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

**NP Factory, Ltd.**

**Plant Floor**

**Industrial Information Security Management System**

Risk Register

Nathan Pocock

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

|  |  |
| --- | --- |
| **I-ISMS Revision** 1 (7) | **Industrial Information Security Management System**  Risk Register  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Risk management**

INTERNAL

|  |  |
| --- | --- |
| Plan - 06 -- Risk Register.Docx  Version: 1 Revision 7  Pages: 9 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\Plan - 06 -- Risk Register.docx  Keywords: risk  Last Saved by Nathan Pocock on 9/20/2016 10:57 AM |
|  | **NP Factory, Ltd.**  [Company Address]  Plant Floor  I-ISMS  704-491-5840  Manager Pocock |

Executive Summary

<<insert summary here>>

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 8-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 5](#_Toc462132921)

[2 Overview 6](#_Toc462132922)

[3 Top Risks 7](#_Toc462132923)

[4 Risk Register 8](#_Toc462132924)

Figures

Figure 1 Top 5 Risks 7

Figure 2 Risk Register 8

# 

# Instructions

This document is a register of all known risks that currently exist.

You can organize this register any way you like.

Instructions:

1. Open the document properties and change the metadata fields.
2. Modify the Risk Register (on page 8):
   1. Add new risks as they are identified.
   2. Remove risks as they are resolved.
3. Hit CTRL+A and then press F9 to update all page numbers, table of contents, and references etc.

Lastly, delete this page and then save the document.

# Overview

This risk register collates information from various document sources, one per networked equipment. Refer to [05 - Guide to Infosec Vulnerability Analysis.docx](05%20-%20Guide%20to%20Infosec%20Vulnerability%20Analysis.docx) for more information.

This risk register is applicable during the year 2016.

# Top Risks

The following risks are currently considered with the highest level of priority.

Figure 1 Top 5 Risks

| # | Asset | Risk | Impact  (hi, med, lo) | Likelihood (hi, med, lo) | Link | Status – Date/Description |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | All | Users accidentally or maliciously changing PC/PLC settings causing loss of monitoring or control, or unauthorized access to information etc. | High | High |  |  |
| 2 | Machines | Overheating due to over-clocking the engine RPM by exploiting a vulnerability in the ladder logic program which does not validate input parameters. | High | High |  |  |
| 3 | Workstations | Virus/malware infection enabling back-doors, unauthorized access to data/settings, loss of control, etc. | High | High |  |  |
| 4 | All | Denial of Service causing loss of monitoring and control | High | Med |  |  |
| 5 | All PLCs/controllers | Vulnerability exploitation of device enabling parameter-value injection directly affecting safety and/or production | High | Med |  |  |

# Risk Register

The following risks are known to exist and have been officially identified.

Figure Risk Register

| ID# | Asset | Risk | Impact  (hi, med, lo) | Likelihood (hi, med, lo) | Link | Status – Date/Description |
| --- | --- | --- | --- | --- | --- | --- |
| Computer Systems | | | | | | |
|  | All | Users accidentally or maliciously changing PC/PLC settings causing loss of monitoring or control, or unauthorized access to information etc. | High | High |  |  |
|  | All | Virus/malware infection enabling back-doors, unauthorized access to data/settings, loss of control, etc. | High | High |  |  |
|  | All | Denial of Service causing loss of monitoring and control | High | Med |  |  |
|  | All | Hardware failure causing complete loss of access to PC | High | High |  |  |
|  | PC #1 | Hardware failure due to exposure from dust from close proximity to industrial hardware | High | High |  |  |
|  | PC #1 | Uncontrolled computer reboots due to ESD from nearby radio equipment | High | High |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Network Infrastructure | | | | | | |
|  | Router/Firewall | Denial of Service causing loss of monitoring and control | High | Med |  |  |
|  | Switch | Unauthorized alteration of configuration settings | High | Low |  |  |
|  | Switch | Unauthorized disclosure of network traffic to/from all ports to/from all ports (MAC/cache overflow) | High | Low |  |  |
|  | Switch | Unauthorized access to the network from unknown devices | High | High |  |  |
|  | Firewall | Allowing unauthorized applications/traffic to traverse firewall | High | High |  |  |
|  | WIFI | Unauthorized access to the network from unauthorized devices | High | High |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Networked Industrial Machinery / Devices | | | | | | |
|  | All | Denial of Service causing loss of monitoring and control | High | Low |  |  |
|  | All | Vulnerability exploitation of device enabling parameter-value injection directly affecting safety and/or production | High | Med |  |  |
|  | All | Unauthorized modification of settings impacting safety, efficiency, and/or production | High | High |  |  |
|  | All | Hardware failure preventing production | High | High |  |  |
|  | Machine #1 | Unable to manufacture if dependent system (in-feed) of asset #???? Is unresponsive | High | Med |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Applications / Ladder Logic | | | | | | |
|  | All | Impact on production, safety, or efficiency due to improper input parameter validation inherently allowing unsafe values being used | High | High |  |  |
|  | Machine #A | Overheating due to over-clocking the engine RPM by exploiting a vulnerability in the ladder logic program which does not validate input parameters. | High | High |  |  |
|  | Ladder Logic | Unauthorized modification of ladder logic being applied to a device thereby impacting production, safety, and/or efficiency | High | Low |  |  |
|  | SCADA | Unauthorized user access leading allowing for information access, settings/configuration control, and process control. | High | Med |  |  |
|  | SCADA | Vulnerabilities in the SCADA itself enabling a remote attacker to bypass all security and gain complete access/control over the the system and process. | High | Low |  |  |
|  | Custom apps | Vulnerabilities in input parameter checking of user-input and file-input enabling buffer-overflow allowing an attacker to execute arbitrary code | High | Low |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |