INCIDENT RESPONSE PROCEDURE - HACKER/CRACKER

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.3.1 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

3. Attempted Probes into XXXXSystems/Network 5

3.1 Identify Problem 5

3.2 Notify Head of IT 5

3.3 Identify Hacker/Cracker 5

3.4 Notify CERT/CSRIT 5

3.5 Follow-up 5

3.6 Follow-Up Analysis 5

4. Active Hacker/ Cracker Activity 7

4.1 Notify Appropriate People 7

4.2 Removal of Hacker/Cracker from the System 7

4.2.1 Snap-shot the System 7

4.2.2 Lock Out the Hacker 7

4.2.3 Restore the System 7

4.2.4 Notify Other Agencies 8

4.2.5 Follow-up 8

5. Procedure Compliance & Enforcement 9

5.1 Compliance Measures 9

5.2 Enforcement 9

6. Glossary / Acronyms 10

6.1 Glossary / Acronyms 10

7. Document Management 11

7.1 Document Revision Log 11

7.2 Document Ownership 11

7.3 Document Coordinator 11

7.4 Document Approvers 11

7.5 Distribution 11

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The objective of this procedure is to list out the steps the XXXX will take to detect, contain, remove and recover from a hacker/cracker attack

## Scope

### Applicability to Employees

XXXX refers to XXXX. as well as its majority-owned subsidiaries and joint ventures (if applicable). This Procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework.*
* *XXXX-PRC-ALL-006 - Incident Response Plan*

# Procedure Statements

Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naive youngsters looking for a thrill. A hacker can also be an insider engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to XXXX network.

Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events which have been discovered after the fact. Of the three, an active hacker/cracker session is the most severe and must be dealt with as soon as possible.

There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to identification and possible criminal conviction.

The method used to handle a cracker/hacker incident will be determined by the level of understanding of the risks involved.

The criticality and sensitivity of the incident is determined in accordance with *XXXX-PRC-ALL-006 - Incident Response Plan and appropriate risk rating will be applied*

# Attempted Probes into XXXX Systems/Network

Incidents of this type would include: repeated login attempts, repeated ftp, telnet or rsh commands, and repeated dial-back attempts.

## Identify Problem

Staff Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such a system logs files, the root history file, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. **Log all actions.**

## Notify Head of IT

Notify the Head of IT within 30 minutes through [helpdesk@XXXX](mailto:helpdesk@zenith-bank.co.uk) or call extension 1234. If the Head of IT cannot be reached, then notify the backup person. The Head of IT or their backup person will be responsible for notifying other levels of management.

## Identify Hacker/Cracker

If the source of the attacks can be identified, then the Head of IT (or a designated person) will contact the system administrator or security analyst for that site and attempt to obtain the identity of the hacker/cracker. If the hacker/cracker can be identified, the information should be provided to the Head of IT, COO and CEO. **Log all actions.**

## Notify CERT/CSRIT

If the source of the attacks can not be identified, then the Head of IT will contact the Internet CERT/CSRIT and CIAC teams and provide them with information concerning the attack.

NOTE - Release of information must be approved by the CEO or a designate. **Log all actions.**

## Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the Head of IT and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.6.

## Follow-Up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). If applicable, a set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the Head of IT and distributed to all appropriate personnel.

# Active Hacker/ Cracker Activity

Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active rlogin or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker/cracker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. This decision must be made by the Head of IT or someone he designates. The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved

## Notify Appropriate People

Notify the Head of IT as soon as possible either through [helpdesk@XXXX](mailto:helpdesk@zenith-bank.co.uk) or call 1234. If unable to reach him/her within 5 minutes, contact the backup person. The Head of IT will then be responsible for notifying other appropriate personnel. The Head of IT, with possible help from third-party vendor, will be responsible for trying to assess what the hacker/cracker is after and the risks involved in letting the hacker/cracker continue his/her activity.

The Head of IT will notify the COO and CEO as soon as possible. If unable to reach them within ten minutes, their backup persons should be contacted. A decision to allow the hacker to continue or to lock him out of the system. Based on the decision, follow the procedures in 4.2.1 or 4.2.2 below.

## Removal of Hacker/Cracker from the System

### Snap-shot the System

Make copies of all audit trail information such as system logs files, event logs, the root history files, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections.

### Lock Out the Hacker

Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. **Log all actions.**

### Restore the System

Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the log book for this incident. **Log all actions.**

### Notify Other Agencies

Report the incident regulatory bodies, law enforcement, Ames CNSRT, the Internet CERT and to CIAC if appropriate.

NOTE- Release of information must be approved by the CEO or someone he designates. **Log all actions**.

### Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the XXXX Head of IT and distributed to the appropriate people. Perform the follow-up analysis as described in section 3.6.

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| FTP | File Transfer Protocol |
| RSH | Remote Shell |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* *IT*