



Data Protection Policy

Origin Date:

November 15, 2008

Last Revised Date:

December 20, 2010

Version: 1.2

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. Ownership Responsibilities 3
 - 3.2. Requirements 4
- 4. Enforcement 6
- 5. Revision History 6



1. Purpose

This purpose of this policy is to establish information security and privacy requirements for all CommunityForce and its customer owned information/data that is processed, managed or stored within CommunityForce's and its partner networks is maintained in accordance with the applicable laws and industry regulations for confidentiality, integrity and availability of information/data.

2. Scope

This policy applies to ALL CommunityForce employees, partners, vendors, and third parties who access or have access to CommunityForce or 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.

3. Policy

ALL information MUST be protected according to the minimum security controls that have been developed as safeguards for its assigned classification level to protect the confidentiality, integrity, and availability of these information assets. They MUST be applied to information at all times which includes when information is being developed, stored, accessed, transmitted or discarded.

3.1. Ownership Responsibilities

- a) ALL CommunityForce employees, partners, vendors, and third parties are responsible for protecting and maintain confidentiality, integrity and availability of CommunityForce and its customer information/data at all times.
- b) ALL CommunityForce employees, partners, vendors, and third parties are responsible for the security and privacy of all information/data, based on its classification and adherence to this policy and associated processes. Where information/data classifications is undefined or not labeled ALL CommunityForce employees, partners, vendors, and third parties MUST treat such information/data as sensitive.
- c) ALL CommunityForce employees, partners, vendors, and third parties are responsible for compliance with all CommunityForce security policies.

3.2. Requirements

a) Access

- i. ALL laptops, desktops, mobile devices (whether owned by CommunityForce, its employees, partners, vendors, and/or third parties) used to access, process, manage any information/data MUST have a disk encryption and CommunityForce IT approved data loss prevention technologies installed, configured and functioning.
- ii. Access to any PII information/data SHOULD use two-factor authentication where supported.
- iii. Anonymous, Guest, Everyone, Authenticated Users, and DomainName/DomainUser groups MUST NOT be used to grant access to PII information/data.
- iv. ALL accounts MUST use passwords that meets or exceeds Microsoft standards and controls for passwords
- v. ALL Information systems/databases containing sensitive information/data must be accessed ONLY by authorized personnel, based on their roles and responsibilities, via an approved method:
- vi. An application whose purpose is to broker such access.
- vii. An approved database management server. Direct database access via desktop programs such as TOAD is strictly prohibited.
- viii. Least privileged access, based on roles and responsibilities, to Information systems/databases processing, managing or storing information/data should be granted ONLY by the information asset owner.
- ix. Access to Information systems/databases processing, managing or storing information/data should be modified IMMEDIATELY upon changes in roles or termination of personnel.

b) Storage

- i. CommunityForce employees, partners, vendors, and third parties are not AUTHORIZED to STORE any sensitive information /data on their laptops, desktops, or mobile devices.
- ii. ALL sensitive CommunityForce or its customer information MUST be stored using CommunityForce IT approved encryption technologies.
- iii. ALL databases containing sensitive information MUST be encrypted CommunityForce IT approved encryption technologies.
- iv. ALL file servers containing sensitive information MUST be encrypted CommunityForce IT approved encryption technologies.



- v. ALL backup to tapes or disks MUST be encrypted CommunityForce IT approved encryption technologies.

c) Transmission

- i. All Sensitive information in transit MUST be encrypted using CommunityForce IT approved encryption technologies.
- ii. Sensitive information/ data transmitted over public networks, when required as a business need, MUST be safeguarded with the use of strong cryptography technologies approved by CommunityForce IT, such as SSL/TLS.
- iii. Use of chat and text messaging is NOT permitted for transfer of any information/data regardless of its level of classification or sensitivity.
- iv. Sensitive information/data MAY not be sent via email. If required ONLY secure email solutions approved by CommunityForce IT, such as PKI or SMIME should be used to transmit sensitive information/data.
- v. USE of FTP and other file transfer technologies, other than those approved by CommunityForce IT is NOT allowed.

d) Handling

- i. Sensitive information/data MUST NOT be forwarded, exported, or copied without the information asset owner's express approval.
- ii. Sensitive information/data MUST NOT be exchanged with any third party, without a formal agreement approved by senior management.
- iii. Users MUST NOT delete, alter or dispose of any information asset that is subject to document retention requirements, litigation hold, or audit notification, or if the user has knowledge or anticipation of possible litigation or other legal, regulatory, or investigative action.
- iv. Hard drives and other memory media such as flash memory devices that are no longer usable MUST be destroyed by an irreversible process that would make the recovery of information impossible (e.g., grinding, degaussing or melting).

e) Database Configurations

- i. Databases storing sensitive information/data MUST be configured according to CommunityForce's Database Configuration Guide, which prescribes the application of all severity 1 and 2 directives contained within Database Security Checklist.

f) Encryption

- i. Symmetric algorithms MUST have at least a 128 bit key length (e.g., AES, TripleDES);
- ii. Asymmetric algorithms MUST have at least a 1024 bit key length (e.g., RSA);
- iii. Any encryption solution MUST provide the ability for authorized CommunityForce personnel to recover the encrypted data.
- iv. ALL databases containing sensitive information MUST be encrypted.
- v. ALL file servers containing sensitive information MUST be encrypted.
- vi. ALL backup tapes or disks or other forms of media MUST be encrypted.

g) Key Management

- i. Cryptographic keys used for encryption of production data will be protected against both disclosure and misuse.
- ii. ONLY a limited number of custodians will have access to cryptographic keys.
- iii. Ensure encryption keys MUST be stored in encrypted form.
- iv. Decryption keys MUST not be stored on the local system.
- v. Key-encrypting keys and data-encrypting keys MUST not be stored together.
- vi. ONLY secure distribution methods approved by CommunityForce IT will be used for distribution of cryptographic keys
- vii. Cryptographic key MUST be changed at least annually.
- viii. Cryptographic key not in use or keys that have been potentially compromised MUST be destroyed.
- ix. Old or invalid keys MUST be revoked immediately.

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. Revision History

Author	Revised by	Revised on	Version	Comments
Muneer Baig	Muneer Baig	11/15/2008	1.0	
Muneer Baig	Muneer Baig	10/11/2009	1.1	Encryption technologies updated and key management revised
Muneer Baig	Muneer Baig	12/20/2010	1.2	Transmission, storage and key management revised Handling revised

				Access controls revised
--	--	--	--	-------------------------