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

**NP Factory, Ltd.**

**Factory floor**

**Industrial Information Security Management System**

Internal Audit Checklist

Nathan Pocock

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

|  |  |
| --- | --- |
| **I-ISMS Implementation Revision** 1 (1) | **Industrial Information Security Management System**  Internal Audit Checklist  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Continuous Improvement**

PRIVATE

|  |  |
| --- | --- |
| Document1  Version: 1 Revision 1  Pages: 2 | Path: Document1  Keywords: iisms, risk, applicability, policy  Last Saved by on 1/1/1601 12:00 AM |
|  | **NP Factory, Ltd.**  [Company Address]  Factory floor  I-ISMS Implementation  704-491-5840  Manager Pocock |

Executive Summary

A checklist for conducting an internal audit to determine compliance with the I-ISMS policy

Revision History

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

Contents

[1 Instructions 2](#_Toc461799018)

[2 Statement of Applicability 2](#_Toc461799019)

Figures

Figure 1 Table of Statement of Applicability 2

# 

# Instructions

The statement of applicability is a mapping between the security policies defined in the [01 - IISMS-CompanyPolicy.docx](01%20-%20IISMS-CompanyPolicy.docx) and how they have been executed to comply with the requirements. This version of SoA is simplified by reducing any need to map with regulations or other standards.

Complete this document by doing the following:

1. Review the table defined in *Statement of Applicability* below.
2. Complete all actions marked as TODO or PARTIAL.
3. Add, edit, or remove rows/sections as necessary.
4. Press CTRL+A and then hit F9 to update the document references and page numbering.

Lastly, delete this page and then save the document.

# Scope

This internal audit applies to the following:

* Physical environment
* Computer systems
* Network infrastructure
* Industrial machinery and devices connected to the network
* Personnel

# Audit Checklist

Please update the table below as you make progress through the implementation.

Figure Internal Audit Checklist

| IISMS Ref | Check | Frequency | Priority | Status | Findings / Notes | Date | Sign-off |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **I-ISMS: Policy** | | | | | | | |
| 1.1 | I-ISMS Policy is in a finalized state and in an accessible location for all employees | Annual | Low |  |  |  |  |
| 1.1 | I-ISMS Policy review is complete and approved by management | Annual | High |  |  |  |  |
| 1.6 | I-ISMS Policy reviewed by factory-floor management and subject-matter experts | 6-month | Med |  |  |  |  |
| 1.6 | I-ISMS Policy reviewed by IT for alignment with overall company objectives | Annual | Med |  |  |  |  |
| 1.6 | I-ISMS Policy audit of factory-floor compliance setup and enforceable | 6-month | High |  |  |  |  |
| 1.6 | Review document security to assure only authorized personnel can modify or delete | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **I-ISMS: RESPONSIBILITIES** | | | | | | | |
| 2 | Principal engineer recognized, documented, and identified in necessary documents, e.g. BCP | Annual | High |  |  |  |  |
| 2 | I-ISMS team(s) created and documented, e.g. BCP. | Annual | High |  |  |  |  |
| 2 | Review process for reporting cyber-security issues/weaknesses; verify is known by employees | Annual | High |  |  |  |  |
| 2 | Review process for visitor/contractor training process for reporting cyber-security issues/weaknesses | Annual | High |  |  |  |  |
| 2 | Review document security to assure authorized modification only | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **I-ISMS: RISK MANAGEMENT** | | | | | | | |
| 3 | Review risk management process for compliance with I-ISMS policy; review meetings and notes | Annual | High |  |  |  |  |
| 3 | Review risk management decision-making process for compliance with company policy | Annual | High |  |  |  |  |
| 3 | Review contingency plans for accuracy and efficiency | Annual | High |  |  |  |  |
| 3 | Review documentation security to assure authorized access and modification only | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **I-ISMS: AWARENESS CAMPAIGN** | | | | | | | |
| 4 | Review awareness campaign to verify employees are being trained on new-hire and transfers etc. | Annual | Med |  |  |  |  |
| 4 | Review training materials for accuracy | Annual | Med |  |  |  |  |
| 4 | Review employee records to verify awareness training is logged | Annual | Low |  |  |  |  |
| 4 | Discuss awareness campaign with employees to determine level of awareness & knowledge | Annual | Med |  |  |  |  |
| 4 | Review awareness improvement process | 2-years | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **BUSINESS CONTINUITY PLAN / DISASTER RECOVERY PLAN** | | | | | | | |
| 5 | Review the BCP/DRP for accuracy and efficiency | Annual | High |  |  |  |  |
| 5 | Verify the documentation is in an accessible location for all employees | 6-months | Med |  |  |  |  |
| 5 | Verify document security to assure authorized access and modification only | Annual | Med |  |  |  |  |
| 5 | Review the process for improving the BCP/DRP | Annual | Med |  |  |  |  |
| 5 | Verify team awareness of the BCP/DRP | Annual | Med |  |  |  |  |
| 5 | Review the schedule for simulation disasters and recovery process | 2-years | Med |  |  |  |  |
| 5 | Verify the employee lists and all other contacts documented are correct | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **ASSET MANAGEMENT** | | | | | | | |
| 6 | Review the asset register exists and is accurate | Annual | High |  |  |  |  |
| 6 | Verify each computer system and networked industrial device is cataloged in the asset register | Annual | High |  |  |  |  |
| 6 | Review the documents are secure for authorized review and modifications only | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **PHYSICAL SECURITY** | | | | | | | |
| 7 | Verify the factory floor perimeter is physically secured to prevent unauthorized entry (doors, windows) | Annual | High |  |  |  |  |
| 7 | Verify all factory-floor office spaces are physically secured to prevent unauthorized entry | Annual | High |  |  |  |  |
| 7 | Verify all lockable cabinets, cages, drawers, panels, and boxes etc. are all locked | Annual | High |  |  |  |  |
| 7 | Review the anchoring of all equipment and computing equipment | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **CLEAN DESK POLICY** | | | | | | | |
| 7 | Verify the clean-desk policy is being observed by all employees in all work-spaces | Annual | High |  |  |  |  |
| 7 | Verify no sensitive information is left in the open | Annual | High |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **COMPUTER USAGE, HARDENING, AND MONITORING** | | | | | | | |
| 10 | Verify employees have been trained on computer-usage policy | Annual | Low |  |  |  |  |
| 10 | Verify all computer systems have been hardened following the hardening guide and documented | Annual | High |  |  |  |  |
| 10 | Verify all industrial networked devices have been suitably hardened and documented | Annual | High |  |  |  |  |
| 11 | Verify the password policy is implemented on all computer systems and industrial equipment (where possible) | Annual | High |  |  |  |  |
| 12 | Review the backup processes are documented and accurate | Annual | High |  |  |  |  |
| 12 | Verify all computer systems and networked industrial devices have been backed-up during a known good-state | Annual | High |  |  |  |  |
| 12 | Verify all computer systems are regularly backed-up, automatically | Annual | High |  |  |  |  |
| 12 | Verify only authorized personnel can access and/or modify the backup settings | Annual | High |  |  |  |  |
| 13 | Verify the anti-virus/anti-malware policy is enforced on all computer systems | 6-months | High |  |  |  |  |
| 13 | Verify only authorized users can modify the anti-virus behavior / settings | Annual | High |  |  |  |  |
| 13 | Verify each protected computer system is reporting its logs to a central server/point | Annual | High |  |  |  |  |
| 14 | Verify each computer system requires user logon | Annual | High |  |  |  |  |
| 14.1 | Verify which users have physical access to restricted areas, locations | Annual | High |  |  |  |  |
| 14.1 | Verify the user access permissions of each user to verify “least privilege” level only | 6-months | High |  |  |  |  |
| 14.2 | Review the procedures for registering new users into the system(s) | Annual | Med |  |  |  |  |
| 14.3 | Review the procedures for removing employees from the system(s) | Annual | Med |  |  |  |  |
| 14.4 | Review the procedures for allowing contractors into the facility and working on equipment | Annual | High |  |  |  |  |
| 14.4 | Interview employees to determine awareness for working with contractors | Annual | Med |  |  |  |  |
| 14.5 | Verify internet access is restricted to authorized computer systems only | Annual | High |  |  |  |  |
| 14.5 | Verify internet access is removed from unauthorized computer systems | Annual | High |  |  |  |  |
| 14.5 | Verify industrial equipment is not permitted to access the internet, or be contacted from the internet | Annual | High |  |  |  |  |
| 14.5 | Verify only approved software is used with the internet (email, browser, etc.) | Annual | High |  |  |  |  |
| 15.1 | Verify all computer systems are physically secured to prevent theft/movement | Annual | Med |  |  |  |  |
| 15.2 | Verify all power supplies for all equipment is protected from unauthorized access and/or removal | Annual | Low |  |  |  |  |
| 15.2 | Verify all important power supplies are documented in the asset-register | Annual | Low |  |  |  |  |
| 15.3 | Verify the network infrastructure devices are locked down for authorized administrators only | Annual | High |  |  |  |  |
| 15.3 | Verify all network cabling is adequately shielded from accidental damage | Annual | Low |  |  |  |  |
| 15.3 | Verify only approved devices and computer systems are attached to the network | Annual | High |  |  |  |  |
| 15.3 | Verify network access is restricted to Ethernet only and approved WIFI only. | 6-months | High |  |  |  |  |
| 15.3 | Verify network logs of firewall, router, switch, computer systems, and industrial devices are being monitored | 6-months | High |  |  |  |  |
| 15.4 | Review the computer system document exists for all computer systems and is up to date | Annual | High |  |  |  |  |
| 15.4 | Review the networked industrial equipment settings are documented and up to date | Annual | High |  |  |  |  |
| 15.5 | Review the system documentation for production line processes etc. for accuracy | Annual | Med |  |  |  |  |
| 15.5 | Verify the system documentation is accessible and/or modifiable to authorized personnel only | Annual | Med |  |  |  |  |
| 15.5 | Review the user-access documentation to verify changes and justifications are logged | Annual | Med |  |  |  |  |
| 15.5 | Review the documentation of system processes and relationships for accuracy | 6-months | High |  |  |  |  |
| 15.5 | Review the documentation versioning system is in tracking document versions | Annual | Med |  |  |  |  |
| 15.5 | Verify the document tracking is restricted to authorized personnel only | Annual | Med |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **CONFIGURATION MANAGEMENT** | | | | | | | |
| 16 | Verify the change management review board behavior of regular meetings and activities | Annual | High |  |  |  |  |
| 16 | Review the documentation of working group minutes and decisions | Annual | Med |  |  |  |  |
| 16 | Verify the procedures for review, i.e. proposal, review, (reject, improve), accept, finalize | Annual | Low |  |  |  |  |
| 16 | Verify all changes are approved and that approval is in writing | Annual | Low |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **MONITORING AND CONTINUOUS IMPROVEMENTS** | | | | | | | |
| 17 | Interview all team members and employees to gauge awareness of continuous improvement program | Annual | Low |  |  |  |  |
| 17 | Review all policies and BCP/DRP | Annual | High |  |  |  |  |
| 17 | Review the schedule of meeting, monitoring, auditing, and testing activities | 3-months | High |  |  |  |  |
| 17 | Verify daily reviews of all computer system and networked industrial device logs is occurring | 1-month | High |  |  |  |  |
| 17 | Verify systems are frequently scanned for vulnerabilities (OpenVAS) | 6-months | High |  |  |  |  |
| 17 | Review summary reports are being created and being reviewed | Annual | High |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **SECURITY BREACH AND INCIDENT HANDLING** | | | | | | | |
| 18 | Review the incident detection and escalation procedures for accuracy | Annual | High |  |  |  |  |
| 18 | Interview employees to determine level of awareness of incident reporting and escalation | Annual | High |  |  |  |  |
| 18 | Review any reported incidents to verify the actions taken and the documentation generated | Annual | High |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |