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

**NP Factory, Ltd.**

**Plant Floor**

**Industrial Information System Management System**

Security Controls Identification and Implementation

Nathan Pocock

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

|  |  |
| --- | --- |
| **I-ISMS Revision** 1 (25) | **Industrial Information System Management System**  Security Controls Identification and Implementation  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Security**

PRIVATE

|  |  |
| --- | --- |
| Do - 2.2 -- Security Controls Identification And Implementation.Docx  Version: 1 Revision 25  Pages: 9 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\Do - 2.2 -- Security Controls Identification and Implementation.docx  Keywords: security controls  Last Saved by Nathan Pocock on 9/18/2016 7:22 PM |
|  | **NP Factory, Ltd.**  [Company Address]  Plant Floor  I-ISMS  704-491-5840  Manager Pocock |

Executive Summary

A framework for storing information about the various security controls that exist within the facility for providing physical and electronic security.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 18-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 5](#_Toc461989853)

[2 Overview 6](#_Toc461989854)

[3 Security controls 6](#_Toc461989855)

[4 Security Controls Matrix 7](#_Toc461989856)

Figures

**No table of figures entries found.**

# 

# Instructions

This page provides quick instructions for using this guide:

1. Read the *Overview* to gain a simple understanding of the need for this document
2. Modify the *Security controls* on page 6
3. Adjust the security columns in the *Security Controls Matrix* on page 7 and then complete the table.
4. Add, edit, and remove table entries and categories as necessary.

Finally, delete this page.

# Overview

There are many ways to protect both physical and electronic assets. This document contains a list of security controls in use by NP Factory, Ltd.

A security control can be something physical, such as a lock/key, or something electronic like a login/password, or key-card etc.

# Security controls

The following security controls shall be utilized:

* Physical:
  + Lock/Key: for doors, windows, cabinets, cages, panels, etc.
* Electronic:
  + Login (username/password) for access to computers, networks, and software
  + Anti-virus protection from malware threats
  + Firewall protection from network-based threats
  + IDS/IPS protection from advanced anomalies
  + File access permissions protection from unauthorized access of file system
  + MAC filtering filtering based on network adapter MAC address
  + IP filtering port and address filtration
* Policy/Rules rules defined in documents

# Security Controls Matrix

| **Layer / Required Control** |  |  | **Control** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **<other 1>** | **<other 2>** | **Lock / key** | **Login / code** | **Anti-virus** | **Firewall** | **IDS/IPS** | **File access** | **Switch / MAC** | **IP Filter** | **Rules / Policy** |
| **PHYSICAL ENVIRONMENT CONTROLS** | | | | | | | | | | | |
| Plant floor access (doors, windows, vents, emergency escape, etc.) |  |  | **X** |  |  |  |  |  |  |  |  |
| Offices within the plant floor |  |  | **X** |  |  |  |  |  |  |  |  |
| Filing, cabinet systems, and desk drawers etc. |  |  | **X** |  |  |  |  |  |  |  |  |
| Storage rooms |  |  | **X** |  |  |  |  |  |  |  |  |
| Computer systems, servers, and networked industrial devices etc. |  |  | **X** |  |  |  |  |  |  |  |  |
| Computer storage racks and/or rooms |  |  | **X** | **X** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **NETWORK LEVEL CONTROLS** | | | | | | | | | | | |
| Network physical access |  |  |  | **X** |  |  |  |  | **X** | **X** | **X** |
| Unauthorized device access detection |  |  |  |  |  |  | **X** |  | **X** |  |  |
| Unauthorized intrusion detection |  |  |  |  |  |  | **X** |  |  |  |  |
| Network segmentation of devices and logical networks |  |  |  |  |  | **X** |  |  | **X** | **X** |  |
| Wireless network (if present) |  |  |  | **X** |  |  |  |  | **X** |  |  |
| Log management |  |  |  | **X** |  |  |  |  |  |  |  |
| Device management |  |  | **X** | **X** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **COMPUTER SYSTEM CONTROLS** | | | | | | | | | | | |
| General usage |  |  |  | **X** | **X** | **X** |  |  |  | **X** | **X** |
| Authorized user access only |  |  |  | **X** |  |  |  |  |  |  |  |
| Detection of unauthorized access |  |  |  |  | **X** | **X** | **X** |  |  |  |  |
| Detection of unauthorized data-changes |  |  |  |  | **X** |  | **X** |  |  |  |  |
| Patch management |  |  |  |  |  |  |  |  |  |  | **X** |
| Application hardening (whitelisting, blacklisting, etc.) |  |  |  |  | **X** | **X** |  |  |  |  | **X** |
| Backup drives, devices, and/or other media |  |  | **X** | **X** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **DEVICE LEVEL CONTROLS** | | | | | | | | | | | |
| Device settings/configuration |  |  | **X** | **X** |  |  |  |  |  |  |  |
| Cabling (power, communications, etc.) |  |  | **X** | **X** |  |  |  |  |  |  |  |
| Protocol / communications filtering / hardening |  |  |  |  |  | **X** | **X** |  |  |  | **X** |
| Cyber-attack detection |  |  |  |  |  | **X** | **X** |  |  |  |  |
| Unauthorized access detection |  |  |  |  |  | **X** | **X** |  | **X** | **X** | **X** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **APPLICATION LAYER CONTROLS** | | | | | | | | | | | |
| SCADA systems |  |  |  | **X** |  |  |  |  |  |  | **X** |
| Other process control based applications |  |  |  | **X** |  |  |  |  |  |  | **X** |
| Unauthorized access to file system |  |  |  |  |  |  | **X** | **X** |  |  |  |
| Unauthorized access to/from the network and/or internet |  |  |  | **X** |  | **X** | **X** |  |  |  |  |
| Other applications… |  |  |  | **X** |  | **X** | **X** | **X** |  |  |  |
| Backup (settings, configuration, data, etc.) |  |  |  | **X** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |