



community^{force}TM
INFORMATION SECURITY

Anti-Virus Policy

Origin Date:

January 17, 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..... 1
- 2. Scope 1
- 3. Policy..... 1
 - 3.1. Ownership Responsibilities 1
 - 3.2. Virus detection software 1
 - 3.3. Monitoring..... 2
- 4. Enforcement..... 2
- 5. Definitions..... 2
- 6. Revision History..... 3



1. Purpose

This purpose of this policy is to establish information security requirements and ensure that all computer systems that are connected to CommunityForce's network to access, process, manage or store information/data are not compromised, and that production services and customer interests are protected against malicious software, such as; Viruses, Worms, and Trojan horses.

2. Scope

This policy applies to ALL CommunityForce employees, partners, vendors, and third parties who are CONNECTED TO or CONNECT TO CommunityForce's network as part of assigned roles and responsibilities to access, process, manage information/data. All existing and future equipment, which fall under the scope of this policy section 3.1.1, must be configured according to the referenced documents.

3. Policy

3.1. Ownership Responsibilities

- a) ALL CommunityForce employees, partners, vendors, and third parties are responsible for maintaining up-to-date Anti-Virus software on their systems.
- b) ALL CommunityForce employees, partners, vendors, and third parties are responsible for the security of the corporate production network, adherence to this policy and associated processes. *Where policies and procedures are undefined ALL CommunityForce employees, partners, vendors, and third parties must do their best to safeguard against security vulnerabilities.*
- c) ALL CommunityForce employees, partners, vendors, and third parties are responsible for compliance with all CommunityForce security policies.

3.2. Virus detection software

- d) ALL laptops, desktops, mobile devices (whether owned by CommunityForce, its employees, partners, vendors, and/or third parties) used to access, process, manage or store any information/data MUST have a CommunityForce IT approved virus detection/protection software installed and functioning.
- e) ALL servers accessing, processing, managing or storing any information/data within or outside CommunityForce facilities (whether owned by CommunityForce, its partners, or third parties) MUST have a CommunityForce IT approved virus detection/protection software installed and functioning.
- f) Anti-Virus software in use MUST be capable of receiving and applying anti-virus definition updates automatically when made available by the product's vendor.



- g) Anti-Virus software MUST be configured to receive and apply updates as soon as it is feasible (where testing is required) after being made available.
- h) Anti-Virus software MUST be configured to automatically scan all files received from internal or external sources and used or stored on workstations covered under section 3.1.1 of this policy. This includes but is not limited to files downloaded over the Internet, attached to e-mail messages, retrieved over the corporate network, or provided on a floppy, CD-ROM or DVD.
- i) Personnel are not permitted to disable anti-virus software without the express approval of CommunityForce IT. Disabling of anti-virus software may be allowed for short periods ONLY when necessary to troubleshoot a problem or to install software that requires or recommends that anti-virus software should be disabled during installation.
- j) In the event a virus is detected and the virus detection/protection software is unable to remove it, users MUST contact CommunityForce IT support desk IMMEDIATELY to assist. Do not use the infected workstation or any data storage media (diskettes, CD-ROM, etc.) until the virus is removed.

3.3. Monitoring

CommunityForce IT will be responsible for reviewing all laptops, desktops, mobile devices and servers (whether owned by CommunityForce, its employees, partners, vendors, and/or third parties) to ensure that anti-virus software is installed and functioning properly, and that anti-virus definitions and patches are being updated automatically. Any discrepancies MUST be corrected during the review. Reviews MUST be documented and retained for at least two years.

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

Virus - a software program that attaches itself to another program in computer memory or on a disk, and spreads from one program to another.

Trojan horse - a destructive program that masquerades as being an application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.



Worm - a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

6. Revision History

Author	Revised by	Revised on	Version	Comments
Muneer Baig	Muneer Baig	02/17/2008	1.0	
Muneer Baig	Muneer Baig	10/11/2009	1.1	Inclusion of laptops, vendors, partners and third parties
Muneer Baig	Muneer Baig	12/20/2010	1.2	Inclusion of mobile devices.