|  |  |
| --- | --- |
|  | **I-ISMS Revision** 1 |

**NP Factory, Ltd.**

**Plant Floor**

**Industrial Information System Management System**

Guide to Incident Handling

Nathan Pocock

https://our.intranet/path/to/document.docx

|  |  |
| --- | --- |
| **I-ISMS Revision** 1 (6) | **Industrial Information System Management System**  Guide to Incident Handling  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Monitoring**

PRIVATE

|  |  |
| --- | --- |
| 05e - Guide To Incident Handling.Docx  Version: 1 Revision 6  Pages: 1 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\05e - Guide to Incident Handling.docx  Keywords: incident attack, response, handling, hack, crack, malware, virus  Last Saved by Nathan Pocock on 9/16/2016 5:09 PM |
|  | **NP Factory, Ltd.**  [Company Address]  Plant Floor  I-ISMS  704-491-5840  Manager Pocock |

Executive Summary

A general guide on how to respond to cyber-attack incidents

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 16-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 1](#_Toc461809139)

[2 Overview 1](#_Toc461809140)

[3 Considerations 1](#_Toc461809141)

[4 Process 1](#_Toc461809142)

Figures

# 

# Instructions

This page provides quick instructions for using this guide:

1. Read the document for a list of considerations
2. Use this document to build a more strategic and specific response suited to your systems
3. Add the various sections as necessary

Finally, delete this page.

# Overview

The systems put in place exist to detect intrusions, attacks, and anomalies. Sometimes such systems can detect attacks, sometimes they are bypassed by the attacker. Ultimately, personnel must see the alerts generated by the systems or see when anomalies have occurred that the systems have missed.

# Considerations

The following list of considerations are essential:

* Has an attack already occurred? If so, what was it?
* What is being targeted? What is the potential/actual fall-out?
* Do you still have control?
* Do you need to shut everything down? Or shutdown some systems only?
* Who did the attack? Outsiders or personnel?
* Do you need to call-in the experts?

# Process

Here are some very generic steps to respond to an incident:

1. Identify:
   1. Which computer(s)/device(s) have been compromised?
2. Contain
   1. Decide on how to contain, i.e. disconnect the device or disconnect other devices
   2. Seek assistance from IT to investigate how the problem occurred
   3. Consider hiring external security experts
3. Eradicate
   1. If appropriate, use anti-virus to clean any virus/malware
   2. If appropriate, restore a system from backup
   3. If required, reinstall a system back to factory state
4. Prevent
   1. Put controls in place to prevent a recurrence, e.g. further O/S or application hardening
   2. Train employees on what happened, how it was identified, how it was resolved, and how to prevent recurrence