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

**NP Factory, Ltd.**

**Factory floor**

**Industrial Information Security Management System**

Statement of Applicability

Nathan Pocock

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

|  |  |
| --- | --- |
| **I-ISMS Implementation Revision** 1 (50) | **Industrial Information Security Management System**  Statement of Applicability  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Correlation of Policy to Deliverables and Completed Tasks**

PRIVATE

|  |  |
| --- | --- |
| 09 - Statement Of Applicability.Docx  Version: 1 Revision 50  Pages: 12 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\09 - Statement of Applicability.docx  Keywords: iisms, risk, applicability, policy  Last Saved by Nathan Pocock on 9/16/2016 2:16 PM |
|  | **NP Factory, Ltd.**  [Company Address]  Factory floor  I-ISMS Implementation  704-491-5840  Manager Pocock |

Executive Summary

A table of company security policies and how they map to the implementation / deliverables.

Revision History

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

Contents

[1 Instructions 5](#_Toc461799018)

[2 Statement of Applicability 6](#_Toc461799019)

Figures

Figure 1 Table of Statement of Applicability 6

# 

# Instructions

The statement of applicability is a mapping between the security policies defined in the [IISMS Company Policy](Plan%20-%2001%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* on page 6.
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.

# Statement of Applicability [[1]](#endnote-1)

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

Figure 1 Table of Statement of Applicability

| IISMS Ref | Section Title | Progress | Evidence | Responsibility | Recommendations/Actions | Document Name/Location |
| --- | --- | --- | --- | --- | --- | --- |
| **SECURITY POLICY** | | | | | | |
| 1.1 | Need for a security policy | Done | IISMS Policy | Nathan Pocock | No action. | [IISMS Policy](Plan%20-%2001%20--%20IISMS-CompanyPolicy.docx) |
| 1.6 | Review and audit | Done | IISMS Policy | Nathan Pocock | No action. | [IISMS Policy](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\Plan%20-%2001%20--%20IISMS-CompanyPolicy.docx) |
|  |  |  |  |  |  |  |
| **RISK MANAGEMENT** | | | | | | |
| 2 | Management commitment to information security of production | TODO |  | Nathan Pocock | Management to write official memo and post to company bulletin-board and/or send company-wide email. |  |
| 2 | Allocation of resources | Done | The business continuity plan has the teams defined | Nathan Pocock | Project leader to collate a team and then update the BCP/DRP. | [08 - Business Continuity Plan.docx](08%20-%20Business%20Continuity%20Plan.docx) |
| 2 | Contact with external third-parties to notify of new infosec policies | TODO |  | Nathan Pocock | Notify each 3rd party in writing that a new infosec policy is in place and we expect their cooperation. |  |
| 2 | Addressing infosec concerns with 3rd parties | TODO |  | Nathan Pocock | Arrange meeting to discuss and define solutions. |  |
| 2 | Risk management plan | Partial |  | Nathan Pocock | Template provides significant starting-point and requires completion. | [03 - Risk Management Plan.docx](03%20-%20Risk%20Management%20Plan.docx) |
| 2 | Risk register | Partial |  | Nathan Pocock | Template provides significant starting-point and requires completion. | [04 - Risk Register.docx](04%20-%20Risk%20Register.docx) |
|  |  |  |  |  |  |  |
| **AWARENESS AND TRAINING** | | | | | | |
| 4 | Training requirements are communicated with HR on new-hires | TODO |  | Nathan Pocock | Formally notify HR with the new training requirements so they may be added to the training packet. |  |
| 4 | Factory floor procedures are documented | TODO |  | Nathan Pocock | Create procedures to describe the processes that each worker does with a particular machine, or for a process. |  |
| 4 | Awareness and training program established and training materials created | TODO |  | Nathan Pocock | Create awareness training material, e.g. DOCX files and provide to HR. |  |
| 4 | Review and approval of initial training resources | TODO |  | Nathan Pocock | Include how to identify cyber-attacks such as social engineering, malicious sites/attachments, and behaviors like denial-of-service, etc. |  |
| 10 | Employees are trained on the correct usage and protection of their computers/machines | TODO |  | Nathan Pocock | Prepare simple one-sided documents that summarize do’s/don’ts. |  |
|  |  |  |  |  |  |  |
| **BUSINESS CONTINUITY** | | | | | | |
| 5 | Business continuity / disaster recovery plans created | Partial | BCP template exists and providing a significant starting-point | Nathan Pocock | Complete the BCP/DRP to be specific to the process/production line. | [08 - Business Continuity Plan.docx](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\08%20-%20Business%20Continuity%20Plan.docx) |
| 5 | BCP/DRP reviewed and approved | TODO |  | Nathan Pocock | Provide the finished document(s) to management and applicable team(s) for formal review and analysis. |  |
|  |  |  |  |  |  |  |
| **ASSET MANAGEMENT** | | | | | | |
| 6 | Identify all applicable assets for cyber-security hardening / monitoring | TODO |  |  | Conduct an analysis of all machines and computers and log them | [08 - Business Continuity Plan.docx](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\08%20-%20Business%20Continuity%20Plan.docx) |
| 6 | Equipment and Software Registers | Done | The business continuity plan contains the hardware and software registers of importance | Nathan Pocock | See appendices 1.22 and 1.23. | [08 - Business Continuity Plan.docx](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\08%20-%20Business%20Continuity%20Plan.docx) |
| 6 | Classification and prioritization of assets | Done | The registers contain this information | Nathan Pocock | See appendices 1.22 and 1.23. | [08 - Business Continuity Plan.docx](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\08%20-%20Business%20Continuity%20Plan.docx) |
|  |  |  |  |  |  |  |
| **PHYSICAL SECURITY** | | | | | | |
| 7 | Production floor access doors/windows, etc. must be lockable to allow being locked at all times | TODO |  | Nathan Pocock | Implement card-swipe or heavy duty key/lock. |  |
| 7 | Office spaces have lockable doors, filing, and storage systems. | TODO |  | Nathan Pocock |  |  |
| 7 | Equipment is anchored to prevent theft or movement | TODO |  | Nathan Pocock | Use chains with padlocks, or purpose-built anchors. |  |
| 7 | Equipment obstructions in place to prevent unauthorized access | TODO |  | Nathan Pocock | Place equipment behind bars, cabinets, plexiglass, panels, cages, or doors, etc. |  |
| 8 | Clean desk policy enforced | Done | Stated in the IISMS | Nathan Pocock |  | [IISMS Policy](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\Plan%20-%2001%20--%20IISMS-CompanyPolicy.docx) |
| 9 | Visitors log in place | TODO |  | Nathan Pocock | Force visitors to report at reception |  |
|  |  |  |  |  |  |  |
| **INFORMATION SECURITY** | | | | | | |
| 10 | All computer systems are cataloged in a register | TODO |  | Nathan Pocock | Complete appendix 1.22 in the BCP/DRP. |  |
| 10 | All computer systems are protected from unauthorized physical and remote access | TODO |  | Nathan Pocock |  |  |
| 10 | All computers are hardened by removing unnecessary software | TODO |  | Nathan Pocock |  |  |
| 10 | All computers are hardened with a firewall | TODO |  | Nathan Pocock |  |  |
| 10 | All computers are hardened by following a Windows hardening guide | TODO |  | Nathan Pocock |  |  |
| 11 | All computers enforced the password policy | TODO |  | Nathan Pocock |  |  |
| 12 | All computers have documented configuration settings | Partial | A template exists with place-holders for recording relevant information | Nathan Pocock | Use the [07 - Computer Change History.dotx](07%20-%20Computer%20Change%20History.dotx) template to build documentation for each computer. |  |
| 12 | All computers have a backup of a known-good-state stored in a remote location (away from PC) | TODO |  | Nathan Pocock | Use the [05c - Guide to Windows Hardening.docx](05c%20-%20Guide%20to%20Windows%20Hardening.docx) guide for backup configuration instructions |  |
| 12 | All computers are configured for frequent automatic system backups | TODO |  | Nathan Pocock |  |  |
| 12 | All computers a vulnerability scanned and documented in the risk register | TODO |  | Nathan Pocock |  |  |
| 13 | All computers hardened with anti-virus / endpoint-security | TODO |  | Nathan Pocock |  |  |
| 13 | All computers hardened to eliminate users from deactivating security controls | TODO |  | Nathan Pocock | Follow the [05c - Guide to Windows Hardening.docx](05c%20-%20Guide%20to%20Windows%20Hardening.docx) guide |  |
| **PERSONNEL** | | | | | | |
| 14 | All personnel have their own unique login | TODO |  | Nathan Pocock | Follow the [05c - Guide to Windows Hardening.docx](05c%20-%20Guide%20to%20Windows%20Hardening.docx) guide |  |
| 14 | Process exists for verifiably adding, modifying, and removing user access | TODO |  | Nathan Pocock | Ensure the procedures are in place for responding to user privilege requests by contacting applicable managers and persons responsible. |  |
| 14 | Assure HR notifies Factory floor when an employee leaves, is fired, or starts, etc. | TODO |  | Nathan Pocock | Notify HR of the new policy and store the email/memo as part of this SoA. |  |
| 14.4 | Visitors and contractors are restricted in their capabilities and know to abide by cyber-security policies. | TODO |  | Nathan Pocock | Create simple single-sided document(s) that quickly describe company policies along with what they can/can’t do without seeking approval etc. |  |
| 14.5 | Internet access is eliminated from the plant-floor network, but allowed in plant-floor offices on designated computers only | TODO |  | Nathan Pocock | Seek assistance from IT on how to segment the network to permit internet from some resources only. |  |
| **EQUIPMENT SECURITY** | | | | | | |
| 15 | Only authorized personnel have physical access to each system | TODO |  | Nathan Pocock | Each device will need to be hardened to assure only authorized personnel have access.  Follow the [05c - Guide to Windows Hardening.docx](05c%20-%20Guide%20to%20Windows%20Hardening.docx) guide |  |
| 15.1 | All computer systems are physically secured in lockable office spaces and/or cable-tied to a secure surface | TODO |  | Nathan Pocock |  |  |
| 15.2 | All power supplies for all electrical equipment is secured to prevent disconnection and accidental shock | TODO |  | Nathan Pocock |  |  |
| 15.2 | All power cables are securely fastened to prevent accidental removal or shock | TODO |  | Nathan Pocock |  |  |
| 15.3 | Network infrastructure equipment is physically accessible to authorized personnel only | TODO |  | Nathan Pocock |  |  |
| 15.3 | Network infrastructure equipment administration is accessible to authorized personnel only | TODO |  | Nathan Pocock |  |  |
| 15.3 | Network cabling is physically secured and fastened to prevent accidental damage or disconnection | TODO |  | Nathan Pocock |  |  |
| 15.3 | Network access (logon to the network) is restricted to authorized personnel only | TODO |  | Nathan Pocock |  |  |
| 15.3 | Network protocol are restricted to authorized protocols only. | TODO |  | Nathan Pocock | Seek assistance from IT to help.  Follow the [05b - Guide to Windows Firewall Hardening.docx](05b%20-%20Guide%20to%20Windows%20Firewall%20Hardening.docx) to restrict computer capabilities. |  |
| 15.3 | External network connections are restricted to authorized personnel only | TODO |  | Nathan Pocock | Seek assistance from IT to help. |  |
| 15.3 | All networked devices are configured to log activities | TODO |  | Nathan Pocock |  |  |
| 15.4 | Network infrastructure device settings are documented and saved offline | TODO |  | Nathan Pocock |  |  |
| 15.4 | Networked machinery and industrial equipment is secured from unauthorized access or control | TODO |  | Nathan Pocock |  |  |
| 15.4 | Networked machinery and industrial equipment settings are documented and saved offline | TODO |  | Nathan Pocock |  |  |
| 15.4 | Device configuration settings are reviewed, approved, and backed-up offline | TODO |  | Nathan Pocock |  |  |
| 15.5 | All computer systems’ settings are documented, reviewed, and approved. | Partial | Existing template provides a significant starting-point for building required documentation | Nathan Pocock |  |  |
| 15.5 | Change management system (location) is structured to accommodate versioning control | TODO |  | Nathan Pocock | Consider a file/folder system where all master documents are one folder, and each past version of a document goes in a “./<doc name>/<filename ver>” format, e.g. “./risk register/risk register 1.1.docx” etc. |  |
| 15.5 | Factory processes and the equipment needed by those processes are documented | TODO |  | Nathan Pocock |  |  |
| 15.5 | Integration and relationship of components, systems, and devices, as they make-up the overall process, are documented. | TODO |  | Nathan Pocock | Consider the relationship between a SCADA and database, OPC Servers, PLCs, GUI, hard disk, event log, and custom applications, etc. |  |
|  |  |  |  |  |  |  |
| **OPERATIONS MANAGEMENT** | | | | | | |
| 16 | Form a change review board | TODO |  | Nathan Pocock |  |  |
| 16 | Change management defined | Done | Defined in I-ISMS policy section 17. | Nathan Pocock | Allocate a shared resource on the network that can store all change controls | [01 - IISMS-CompanyPolicy.docx](01%20-%20IISMS-CompanyPolicy.docx) |
|  |  |  |  |  |  |  |
| **MONITORING AND CONTNUOUS IMPROVEMENT** | | | | | | |
| 17 | Document the procedure for the daily review of logs and monitoring of network systems activities | TODO |  | Nathan Pocock | Develop a single-page document for those responsible, for conducting daily inspections of logs and activities to determine if a breach has occurred |  |
| 17 | Implement system-wide monitoring | TODO |  | Nathan Pocock | Follow the Windows monitoring guide. | [05d - Guide to Windows Monitoring.docx](file:///C:\Users\nathan%20pocock\OneDrive\wgu-capstone\templates\05d%20-%20Guide%20to%20Windows%20Monitoring.docx) |
|  |  |  |  |  |  |  |
| **SECURITY BREACH AND INCIDENT MANAGEMENT** | | | | | | |
| 18 | Train key resources on how to identify a potential security breach from the review of logs and network activities | TODO |  | Nathan Pocock |  |  |
| 18 | Train key individuals on how to escalate a potential breach situation | TODO |  | Nathan Pocock |  |  |
|  |  |  |  |  |  |  |

1. SoA table based on a template provided by Manchester Fire, UK (http://authority.manchesterfire.gov.uk/documents/s50001812/Worksheet%20in%20O.pdf) [↑](#endnote-ref-1)