



Information Classification Policy

Origin Date:

September 21, 2007

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. Classification Categories | 1 |
| 3.3. Information Asset Owners..... | 3 |
| 3.4. Classification and Handling | 4 |
| 3.5. Authorization | 4 |
| 3.6. Paper Disposal..... | 5 |
| 3.7. Other Media Disposal..... | 5 |
| 3.8. Encryption – Data at Rest | 6 |
| 3.9. Encryption – Data in Transit..... | 6 |
| 3.10. Event Logging..... | 6 |
| 3.11. Labeling..... | 7 |
| 4. Enforcement | 7 |
| 5. Definitions of Terms..... | 7 |
| 6. Revision History..... | 9 |



1. Purpose

The purpose of this policy is to help CommunityForce employees, partners, vendors, and third parties, who have been granted access to CommunityForce network and its customer information/data, understand the process of how to manage, handle, and process information/data based on the nature or information/data and sensitivity. It should also help them determine what information can be disclosed to non-employees and what should not be disclosed outside of CommunityForce without proper written authorization.

Inappropriate or improper use of CommunityForce's corporate network, resources, and customer information/data 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.

3. Policy

This policy describes the minimum security requirements that apply to information assets based upon their classification. The higher the classification, the greater its potential impact if it were compromised or lost, the tighter the security controls need to be surrounding it.

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. All employees should familiarize themselves with the information labeling and handling procedures.

3.1. Classification Categories

Classification categories are assigned to information assets based upon their value and the potential impact to CommunityForce and its customers in an event of unauthorized disclosure or loss. All information assets MUST be classified and SHOULD be labeled with one of the three Classification designations described below:



a) CONFIDENTIAL

This classification category MUST be assigned to information assets where unauthorized disclosure could cause severe or catastrophic material loss to CommunityForce, the information asset owner, or relying parties. Access to Confidential assets MUST be strictly controlled and limited for use on a "need to know" basis only. Some examples of Confidential may include but are not limited to:

- i. Information that can be used to directly or indirectly authenticate or authorize valuable transactions
- ii. Highly Sensitive Personally Identifiable Information (PII)
- iii. Government-provisioned identification credentials (e.g., social security or driver's license numbers)
- iv. Financial transaction authorization data (e.g., credit card numbers, expiration dates, and credit card ID's)
- v. Financial profiles (e.g., consumer credit reports or personal income statements)
- vi. Medical profiles (e.g., medical record numbers or biometric identifiers)
- vii. Authentication/authorization credentials (e.g., username/password pairs, private cryptographic keys, or numeric identification sequences such as PIN's, hardware, or software tokens)
- viii. Highly sensitive business secrets (e.g., unannounced financials)
- ix. Information under strict regulatory handling requirements could also be under this category (e.g., GLBA, HIPAA, and CA SB1386)

b) HIGHLY SENSITIVE

This classification category MUST be assigned to information assets where unauthorized disclosure could cause serious material loss to CommunityForce, the information asset owner, or relying parties. Access to Highly Sensitive assets MUST be limited for use by only those who have a legitimate business need for access. Some examples of Highly Sensitive may include, but are not limited to:

- i. Personally Identifiable Information (PII) that is not listed as Highly Sensitive PII
- ii. Some Internal CommunityForce's information, such as unreleased product updates, patches, schedules and network infrastructure configurations and/or designs.

c) SENSITIVE

This classification category MUST be assigned to information assets where unauthorized disclosure could result in none to limited material loss to



CommunityForce, the information asset owner, or relying parties. Some examples of Sensitive may include:

- i. Policies, News articles, and Everyday Productivity Education (EPE) guides
- ii. Information that all employees, contingent staff, and those under NDA have been approved to read.

3.2. Information Asset Owners

Information asset owners are the Executive Office Leadership Team, business division heads, and Sales & Operations heads.

a) Responsibilities

All information asset owners are responsible for engage in all of the following:

- i. Classifying all the information assets they are responsible for as either CONFIDENTIAL, HIGHLY SENSITIVE or SENSITIVE.
- ii. Reclassifying information asset as necessary until the information has been appropriately retired or destroyed;
- iii. Immediately notifying Information Security if the information is lost, stolen or otherwise compromised;
- iv. Ensure that inappropriately protected information assets identified by Information Security are mitigated accordingly;
- v. Information asset owners MAY determine that additional protection is required for a particular business asset and MAY choose to require stricter security controls. In such a case, the information asset owner is responsible for documenting the requirements and communicating them.
- vi. Information asset owners MAY assign a delegate to classify designated information assets and/or to answer questions about those assets and their classification.
- vii. When assigning a delegate, an information asset owner does not transfer the accountability and responsibility for ensuring the proper classification has been assigned.
- viii. The delegate MUST also assume responsibility for following the information asset owner's direction and obtaining any approvals prior to releasing or modifying a classification.

b) Information Custodians

Information custodians develop, manage, transmit, maintain, and store information assets as part of their daily work. Regardless of employment status, anyone that does work for CommunityForce is at least an information custodian. It is the



information custodian's responsibility to handle any information they access or have in their care according to its classification. This means that EVERYONE is an Information Custodian and is responsible for managing and protecting information in their care regardless of where they reside or what form the information is in.

3.3. Classification and Handling

The classification of any information asset as CONFIDENTIAL, HIGHLY SENSITIVE or SENSITIVE does not replace the requirements imposed by related legal documents, such as a nondisclosure agreement (NDA) or other contracts. Check with the information asset owner if you have any questions regarding a classification. The following also applies:

- a) All information assets MUST be classified as either CONFIDENTIAL, HIGHLY SENSITIVE or SENSITIVE based upon possible impact to CommunityForce and/or relying parties.
- b) When information assets are not classified or labeled they MUST be handled as HIGHLY SENSITIVE until otherwise labeled by the information asset owner.
- c) Information custodians MUST appropriately retire or discard information assets that have outlived their usefulness.
- d) When information assets with different classifications are mixed together, the protection requirements of the more restrictive classification MUST be used.
- e) When information assets from one classification are aggregated, the entire set of aggregated information MAY require a higher more restrictive classification
- f) Classification of an information asset may be more restrictive than what is specified in any particular contract and MUST be considered a supplemental contract requirement.

3.4. Authorization

CONFIDENTIAL or HIGHLY SENSITIVE information asset, Authorization MUST be restricted to the information asset owner and a minimum number of trusted parties who have a legitimate business purpose, as designated by the asset owner. All of the following MUST also be applied:



- a) Anonymous, Guest, Everyone, Authenticated Users, and DomainName or DomainUser groups MUST NOT be used to grant access to CONFIDENTIAL or HIGHLY SENSITIVE information asset.
- b) CONFIDENTIAL or HIGHLY SENSITIVE information asset MUST NOT be forwarded, exported, or copied without the information asset owner's express approval;
- c) CONFIDENTIAL or HIGHLY SENSITIVE information asset MUST NOT be exchanged with any third party, without a formal agreement approved by senior management.

3.5. Paper Disposal

When disposing of paper documents and files classified as CONFIDENTIAL or HIGHLY SENSITIVE information assets or containing CONFIDENTIAL or HIGHLY SENSITIVE information, the materials MUST be incinerated. The following also applies:

- a) 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.

3.6. Other Media Disposal

When disposing of magnetic, electronic or optical media containing HBI classified information assets, all of the following apply:

- a) Users MUST NOT delete, alter or dispose of any information asset that is subject to document retention requirements, litigation hold, or audit notification, or when the user has knowledge or anticipation of possible litigation or other legal, regulatory, or investigative action;
- b) All whiteboards MUST be wiped clean of any CONFIDENTIAL or HIGHLY SENSITIVE data immediately upon completion of use;
- c) Functioning hard drives MUST be erased using CommunityForce IT approved disk wipe software when they are no longer needed and prior to being reused, sold, or recycled;
- d) 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) Tapes, optical disks (e.g. CD-ROM's, DVD) and floppy disks MUST be shredded prior to disposal.
- f) Optical disks (CD-ROM's and DVD's) MUST NOT be reused and MUST be shredded when no longer functioning.

3.7. Encryption – Data at Rest

Encryption MUST be used when CONFIDENTIAL or HIGHLY SENSITIVE information asset that is being stored (i.e., not actually in transit via wireless or wired connections). The following also apply:

- a) Symmetric algorithms MUST have at least a 128 bit key length (e.g., AES, TripleDES);
- b) Asymmetric algorithms MUST have at least a 1024 bit key length (e.g., RSA);
- c) Any encryption solution MUST provide the ability for authorized CommunityForce personnel to recover the encrypted data.

3.8. Encryption – Data in Transit

When conducting either an internal or external data transfer, or whenever data is in transit, CONFIDENTIAL or HIGHLY SENSITIVE classified information assets MUST always be encrypted. The following also apply:

- a) Symmetric algorithms MUST have at least a 128 bit key length (e.g., AES, TripleDES);
- b) Asymmetric algorithms MUST have at least a 1024 bit key length (e.g., RSA);
- c) Any encryption solution MUST provide the ability for CommunityForce to recover the encrypted data.

Approaches for encrypting the transport would be to simply configure SSL directly on the front-end web server, or configure "SSL proxy" mode on an encryption accelerator to re-encrypt data to the front-end server. An unacceptable approach would be to configure SSL to terminate on an encryption accelerator device and then forward the data in clear text to the destination web server. In other words, CONFIDENTIAL or HIGHLY SENSITIVE data MUST always be encrypted while in transit (i.e. "on the wire").

3.9. Event Logging



For any information asset classified as CONFIDENTIAL or HIGHLY SENSITIVE all of the following applies with regard to event logging:

- a) Log logon events, account management changes, policy changes, system events and content modification MUST all be logged;

3.10. Labeling

All information assets SHOULD be labeled based on their level of classification as "CONFIDENTIAL, HIGHLY SENSITIVE or SENSITIVE".

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 | 09/21/2008 | 1.0 | |
| Muneer Baig | Muneer Baig | 06/11/2009 | 1.1 | Classification Levels Changed |
| Muneer Baig | Muneer Baig | 12/20/2010 | 1.2 | Handling requirements added |
| | | | | |
| | | | | |
| | | | | |