|  |  |
| --- | --- |
|  | **Project Name (custom) Revision** 1 |

**NP Factory Ltd.**

**Factory floor**

**Industrial Information Security Management System**

Risk Management Plan

Nathan Pocock

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

|  |  |
| --- | --- |
| **Project Name (custom) Revision** 1 (25) | **Industrial Information Security Management System**  Risk Management Plan  Editor: *Editor Name (custom)*  Authors: *Nathan Pocock* |

**Risk Management**

INTERNAL

|  |  |
| --- | --- |
| 03 - Risk Management Plan.Docx  Version: 1 Revision 25  Pages: 8 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\03 - Risk Management Plan.docx  Keywords: iisms, risk, mitigate, accept, avoid, transfer, register  Last Saved by Nathan Pocock on 9/8/2016 9:00 PM |
|  | **NP Factory Ltd.**  [Company Address]  Factory floor  Project Name (custom)  704-491-5840  Manager Pocock |

Executive Summary

The general rules and processes for the discovery, assessment, response, and overall management of risk; specific to industrial automation equipment and cyber-security.

Revision History

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

Contents

[1 Instructions 5](#_Toc461132023)

[2 Risk management overview 6](#_Toc461132024)

[3 Top three risks 6](#_Toc461132025)

[4 Risk management approach 6](#_Toc461132026)

[1.1 Risk identification 7](#_Toc461132027)

[1.2 Risk analysis (qualification and prioritization) 7](#_Toc461132028)

[1.3 Risk response planning 8](#_Toc461132029)

[1.4 Risk mitigation and avoidance 8](#_Toc461132030)

[1.5 Risk monitoring, controlling, and reporting 8](#_Toc461132031)

[5 Tools and Practices 8](#_Toc461132032)

Figures

Figure 1 Risk Rating based on Impact and Probability 7

# 

# Instructions

1. Open the document properties and set all variables as appropriate
2. Carefully read this risk management plan and modify the contents where applicable
3. Delete this page
4. Save the document

# 

# Risk management overview

In accordance with NP Factory Ltd. [I-ISMS policy](Plan%20-%2001%20--%20IISMS-CompanyPolicy.docx), risks to production floor industrial automation equipment and infrastructure must be managed to reduce or eliminate the potential for downtime, safety hazard, or unauthorized access to systems, information, or data.

This document describes the methodologies that will be used to exercise risk management of industrial infrastructure from a cyber-security standpoint.

# Top three risks

The top 3 risks that have the highest probability and impact for this project are:

* Exposure of systems and applications
* Decreased level of safety for personnel
* Negative impact on production

# Risk management approach

A risk management team will be responsible for the methodical assessment for the identification, categorization, prioritization, and response to risks. Risks that are identified with the potential to impact production or safety will require the assistance of those responsible for those areas.

Risks are recorded in the [Risk Register](04%20-%20Risk%20Register.docx).

Risks that have a high impact and high probability will be assigned a higher priority, assigned to a manager/engineer, and scheduled accordingly.

The risk management team will monitor the status of risks and ensure work is being done to handle appropriately.

Upon completion of a risk response, the process will be documented and reviewed and a decision will be made to determine if and where improvements can be made.

## Risk identification

The identification of risks for production processes, machinery, controllers, network/communications infrastructure, computers, and software systems etc. will utilize the following resources in a closed-door meeting:

* Those responsible for the factory/business process
* Those responsible for the industrial equipment, infrastructure, computers, or software
* Skilled personnel with expert-level knowledge
* Project managers

The risks will be determined by reviewing the [Asset register](02%20-%20Asset%20Register.docx) and identifying risk based on criteria such as:

* Is Ethernet, serial, USB, or wireless communications possible?
* Is data sent and/or received?
* Is configuration information stored?
* Is sensitive information such as recipes etc. available?
* Is re-programming and/or re-configuring possible?
* Is an upstream and/or downstream device connected?

## Risk analysis (qualification and prioritization)

Each risk that is identified will be analyzed to determine:

* **Impact** *High*: significant impact safety, costs, efficiency, or privacy  
  *Med*: some potential impact on costs or efficiency  
  *Low*: very little impact on costs or efficiency
* **Likelihood** *High*: 70% or greater probability of occurrence  
  *Med*: 30-70% probability of occurrence  
  *Low*: 0-30% probability of occurrence

An overall risk rating and prioritization will be based on the cross-section of both variables:

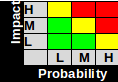


Figure Risk Rating based on Impact and Probability

Risks in the red or yellow zones require risk mitigation and contingency planning.

## Risk response planning

Risks identified in the red or yellow areas will receive a higher level of priority and focus, and will receive one of the following risk responses, in accordance with the [I-ISMS company policy](01%20-%20IISMS-CompanyPolicy.docx) (section Risk Management):

* **Avoid**: prevent the risk from occurring
* **Mitigate**: reduce the impact of the risk if it occurs
* **Accept**: do nothing about the risk
* **Transfer**: select an external/third-party to assume responsibility of the risk (insurance, outsource, etc.)

Risks that can be avoided or mitigated in-house may require additional time and resources to assure success, such as the need to do prototyping and testing in advance.

## Risk mitigation and avoidance

Risks in this category:

* must exist in the risk register
* must have one or more mitigation plans defined with each being rated as a solution and prioritized in preference order, and each documented and documented in the risk register with a reference to the document filename and path
* must be prioritized for more rapid response
* Require monitoring to assure completion within scope, time, and budget

## Risk monitoring, controlling, and reporting

Each high priority risk must be tracked by the risk management group, who must maintain focus on the risk to avoid lack of implementation or implementation failure; to track costs and further assure no further risks emerge.

# Tools and Practices

The risk register will be utilized for documenting risks and will be utilized during risk management meetings.