this document is to establish a CommunityForce organizational Information Security Policy Review process to ensure that all policies and procedures stay current with the changing business needs.

## 3. Scope

This process applies across the company to all documented policies and procedure used to conduct CommunityForce business. All employees, vendors, contingent staff, partners, and business guests are accountable and responsible for complying with this process.

## 4. Process

Notice MUST be posted on the CommunityForce Internal website to communicate development of any new policy or procedure document or changes to existing policy or procedure. In addition other means of communication should be used to ensure enterprise wide awareness for any changes.

### 4.1. Development:

For each proposed policy, the VP Information Security will assemble a group of Subject Matter Experts (SMEs). This group will meet to evaluate the need and the required policy or procedure documents. This group will have the following responsibilities:

- a) Identify the key issues and what to include in the policy/guideline.
- b) Determine what is most appropriate for the particular issue: a policy or a guideline.
- c) Collaborate to draft the language of the document.
- d) The draft document will have a two week review period to solicit comments from CommunityForce personnel.
- e) Comments received will be incorporated, where applicable, into the final version .



#### 4.2. Publishing:

Policy document MUST be approved and signed off by the VP of Security services before publishing.

#### 4.3. Training and Awareness:

- a) All training materials MUST be updated to reflect the policy changes.
- b) All CommunityForce personnel MUST be notified of the new policy changes immediately and how it effects their day-to0day tasks..
- c) Brown bag sessions MUST be conducted to solicit information or answer any questions about policy changes.

### 5. Enforcement:

Violations of CommunityForce's Information Security policies or procedures may result in corrective action, up to and including immediate termination of employment, contract or assignment. In some cases, a breach of CommunityForce's Information Security policies or procedures may also violate an international, federal, state, or local law. In such cases, the individual may also be subject to civil and/or criminal liability.

### 6. Revision History

Author	Approved by	Revised on	Version	Comments
Muneer Baig	Khaja Syed	01/12/2008	1.0	
Muneer Baig	Khaja Syed	09/11/2009	1.1	
Muneer Baig	Khaja Syed	01/10/2011	1.2	