



Incident Reporting and Handling Policy

Origin Date:

January 12, 2008

Last Revised Date:

December 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. Introduction	2
2. Purpose.....	2
3. Scope.....	3
4. Policy	3
4.1. Roles and Responsibilities	3
4.2. Detecting and Reporting	4
4.3. Dealing with Viruses, Worms, and Trojans:.....	5
4.4. Incident Handling	5
4.5. Documenting Incidents	6
4.6. Evidence Gathering	6
4.7. Eradication and Recovery	7
4.8. Follow up Analysis	7
5. Publishing:	8
6. Training and Awareness:	8
7. Definitions	8
8. Enforcement:.....	9
9. Revision History.....	9

1. Introduction

Threats against accessible computer systems networks are becoming more prevalent and sophisticated in nature. Weaknesses inherent in almost all computer operating systems, many support services and network applications that can be exploited in a variety of ways e.g.,

- Intruders gaining privileged status
- Viruses, Worms, Trojans, etc.
- Denial of Service attacks

Computer systems and/or network compromises can cause significant damage to CommunityForce's organizational reputation, customer confidence, Information Technology resources and potentially harm other systems and networks via compromised systems.

CommunityForce and its employees, vendors, contingent staff, partners, and business guests need to be vigilant and proactive in reporting any anomalies in the desktops, laptops, mobile devices or server behavior. Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of employees and the company as a whole.

2. Purpose

The purpose of this Policy is to establish a framework to ensure that all 'security incidents' that occur or are suspected of having occurred on any part of the CommunityForce Information Technology Infrastructure are handled and reported in a structured and consistent manner.

Information security breaches if not handled properly can significantly impact the business reputation, result in loss of sensitive data, violate privacy laws or regulations and result in heavy fines of loss of customer confidence.

This policy will establish procedures that ensure:

- a) Incidents are properly reported
- b) Incidents are handled by appropriate authorized personnel with 'skilled' backup as required
- c) Incidents are properly recorded and documented

- d) All evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- e) The full extent and implications relating to an incident are understood
- f) Incidents are dealt with in a timely manner and service(s) restored as soon as practical
- g) Weaknesses in procedures or policies are identified and addressed

3. Scope

This policy applies across the company to all employees, vendors, contingent staff, partners, and business guests.

4. Policy

In the case of a security incident that threaten or has a potential to threaten the confidentiality, integrity and availability of CommunityForce or its customer information/data all CommunityForce employees, partners, vendors, and third parties are responsible for ensuring that information security reported to Information Security. CommunityForce information security team is the final authority in handling the incident and developing a response plans for all stakeholders.

Platform, operating system and application specific procedures will be produced and advertised by the Information Security. Systems managers, IT support staff, Network and systems administrators must familiarize themselves with this Policy and the specific recommendations pertaining to their areas of work.

4.1. Roles and Responsibilities

The Information Security team will have overall responsibility and authority for managing all reported security incidents. Specific responsibilities for handling certain incidents or aspects thereof will lie with other groups, these are:

- a) System Managers - for incidents that span systems or areas where they have managerial authority
- b) Systems/Network Administrators - for incidents that affect their systems and networks.
- c) Web masters - for web related incidents.
- d) IT support staff - for incidents involving end users
- e) Users - for incidents that affect them or that they initiate

These groups must work with or under the direction of the Information Security. If disciplinary or legal proceedings are indicated then relevant, sustainable and reliable evidence must be submitted to the appropriate law enforcement authorities.

4.2. Detecting and Reporting

'Incidents' will be detected via a variety of methods and may involve employees, vendors, contingent staff, partners, and business guests:

a) External events:

- i. Scans or Probes detected on external systems.
- ii. Intrusion Detection Systems (IDS) Alerts
- iii. Intrusion Prevention Systems (IPS) Alerts
- iv. Firewall and gateway router Alerts
- v. Complaints received from external network/systems administrators or users.

External events detected should be reported via e-mail or telephone to Information Security team. Once reported Information Security team will:

- i. Notify relevant support personnel and user to validate the incident.
- ii. Remove or block the systems(s) from accessing the campus network until the incident has been resolved.
- iii. Secure the system and evidence for investigation.
- iv. Assess the need for notifying law enforcement agencies.
- v. Communicate illegal activities to the Senior Management.

b) Internal events:

- i. Network/systems administrators detect incidents or potential incidents during the course of their work
- ii. System or application log files
- iii. Monitoring system parameters
- iv. Monitoring data communications facilities
- v. Reports received from users or other sources
- vi. Virus, Worms, Trojan, etc.
- vii. Users complaining about a particular topic
- viii. Notice inappropriate material on a system monitor
- ix. Receive defamatory or suspicious e-mail
- x. Notice unusual file store activity
- xi. Notice unusual login times and dates
- xii. Experience problems accessing IT resources

Such incidents should be reported via e-mail or telephone to Information Security team.

Once reported Information Security team will:

- i. Notify relevant support personnel and user to validate the incident.
- ii. Remove or block the systems(s) from accessing the campus network until the incident has been resolved.
- iii. Secure the system and evidence for investigation.
- iv. Assess the need for notifying law enforcement agencies.
- v. Communicate illegal activities to the Senior Management.

4.3. Dealing with Viruses, Worms, and Trojans:

Employees and information technology support professionals MUST report all security incidents including the ones involving viruses, worms, and Trojans that pose a significant threat to CommunityForce and its business environment. Because viruses and worms can reduce the functionality or otherwise affect the company computing and communication environment, Employees and information technology support professionals are expected to:

- a) prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring, and
- b) take immediate action to prevent the spread of any acquired infections from any computers under their control.

Assistance is available from local information technology support professionals and from CommunityForce-wide Information Technology.

4.4. Incident Handling

Once an Incident has been detected and reported it must be handled as follows:

a) Impact Assessment

An impact assessment will be performed at regular intervals; this will generally be done by the Information Security team in collaboration with person reporting the incident and any other stakeholders. The object of the impact assessment is to categorize the incident, determine its likely impact and allocate the most appropriate resources to handle it. CERT provides generic incident classifications for computer systems as follows:

- i. Compromise of integrity - Virus or serious system vulnerability
- ii. Denial of Service - Service has been disabled or network bandwidth saturated
- iii. Misuse - Unauthorized use of account or other breaches of acceptable use
- iv. Damage - Data destroyed or reputation impacted

v. Intrusions - Breaches of systems security

In addition security 'Risk assessments' will be available for core systems and services, which will aid the Information Security team and other stakeholders in providing an accurate Impact assessment. Once the Impact has been assessed an 'Impact level' will be assigned indicating the seriousness of the incident as follows:

High Impact Level: The incident has seriously affected CommunityForce's Information Technology resources or reputation and will require immediate action. Any incident involving Law enforcement agencies will have an automatic High Impact level.

Medium Impact Level: The incident has affected CommunityForce's Information Technology resources and should be dealt with as soon as possible.

Low Impact Level: The Incident won't immediately affect any elements CommunityForce's Information Technology resources but has a potential to cause damage or affect CommunityForce's Information Technology resources. Such incidents should be monitored in case the impact level changes.

4.5. Documenting Incidents

Documenting events will be critical to effective investigation and successful 'Incident handling'. Poor documentation is the most common cause of bad or inappropriate 'Incident handling'. It is essential to document all events, names, dates, and times in detail and as they occur; this may be done electronically or by hand. Screenshots and photographic images can provide valuable and unambiguous evidence in certain cases. Detailed documentation must be done throughout the incident handling process as this will provide the audit trail and evidence for detailed analysis and proposed courses of action.

4.6. Evidence Gathering

Evidence gathering relates to the identification, capture and recording of data relevant to the incident investigation. Information Security team has the authority to inspect any system that is deemed to be part of an incident investigation. Evidence MUST be gathered in a manner that ensures the integrity of the data and establishes an evidence chain of custody. Since the process of gathering evidence may lead to the disclosure of sensitive, restricted or personal information only authorized trained Information Security personnel may undertake this task. Evidence gathering may also involve systems not directly implicated in the incident e.g., Router, IDS, BootP/DHCP, and e-mail logs, building access (sign in) books, surveillance videos etc; in such circumstances the Information Security team will engage with the relevant providers to obtain evidence. It

is essential that internal system clocks be synchronized via the Network Time Protocol, NTP, to ensure accurate correlation between evidence gathered from system logs. Certain incidents may require a more rigorous forensic analysis approach to be undertaken. Forensic analysis techniques would be used to discover and record evidence that established the following:

- a) What happened
- b) Where it happened
- c) When it happened
- d) Who was responsible
- e) How it was done

Forensic evidence gathering requires that everything be documented in a form that is capable of recreating the exact steps that were followed to gather the evidence. The evidence itself must not be altered or contaminated and a chain of custody must be maintained; RFC-3227 provides a best practice guide.

A chain of custody consists of the logs containing dates, times and signatories of the personnel who had custody of the evidence.

4.7. Eradication and Recovery

It will be necessary to get rid of all artifacts associated with the incident and recover any systems and services affected; this might involve:

- a) A forensic analysis if incident and assessment warrants
- b) Removing 'illegal' copyright material, offensive or defamatory material, Trojans, root kits, scanners or sniffers
- c) Re loading systems or network equipment to last known good working state
- d) Re installing operating systems
- e) Re instating file systems and user data
- f) Applying all operating system, applications and manufactures recommended security patches

Once all artifacts have been removed and all affected systems or services recovered then under the direction of the Information Security any containment measures may be removed. Prior to removing any containment measures the Information Security may perform independent tests to ensure that vulnerabilities have in fact been removed or addressed.

4.8. Follow up Analysis

The follow up analysis is intended to provide a detailed incident report, archive evidence, review the incident handling process, gauge its effectiveness and learn from the experience; in particular:

- a) Collate and secure all documentation and evidence
- b) Produce reports to include
- c) Actual impact assessment
- d) Actions taken
- e) Follow up actions to eliminate or mitigate weaknesses
- f) Identify lessons learned and any changes required to CommunityForce Organizational Policies or procedures

It is the responsibility of the Information Security to ensure that a proper 'follow up analysis' is conducted and that all evidence is securely stored. In most cases it will be necessary to archive all incident reports and original and backup copies of evidence collected. Under exceptional circumstances it may be necessary to destroy some of the material collected and this must be done using secure disposal methods.

5. Publishing:

Policy document MUST be approved and signed off by the VP of Security services before publishing.

6. Training and Awareness:

- a) All training materials MUST be updated to reflect the policy changes.
- b) All CommunityForce personnel MUST be notified of the new policy changes immediately and how it affects their day-to-day tasks.
- c) Brown bag sessions MUST be conducted to solicit information or answer any questions about policy changes.

7. Definitions

There are many definitions associated with 'security incidents' e.g.,

Event: An observable occurrence; an aspect of an investigation that can be verified and analyzed

Incident: An adverse event or series of events that impact the security requirements of an organization

Incident: Any irregular or adverse event that occurs on any part of organizations computing systems and facilities

Incident: The act of violating or threatening to violate an explicit or implied security policy

Evidence: Data on which to base proof or to establish a truth or falsehood

Forensic Analysis: Examination of material e.g., data to determine its features and relationships in an effort to discover evidence that will be admissible in disciplinary or legal proceedings

8. 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.

9. Revision History

Author	Approved by	Revised on	Version	Comments
Muneer Baig	Khaja Syed	01/12/2008	1.0	
Muneer Baig	Khaja Syed	09/11/2009	1.1	
Muneer Baig	Khaja Syed	12/10/2010	1.2	