



communityTMforce

INFORMATION SECURITY

Enterprise Information Security Policy

Origin Date:

April 12, 2007

Last Revised Date:

November 10, 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.....	2
2. Scope.....	2
3. Policies	2
3.1. Awareness and Compliance:.....	2
3.2. Information Assets:.....	3
3.3. Identity and Access Management (IAM):.....	3
3.4. Resources:.....	4
3.5. Design, Development, Acquisitions, & Deployment:	4
4. Exceptions:.....	4
5. Definitions of Terms.....	4
6. Enforcement:.....	6
7. Revision History.....	7

1. Purpose

This purpose of this policy is to create an overall CommunityForce Business Solutions Inc. (CommunityForce) Enterprise Information Security and Privacy Program (EISPP) that can be used as the foundation for the development and implementing of any organization-specific policies, standards, controls, guidelines, and procedures.

2. Scope

This policy applies across the company to all information and processes used to conduct CommunityForce business. All employees, vendors, contingent staff, partners, and business guests are accountable and responsible for complying with this policy. This includes those located at CommunityForce subsidiaries and locations not owned by CommunityForce such as offshore research and development facilities.

3. Policies

3.1. Awareness and Compliance:

Security of organization is ONLY possible through coordination and collaboration all parties in the organization. Everyone is responsible for security.

- a) When conflicts or omissions exist between this policy and other business policies, contracts, or regulations, the more restrictive requirements allowed by law MUST apply.
- b) Anyone who has access to CommunityForce's information/data, Information systems or facilities MUST be apprised of applicable information security policies and procedures appropriate to their assigned job responsibilities.
- c) Anyone who has access to CommunityForce's information/data, Information systems or facilities MUST be held responsible and accountable for complying with and remaining current on all applicable information security policies and procedures.
- d) Anyone who has access to CommunityForce's information/data, Information systems or facilities MUST immediately report all known or suspected violations of security policies and procedure to Information Security.
- e) Computing or storage devices suspected of violating this policy or any other CommunityForce policies and/or procedures MAY be inspected and/or confiscated by Information Security or their authorized delegates.
- f) All Managers MUST support information security awareness and training and assist in the compliance of security policy and procedures within their area of responsibility

- g) Anyone who is provided an account to access CommunityForce's information/data, Information systems or facilities, whether or not employed by CommunityForce, SHOULD participate in annual security training.

3.2. Information Assets:

- a) Security controls and safeguards, appropriate to the value of the information, MUST be deployed to protect the confidentiality, integrity and availability of information wherever it is and whatever form it resides in.
- b) Information assets MUST only be used for the business purpose it was intended for.
- c) Access to business information MUST be based on the information's classification.
- d) Information necessary for conducting business MUST be backed-up in a secure and recoverable manner.
- e) Critical business processes MUST provide the ability to securely recover from the loss of information assets to an acceptable level through a combination of preventive and recovery controls.
- f) Risks to information assets MUST be identified and reviewed regularly by the information owner to ensure that their related mitigation controls and safeguards are appropriately updated.
- g) For data recovery, investigations, and to ensure business continuity, authorized personnel MUST have the ability to obtain and decrypt any encrypted information used for a business purpose.
- h) All employees, vendors, contingent staff, partners, and business guests MUST return all assets and software licensed to and/or belonging to CommunityForce to their manager upon termination of their employment, contract, or assignment unless otherwise agreed to in writing by CommunityForce.
- i) Sensitive digital information MUST not be stored on any equipment unless authorized by senior management.
- j) Non-sensitive digital information stored on equipment MUST be removed in a non-recoverable manner upon end of employment, contract, or assignment.

3.3. Identity and Access Management (IAM):

- a) Each account provisioned MUST be associated with an authorized individual.
- b) Access to CommunityForce's information/data, Information systems or facilities MUST require authentication.
- c) Access rights and the ability to conduct specific functions and tasks MUST only be granted based on those necessary for performing assigned job responsibilities.

- d) Any change, including technology, environmental, or procedural, that impacts critical business functions MUST go through a formally documented and approved change control process.

3.4. Resources:

- a) CommunityForce reserves the right to scan any device connected to CommunityForce network for compliance to established and approved policies and procedures.
- b) All points of interconnectivity to CommunityForce's network or to any other connected networks MUST be configured, controlled, and managed by CommunityForce IT or its authorized delegates.

3.5. Design, Development, Acquisitions, & Deployment:

- a) All applications and products MUST undergo a security review process.
- b) Information technology designs for applications, systems, and networks MUST include auditing mechanisms and controls to detect unauthorized use and to support incident investigations.
- c) Information technology designs MUST employ protection approaches that address people, process and technology.
- d) Information technology designs MUST ensure that authentication is successful prior to checking authorization rights.
- e) Information technology designs MUST NOT rely upon any single security control or safeguard when more than one is available.

4. Exceptions:

There are no exceptions to the expectations set forth in this policy unless authorized by the policy owner or the

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. 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.

It is also every individual's responsibility to promptly report known or suspected violations of CommunityForce's Information Security policies to Information Security.

7. Revision History

Author	Approved by	Revised on	Version	Comments
Muneer Baig	Khaja Syed	09/12/2008	1.0	
Muneer Baig	Khaja Syed	09/11/2009	1.1	Awareness & Training
Muneer Baig	Khaja Syed	09/10/2010	1.2	IAM