MALWARE Incident Response Procedure

*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. Procedures Steps 5

4. Procedure Compliance & Enforcement 6

4.1 Compliance Measures 6

4.2 Enforcement 6

5. Glossary / Acronyms 7

5.1 Glossary / Acronyms 7

6. Document Management 8

6.1 Document Revision Log 8

6.2 Document Ownership 8

6.3 Document Coordinator 8

6.4 Document Approvers 8

6.5 Distribution 8

# 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 malware 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

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.

Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.

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

# Procedures Steps

| Response Task | Action | Results |
| --- | --- | --- |
| User suspect/discover Malware on System | Send a mail to helpdesk @xxxx.com or call extension 1234 | Request received by IT and the steps below are carried out |
| Scan Endpoint - Malware Found? | After running a scan, determine whether malware was found.  **Yes** or **No** | If **Yes**, the **Remove Malware - Success?** task is executed.  If you select **No**, the flow ends. |
| Remove Malware - Success? | Determine whether the malware was successfully removed.  **Yes** or **No** | If **Yes**, the **Was there a larger breach?** task is executed.  If **No**, the **Wipe & Reimage** task is executed. |
| Wipe & Reimage | If you did not successfully remove the malware found, perform a wipe and reimage on the computers infected with the malware. | After the task is complete, the **Set State to Review** task is executed. |
| Was there a larger breach? | Determine whether the breach caused by the malicious software is larger than first believed.  **Yes** or **No** | If **Yes**, the following tasks are executed in parallel:  Notify ExCo, DPO, Compliance and if required Law Enforcement Agency  If **No**, the flow ends. |
| Notify Legal  Notify HR  Notify Law Enforcement | Notify each of these departments to review the process you followed to eradicate the malicious software. | When the tasks are complete, the **Set State to Review** task is executed. |
| Set State to Review | No action required. | The **State** of the security incident is changed automatically to **Review**, and the flow ends. |
| Prepare an incident report for the security committee |  |  |

# 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

|  |  |
| --- | --- |
| DPO | Data Protection Officer |

# 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*