



## Acceptable Use Policy

**Origin Date:**

February 12, 2008

**Last Revised Date:**

December 20, 2010

**Version: 1.3**

**Owner:**

Muneer A. Baig  
VP Information Security Services

**Contact:**

CommunityForce Information Security

**Executive Sponsor:**

Khaja Syed  
President

## Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy .....	3
3.1. Requirements .....	3
3.2. Facilities Access.....	4
3.3. Computing Devices.....	4
3.4. Computer Accounts.....	6
3.5. Acceptable Corporate Network Use.....	7
3.6. Account and Password Handling.....	8
3.7. Terminations and End of Contracts .....	9
3.8. Mandatory Application.....	10
3.9. Electronic Messaging (Email).....	10
4. Enforcement .....	11
5. Definitions of Terms.....	11
6. Revision History.....	13

## 1. Purpose

This purpose of this policy is to protect CommunityForce personnel, the corporate network, customer information/data and other business critical information assets. It will establish the requirements for anyone who has been granted access to CommunityForce's network resources. This policy will outline responsibilities regarding the acceptable use of accounts and passwords, building and network access, computing devices, and application usage.

Inappropriate or improper use of CommunityForce's corporate network, resources, and information can expose CommunityForce to risks including virus attacks, compromise of systems and services, as well as legal and regulatory issues.

## 2. Scope

This policy applies to ALL CommunityForce employees, partners, vendors, and third parties who have been granted access to CommunityForce network, its customer information/data regardless of where it resides or what form it takes, the technology used to handle it, or what purpose(s) it serves.

It also applies to any computing or storage device used to connect to CommunityForce's corporate network which may include:

- Desktop or Laptop Computers
- Personal Digital Assistants (PDA's)
- Cell Phones or Digital Cameras
- Copiers or Fax Machines

## 3. Policy

ALL information MUST be protected in accordance with the minimum security controls established in this and other CommunityForce policies to ensure confidentiality, integrity, and availability of information assets.

### 3.1. Requirements

#### a) General Use and Responsibilities

When using CommunityForce owned or leased resource, including the use of the corporate network all of the following apply:

- i. CommunityForce's business information **MUST** be classified as CONFIDENTIAL, HIGHLY SENSITIVE or SENSITIVE in accordance with the Information Classification & Handling Policy regardless of where it resides, what form it takes, or who accesses it;
- ii. CommunityForce owned or leased resources **MUST NOT** be used to engage in activities that are illegal under any local, state, federal or international law;
- iii. Users **MUST NOT** bypass security mechanisms or violate company policies, standards, or procedures;
- iv. Users **MUST NOT** engage in activities that attempt to gain access to systems, information or accounts for which they have not been granted access to and for which they do not have a justifiable business need;
- v. Users **MUST NOT** impersonate anyone else or misrepresent themselves.

### 3.2. Facilities Access

In regard to accessing CommunityForce facilities, the following apply:

#### a) Controlled Entry Doors

Every individual **MUST** appropriately use the access controls on all protected entry doors, the following also applies:

- i. Access controls on doors at **MUST NOT** be circumvented.
- ii. Access controlled doors **MUST** always be closed and locked when not in use.
- iii. If you notice a door is not working properly, you **MUST** immediately contact facilities operations in the lobby to report the problem.

### 3.3. Computing Devices

This section applies to computing devices such as desktops, laptops, personal digital assistant (PDAs), smart phones, printers, faxes, and any device that can process digital information that connects to the corporate network regardless of ownership.

#### a) Accessing CommunityForce or its customer information/data from computing devices

There are instances when it is necessary to grant management access to a user's workstation. This may be just logging on to the machine or it may be retrieving data from the machine of a departed or incapacitated employee. Request **MUST** be from the employee's manager and have Human Resources (HR) and Security approval.

#### b) Compromised Computing Devices

- i. If a system has been compromised, or is suspected of having been compromised, it **MUST** be formatted and rebuilt.
- ii. Regardless of whether any "cleaning" tools were used, the system **MUST** be formatted. These types of tools may not be able to detect secondary vulnerabilities such as malicious code or backdoors which may have been placed on the system as a result of the initial compromise.
- iii. The computer account and all local accounts and domain user passwords used on or for that system **MUST** be changed by the user.
- iv. Users **MUST NOT** transfer or save any executable or system files from the compromised system without approval first from Information Security.

#### c) Lost or Stolen Computing and Digital Storage Devices

If a computing or storage media device (hard drive, USB thumb drives, CD, tape, etc..) that contains CommunityForce business information is lost or stolen, the user **MUST** perform the following as soon as possible:

- i. For lost or stolen systems, all passwords associated with any corporate accounts used to log on to that device **MUST** be changed. If unable to do so, contact Helpdesk for assistance;
- ii. For Smartphones and PDAs contact your service provider
- iii. If customer or employee data was on the device, you **MUST** immediately contact the Information Security Team.

#### d) Auditing & Logging

Auditing is important for protecting users from computer crime and abuse, for detecting possible intruders, and to maintain data integrity.

- i. CommunityForce **MAY** log, review, and otherwise utilize any information stored on or passing through its systems. For these same purposes, CommunityForce **MAY** also capture user activity such as web sites visited and servers accessed.
- ii. All computing devices and systems that connect to the corporate network **MUST** have their auditing capability enabled according to approved audit settings.
- iii. Systems that are joined to CommunityForce managed domains will already have these settings automatically configured via Windows Group Policy Objects (GPOs).
- iv. Audit logs **MUST** never be altered.
- v. Audit logs **MUST** never be deleted by the user and **SHOULD** automatically be set when joining the domain to overwrite when full.

- vi. Users SHOULD review their security logs frequently for unauthorized access and immediately report suspicious activity to Information Security.

e) Accounts Residing on the Computing Device

The following apply to accounts that reside on or come with a computing device that contain CommunityForce business information or that are used to access the CommunityForce corporate network:

- i. Local administrator account passwords MUST be unique and not duplicated across multiple systems. This is to prevent services from running under the same local administrator across environments or more than one system.
- ii. Passwords used for accounts that reside on or come with the system MUST also follow the same password constructions and change rules as for domain account passwords.

### 3.4. Computer Accounts

In order for computer system to join the CommunityForce domain it MUST have a computer account created in the Active Directory (AD). This is usually accomplished during system setup and the computer account object created in the AD will have the same name as the computer. The following apply to computer accounts of systems joined to CommunityForce domains:

- a) Systems MUST NOT have their settings or registry modified to prevent or increase the amount of time the computer account's password automatically changes.
- b) Computer account names MUST NOT be offensive.
- c) Users SHOULD know their system's computer name so it can be provided to security or Helpdesk for deletion if the device is ever stolen or compromised.
- d) This information can be found in under the "System" option in the Control Panel. You can also contact Helpdesk if you need help finding this information.
- e) Computing devices MUST be physically secured from unauthorized users and to help prevent theft of the device.
- f) Computing devices MUST require a password to be entered in order to access information residing on the device.
- g) Computing devices MUST NOT be configured to log on automatically.
- h) Computing devices MUST require a password to be entered before coming out of hibernate mode, a locked state, or to log back onto the corporate network.
- i) Computing devices MUST be configured to automatically lock or log out after no more than fifteen (15) minutes of inactivity.
- j) Non-privileged account will be locked after 3 failed attempts for 30 minutes.

- k) Privileged Service-Accounts and individual accounts with Privileged accounts with administrative access will be disabled after 3 failed attempts.
- l) Computing devices MUST be in compliance and up-to-date with all service packs and hot fixes.
- m) Computing devices MUST be running CommunityForce IT approved anti-virus protection programs.
- n) Non-Microsoft operating systems SHOULD NOT be used on the corporate network unless they are required as part of your job responsibilities and approved by the management. If they are required for business purposes then they MUST stay up-to-date with all patches and have a current anti-virus protection program running at all times.
- o) The registry or other settings on computing devices MUST NOT be modifying in order to disable or circumvent Group Policies or other setting from being applied.
- p) For all devices that can implement BitLocker Drive Encryption (BDE), BDE MUST be enabled for devices that do not have persistent strong physical protection.
- q) Only features and services necessary for the operation and support of a business application or service SHOULD be installed or enabled.
  - For example, services such as SNMP, telnet, and ftp should not be required and therefore be removed or disabled.
- r) Services configured to "Log On" MUST use either the "localservice" or "networkservice" built-in accounts.
- s) Systems MUST NOT have the same service running under the same domain user account on more than one system.

### 3.5. Acceptable Corporate Network Use

In regard to the acceptable use of the corporate network, the following apply:

- a) Access to CommunityForce's corporate network MUST be through approved and valid individual CommunityForce IT assigned accounts.
- b) Anyone who connects to the corporate network from any account or system that is suspected of being compromised, or of being susceptible to serious vulnerabilities, MUST have their access privileges disabled until the situation has been resolved.
- c) Visitors and family members MUST NOT be allowed to access CommunityForce's corporate network or to use it as a way to reach the Internet.
- d) All corporate network perimeter edge devices MUST only be managed and monitored by CommunityForce IT or their authorized delegates.
- e) Users MUST NOT enable routing between any network and the corporate network.

- f) Any wireless access point that is connected to the corporate network MUST be managed by CommunityForce IT and approved by Information Security.
- g) CommunityForce MAY log, review, and otherwise utilize any information stored on or passing through its systems and the corporate network in order to ensure compliance with company policies and standards.
- h) CommunityForce MAY also capture user activity such as web sites visited and servers accessed.
- i) CommunityForce MAY retain and access any device logs, information, or configuration as evidence to respond to audit, legal, HR, or security investigations.

### 3.6. Account and Password Handling

Only current employees of CommunityForce, its subsidiaries and affiliates, contingent staff on assignment at CommunityForce, and vendors who have an approved business need to access the corporate network will be provided accounts.

In regard to the handling of accounts and their passwords used to access CommunityForce information and resources, the following apply:

- a) All passwords used to access the CommunityForce's network or business information MUST be considered and handled as "CONFIDENTIAL" information
- b) Individual user accounts MUST only be used by the individual to whom it was issued;
- c) Passwords and corporate credentials MUST NOT be cached or stored in readable form.
- d) All passwords used to access the corporate network, or used to access resources residing on the corporate network, MUST be changed at least once every 70 days.
- e) All passwords used to access the corporate network, or used to access resources residing on the corporate network, MUST NOT be able to reuse their previous 10 passwords.
- f) Individual user passwords and corporate credentials MUST NOT be shared with anyone.
- g) Anyone with access to CommunityForce systems or to its corporate network MUST take responsibility for selecting and securing appropriate strong passwords;
- h) Passwords not used for domain or network administration MUST be at least 8 characters long.
- i) Passwords used for domain or network administration MUST be at least 15 characters long.

- j) Domain account passwords MUST contain at least 3 of the following; upper and/or lower case letters, numbers, symbols, and punctuation marks.
- k) Domain account passwords SHOULD have at least one number, symbols and/or punctuation mark in the second to sixth positions.
- l) Passwords MUST NOT include words in any language or dictionary.
- m) Passwords MUST NOT be family or pet names.
- n) Password resets MUST only be requested by the actual user.
- o) Password resets MUST be configured to require the password to be changed at the next logon.
- p) Passwords MUST NOT be relayed over the phone.

### 3.7. Connecting to External Resources

While inside the CommunityForce corporate network, employees of CommunityForce, its subsidiaries and affiliates, contingent staff on assignment at CommunityForce, and vendors who have an approved business need to access the corporate network MUST NOT establish connections to services or resources residing outside of the network unless approved business purpose ONLY.

### 3.8. Remote Access (RAS)

Remote access points can be a significant security risk as they are targets for anyone attempting to gain unauthorized and unaudited access into the CommunityForce network. Remote access into or out of the network MUST be configured, controlled and managed by CommunityForce IT or their authorized delegates. The following also apply:

- a) Remote access MUST require the use of VPN Client approved by CommunityForce IT.
- b) Remote access is granted ONLY for business need and MUST be approved by the manager.
- c) Service accounts and other types of shared accounts MUST NOT be enabled for remote access.
- d) Systems connecting remotely to the corporate network MUST NOT have routing enabled between any networks.
  - i. Modifying routing tables with the intention of concurrently connecting to the Internet or other network and the corporate network is strictly prohibited. This includes not enabling Internet Connection Sharing (ICS) while connected to CommunityForce corporate network.
- e) Systems connecting remotely to the CommunityForce corporate network MUST have the Internet Connection Firewall (ICF) turned on.

### 3.9. Terminations and End of Contracts

Regarding terminations and end of contracts, the following apply:

- a) The Employee manager MUST collect all CommunityForce assets and resources.
- b) Immediate or urgent terminations, the Manager MUST notify CommunityForce IT immediately..
- c) Non-immediate terminations or end of contracts, the employee's manager MUST follow the termination procedures.
- d) When employment status changes from an employee to a non-employee (contractor) the account MUST be deleted and recreated in order to make sure all access and privileges granted based on employment status are removed.

### 3.10. Mandatory Application

The following applies to computing devices that connect to the corporate network, regardless of ownership or function:

- a) Computer systems MUST be kept up-to-date with the appropriate service packs and hot fixes.
- b) Users are responsible for making sure systems and applications are kept up-to-date with patches, fixes, and end-user licensing agreements (EULA).
- c) Laptops and Desktop MUST have the CommunityForce IT approved anti-virus software running and "active".
- d) Servers MUST have the CommunityForce IT approved anti-virus software running and "active", at a minimum, on all operating system volumes and shared folders on the system.

### 3.11. Electronic Messaging (Email)

The following applies to electronic messaging:

- a) Manager's requests to access their employee's email MUST go through their senior management.
- b) When sending or replying to email, user's MUST make sure only those authorized to receive the information are on the email.
- c) Users MUST only use their CommunityForce corporate email accounts to conduct CommunityForce business.
- d) Users MUST NOT forward CommunityForce HIGHLY SENSITIVE or CONFIDENTIAL business information to personal accounts.
- e) Users MUST NOT configure their accounts to auto-forward.
- f) Digitally signed email sent from CommunityForce aliases MUST only be signed with a certificate that was issued by CommunityForce.

- g) Users MUST NOT engage in misrepresenting, obscuring, suppressing, or replacing the sender's identity in electronic messaging.
- h) Users MUST NOT modify the internal mail transport header to forge a routing path an electronic message takes through the Internet.
- i) Cracking tools MUST NOT be used on password-protected email files, except by the owner of the file or by CommunityForce Information Security.

## 4. Enforcement

Any CommunityForce employee, partner, vendor, and/or third party found in violation of this policy will be subject to disciplinary action, up to and including termination of employment or contract.

## 5. Definitions of Terms

**Account:** A user or computer object in the Active Directory.

**Accountable:** The property that ensures that the actions of an entity may be traced uniquely to that entity.

**Active Directory:** The Windows-based directory service.

**Asset:** Anything that has value to the organization. Any piece of information or any physical item that can be linked to CommunityForce's business objective is an asset.

**Assurance:** Being confident that the information upon which decisions are based is reliable, confidential, secure and available when needed.

**Authentication:** The act of establishing or confirming the identity of something or someone as genuine.

**Authorized:** Given official permission.

**Availability:** The property of being accessible and usable upon demand, by an authorized entity.

**Computing Devices:** Any device that contains a processor or is capable of processing digital information is a computing device.

**Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**Controls or Safeguards:** Limits and restrictions that are meant to protect business assets and minimize risk.

**Digital Information Asset:** An information asset in electronic form.

Environment: A set of external factors and conditions influencing activities, including physical surroundings.

Information: Any type or combination of written or spoken words, numbers, characters, or images in visual, audio, or digital form.

Information Assurance: Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

Information System: One or a combination of devices that operate together in a systematic way. Systems may include computers, network devices, applications software, and automated services. It includes operating systems, hardware, business applications, off-the-shelf products, software services, and user-developed applications.

Infrastructure: The basic facilities, hardware, software, and services needed for the functioning of an organization and or an information system.

Integrity: The property of safeguarding the accuracy and completeness of assets.

Resource: Any piece of information or any physical item that is owned by CommunityForce or provided by CommunityForce in order to meet a business objective.

Non-Repudiation: The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later.

Procedure: A series of instructions, tasks, or steps that produce repeatable results.

Policy: Overall intention and direction as formally expressed by management. (ISO/IEC 17799:2005)

Principles: General high level ideas, values, and guiding rules which form the underlying assumptions for the development of standards and procedures.

Privacy: The rights and responsibilities of an individual or organization with respect to the collection, use, retention, and disclosure of personal data.

Privileges: The authority to conduct specific functions or tasks.

Risk: Combination of the probability of an event and its consequence.

Storage Device: Anything that stores or holds information.

Threat: A potential cause of an unwanted incident, which may result in harm to a system or organization.

Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats.

## 6. Revision History

Author	Revised by	Revised on	Version	Comments
Muneer Baig	Muneer Baig	02/12/ 2008	1.0	
Muneer Baig	Muneer Baig	10/11/2009	1.1	
Muneer Baig	Muneer Baig	12/20/2010	1.2	