|  |  |
| --- | --- |
| **NP Factory Ltd.** | INCLUDEPICTURE "C:\\Users\\nathan pocock\\OneDrive\\wgu-capstone\\templates\\CompanyLogo.jpg" \\* MERGEFORMATINET INCLUDEPICTURE "C:\\Users\\nathan pocock\\OneDrive\\wgu-capstone\\templates\\CompanyLogo.jpg" \\* MERGEFORMATINET INCLUDEPICTURE "C:\\Users\\nathan pocock\\OneDrive\\wgu-capstone\\templates\\CompanyLogo.jpg" \\* MERGEFORMATINET |

Policy Industrial Information Security Management System Policy

**Abstract** Company policy for the safety, security, and integrity of factory-floor processes, equipment, and personnel; and assurance of business continuity in the event of security breaches or attacks

**Author** Nathan Pocock

Document version 1 *revision 90*

Filename 1 - IISMS-CompanyPolicy.docx

Last modification 18-Sep-2016 by Nathan Pocock

Contents

[1 Introduction 4](#_Toc461096453)

[1.1 Need for a security policy 4](#_Toc461096454)

[1.2 Legal requirements 4](#_Toc461096455)

[1.3 \*Purpose and scope of the policy 4](#_Toc461096456)

[1.4 Who is affected by the policy 5](#_Toc461096457)

[1.5 Where the policy applies 5](#_Toc461096458)

[1.6 Security policy objectives 5](#_Toc461096459)

[1.7 Review and audit 6](#_Toc461096460)

[2 Responsibilities 6](#_Toc461096461)

[3 Risk Management 7](#_Toc461096462)

[4 Awareness 9](#_Toc461096463)

[5 Business Continuity 9](#_Toc461096464)

[6 Equipment and Software Registers 10](#_Toc461096465)

[7 Physical security 10](#_Toc461096466)

[8 Clean Desk Policy 11](#_Toc461096467)

[9 Security of third party access 11](#_Toc461096468)

[10 Computer Usage 12](#_Toc461096469)

[11 Password Controls 13](#_Toc461096470)

[12 \*Data and Configuration Backup 14](#_Toc461096471)

[13 Virus / Malware 14](#_Toc461096472)

[14 User access control 15](#_Toc461096473)

[14.1 Access to systems 15](#_Toc461096474)

[14.2 Registering users 15](#_Toc461096475)

[14.3 Employees leaving 16](#_Toc461096476)

[14.4 Visitors and contractors 16](#_Toc461096477)

[14.5 The internet 16](#_Toc461096478)

[15 Equipment security 17](#_Toc461096479)

[15.1 Equipment sitting and protection 17](#_Toc461096480)

[15.2 Power supplies 17](#_Toc461096481)

[15.3 Network security 18](#_Toc461096482)

[15.4 Operational security 18](#_Toc461096483)

[15.5 System documentation 19](#_Toc461096484)

[16 Configuration Management 19](#_Toc461096485)

[17 Monitoring and Continuous Improvements 20](#_Toc461096486)

[18 Security Breach & Incident Management 21](#_Toc461096487)

[19 Revision History 21](#_Toc461096488)

# Introduction

**NP Factory Ltd.** must strive for the highest levels of safety and security of all information technology and industrial automation equipment to prevent or minimize the risk of physical harm to personnel, damage to equipment, loss of production, or unauthorized access and/or theft or destruction of company data/information.

## Need for a security policy

This Industrial Information Security Management System (IISMS) policy describes the **NP Factory Ltd.** requirements for maintaining a safe and secure environment.

This IISMS is mandated by Management.

The frequency of cyber-security related attacks on factories is increasing. The implementation of appropriate security controls will help to reduce or eliminate any risks to the safety of employees, of equipment, information/data, and the business itself.

## Legal requirements

**NP Factory Ltd.** is required by law to comply with the following local, Federal, or International laws:

* None

## Who is affected by the policy

All employees, contractors, and visitors are required to abide by this IISMS policy, and all related policies and procedures.

## Where the policy applies

This IISMS policy applies to the factory automation/ production Department where the **NP Factory Ltd.** IT department do not have control.

This policy covers:

* Computer workstations, laptops, servers, and display panels
* Network equipment, switches, routers, firewalls, cabling, and wireless communications
* PLCs and any connected controllers
* Industrial equipment
* Software installed on any computer system

## Security policy objectives

The objectives of this security policy are:

* Assure the physical safety of all personnel, visitors, and contractors
* Maintain confidentiality of information and configuration and prevent information disclosure to unauthorized personnel through deliberate or careless action
* Protect the integrity of information to prevent unauthorized modification or destruction of information or configuration
* Assure availability of information and equipment when needed
* Maintain production quality, quantity, and safety
* Comply with legislative regulations (see Legal requirements on page 4)
* Prepare, maintain, and test business continuity plans
* Provide security training to all employees, contractors, and visitors
* To detect and contain security breaches as soon as possible, are escalated and investigated

## Review and audit

This policy and all related policies and procedures are required to:

* Twice-yearly reviews by the factory floor engineers, led by the principal engineer, to Identify areas of weakness, to determine accuracy, and to make revisions where necessary.
* Annual reviews by IT department cyber-security team to provide sanity checking and recommendations
* Review by management every 2 years.

In addition, the following list outlines audit requirements:

* An audit checklist contains all tests and verifications for factory floor infrastructure
* Twice-yearly audit of activies conducted on the factory floor to assure compliance with all policies
* Audit documentation to describe all findings
* Non-compliances are identified and are escalated for review.

This I-ISMS must be continually improved to increase security coverage, decrease vulnerabilities, and be better prepareed to handle security breaches.

# Responsibilities

The management of NP Factory Ltd. create and review this policy. Management will approve the policy and show public support by officially endorsing the immediate implementation and adioption.

The principal engineer of the industrial automation Department facilitates the implementation in accordance with standard operating procedures, and is the project manager and acting Chief Security Officer.

The principal engineer will form the required teams to facilitate the implementation and ongoing maintenance of this I-ISMS.

All personel, contractors, and visitors are required to report security incidents or to notify of any identified weaknesses.

# Risk Management

Risk management is the process of making decisions that will minimize or eliminate risk to the safety of employees, equipment, or property; to protect the investments made in infrastructure and research and development; and to protect business interests.

A formal process of risk identification, review, and management is required with complete documentation which must include:

* Risk register containing all identified risks (name and description)
* Category of risk (process, mechanical, chemical, information, etc.)
* Likelihood of the risk occurring (high, medium, low)
* Impact analysis (including upstream/downstream impacts)
* Action (mitigate, transfer, avoid, accept)
* Decision justification
* Decision makers (contacts)

The risk management objectives are to:

* Prevent the reduction or elmination of safety for employees, equipment, and processes
* Prevent the exposure of industrial automation resources (infrastructure, controllers, equipment, processes, or information, etc.) to unauthorized personnel as well external actors outside of the factory-floor network (internet, WI-Fi, corporate network, WAN, etc.)
* Prevent unauthorized access/modification/destruction of industrial automation resources equipment, information, or processes
* Determine the most cost-effective response to risk that does not jeopardize safety
* Develop contingency plans
* Prevent financial losses due to production loss, equipment damage, process disruption, or non-compliance to regulations (see *Legal requirements*, on page 4)

The following guidelines apply to the risk management of NP Factory Ltd. and must be documented in a risk management plan:

* Avoidance:
  + Decreased safety of personnel, equipment, or property
  + Exposure of systems, services, configuration, or information to unauthorized persons
  + Vulnerabilities that can be exploited in equipment, controllers, computers, software, or infrastructure, that could be exploited by an attacker to gain unauthorized access, control, or configuration.
* Mitigation:
  + Potential for decreased safety of personnel, equipment, or property
  + Potential exposure of system services or information to unauthorized persons
  + Disruption of production
  + Financial losses or increases to business expenses
* Transference:
  + Where the costs for mitigation are too high, but the costs to transfer to a third party (insurance, contractor, etc.) are justifiable
  + Internal resources are unable to mitigate (e.g. lack of skills, lack of labor, etc.)
* Acceptance:
  + There is no way to mitigate, transfer, or avoid the risk, and the identified risk item/asset/process/resource/material is required
  + The costs for mitigation/transfer are too high, but the impact is negligible if the risk transpires

# Awareness

Cyber-security at the plant-floor is essential and requires the participation of all personnel, and must cover by minimum:

* Awareness and training is required for all personnel on the existence of this I-ISMS policy
* How to conduct their work safely
* How to identify social engineering attacks (email, phone, in-person)
* Identifying tell-tale signs of a breach, how to respond, and who to notify and when

Awareness training must:

* Continually evolve and improve as needed
* Occur immediately for new employees, contractors, and visitors
* Occur annually for all engineers and factory-floor workers

# Business Continuity/Disaster Recovery

The business continuity (BC) / disaster recovery (DR) policy is to ensure all factory floor processes can be kept at normal or near-normal performance following an incident that has the potential to significantly harm the viability of NP Factory Ltd. as follows:

* The industrial automation Department of NP Factory Ltd. are responsible for the creation, review and approval, testing, and continuous evolvement of the BC/DR plan.
* BC/DR must be reviewed annually
* BC/DR must be tested at least once 2-Years

# Asset Management

All industrial automation equipment, infrastructure, computers, devices, peripherals, and software must be logged in an an asset register to:

* Identify all assets and categorize (critical, important, neutral, negligible, etc.)
* Complement the risk register (see *Risk Management*, on page 7)
* Catalog all equipment (network infrastructure, computers, servers, industrial equipment, controllers, etc.)
* Catalog all software systems and components

Frequent review and maintenance of the equipment register is required.

# Physical security

NP Factory Ltd. factory floor contains dangerous equipment that can cause serious physical harm or death.

The following applies to the factory floor:

* Access doors into the production area must remain locked at all times to prevent unauthorized access
* Other access methods (windows, vents, fire-escape, etc.) to the production area must also be protected to prevent unauthorized access

Office space within the factory floor must be secured as follows:

* Lockable door, to remain locked at all times
* Lockable filing systems / storage
* No sensitive information is visible or easily accessible (see *Clean Desk Policy* on page 11)

The following applies to the heavy equipment, devices, controllers, and computers, etc.:

* Suitably anchored to a strong surface to prevent theft or movement, etc.
* Suitably obstructed to prevent unauthorized access (e.g. behind door or secure access panel, in a lockable cage/rack, etc.)

# Clean Desk Policy

Sensitive information such as login credentials, instructions, or sensitive/confidential information etc., must not be available to unauthorized personnel. Therefore, the clean-desk policy exists as follows:

* Sensitive information must not be left in a visible and/or accessible location such as a desk, monitor, or wall, etc.
* Sensitive information must be moved to a secure location (filing cabinet, lockable drawer, etc.) when not being actively used, or when the employee must leave the location.
* Computers and operator displays must be locked or logged-out when not in use, or if an employee must temporarily leave their station.
* Desks, drawers, cabinets, closets, and other storage medium must remain locked when not in use.
* Sensitive information that is no longer needed must be disposed of via a document shredder.
* Other writing instruments such as whiteboards, blackboards, flipcharts, or electronic displays that contain sensitive information must be erased/cleaned/shredded as appropriate.
* Any portable media (CDROM, DVD, Blu-ray, USB stick, memory cards, external drives, etc.) that contains sensitive information must be locked-away or properly disposed of (destroyed) as appropriate.

# Security of third party access

The following list applies to external parties (contractors/visitors) that require access to NP Factory Ltd. assets:

* Must sign-in to a visitor’s log
* Bound to the information security policies of NP Factory Ltd.
* Access to secure areas and critical assets requires supervision at all times
* Access to controllers, computers, and servers requires either:
  + Supervision at all times, or
  + Restricted access that will limit access/capabilities and not necessitate the need for supervision

The following list applies to external parties (service-providers) that require access to infrastructure such as the network, SCADA, or equipment/devices for monitoring purposes:

* Bound to the information security policies of NP Factory Ltd.
* An appropriate agreement (service level agreement) is signed by (has legal authority) exists

A documentation trail of all third-party access, contact information, and summary of activities are required.

# Computer Usage

Computer systems are provided for employees to conduct their work in accordance with the following rules:

* Computer systems are company property and for company use only
* Employees adhere to all company policies including *acceptable use* etc.
* Software installation is prohibited, except when the software is for official company use
* Storage of personal information/data is prohibited
* Internet use is permitted on designated workstations only and is not permitted on any computer hosting SCADA systems or monitoring/controlling factory-floor equipment or processes
* Removal or deactivation of any security controls, software systems, or data, is not permitted

Factory floor computer systems must be secured as follows:

* Prevent unauthorized physical access
* Prevent unauthorized remote access
* Prevent internet access during normal operations
* Enable monitoring of key system files to detect changes
* Contain a suitably configured firewall
* Prevent the automatic update of O/S and application patches/updates
* Enable audit logging of user/system activities
* Harden the O/S and applications to remove unnecessary/unused components, services, applications, and interfaces, etc.

All other computer systems such as workstations, servers, and laptops etc. must also be secured as defined in the previous list for factory floor computers, but with the following exceptions:

* Operating system and applications are configured to automatically update with the latest patches and service packs
* Anti-virus and anti-malware components are configured to automatically update signatures

# Password Controls

Passwords must be implemented where possible, for computers, software, network infrastructure, and devices etc. and must abide by these rules:

* All users to have their own unique login password
* Passwords must be complex:
  + A minimum of 7 characters
  + Must contain upper case and lower case characters
  + Must contain a number and special character
* Passwords must be changed frequently; the interval may vary from system to system as appropriate

# Data and Configuration Backup

All company information/data and configuration settings must be backed-up as it may be required for restoration in the event of destruction or equipment failure, as follows:

* Machine configuration settings must be exported to file for secure backup; if this is not possible, then all settings must be documented instead
* PLC/controller settings and ladder-logic (programming) code must be exported to file
* Computer systems complete backup of operating system and data must be backed-up
* Backups must be automated, where possible
* Manual backups must be scheduled and under the responsibility of two or more people to assure the work is done
* Backup media (disks, CD/DVD/Blu-ray, memory-sticks, tape, etc.) must be secured using password-based encryption
* Backup media must be stored in a lockable location
* Backup media must also be stored in a Management-approved offsite location

# Virus / Malware

All computer systems are required to

* Contain adequate and up-to-date anti-virus and anti-malware
* Must be configured to:
  + automatically update anti-virus signatures
  + enable real-time scanning
  + automatically scan the whole computer system at least weekly
* Deactivation of anti-virus is prohibited

# User access control

All Department employees need access to computer equipment and/or industrial equipment and are therefore subject to the policies contain in the following sub-sections.

## Access to systems

A policy of least-privilege must be enforced for all locations, computer systems, applications, and devices/machines etc.:

* Physical systems:
  + Keys to doors, drawers, cabinets, cages, or closets, etc. are the responsibility of managers and must remain in the possession of managers only
* Electronic systems:
  + Users that need access shall be granted access, only
  + Users that are granted access must receive the capabilities they need only

## Registering users

The modification of systems to adjust access must be continuous and based on a review of the appropriate manager/management as follows:

* The addition of new users must be approved by a manager with clear direction on the capabilities needed by the user
* The modification of existing users must be approved by a manager
* The removal of existing users must be approved by a manager

## Employees leaving

This policy requires the following whenever an employee leaves NP Factory Ltd.:

* Keys to doors, cages, cabinets, drawers, etc. must be retrieved
* Information and confidential information that is in print, or stored on medium such as CD/DVD, USB, online storage etc. must be returned
* Access to computer systems must be removed
* Access to industrial equipment must be removed
* Access to sensitive/confidential information must be removed

## Visitors and contractors

The following must be enforced in order to protect company assets, processes, configuration settings, and confidential information:

* Administrative access to any device, computer, or system etc., is prohibited unless constant supervision from NP Factory Ltd. employee(s) is available.
* If visitor requires access to a device or computer system for extended periods of time, then a temporary account should be created and used that is:
  + Limited in capabilities
  + Expires at a specific date/time

## The internet

Internet access has the potential to completely disrupt business operations. Therefore, all persons accessing the internet do so within the scope and boundaries of all NP Factory Ltd. policies.

* Internet access from factory-floor computers is strictly prohibited
* Internet access is permitted on designated computers only
* Use of an approved browser with an approved configuration only
* Use of an approved email client with approved client configuration only
* All activity is logged
* The removal of browsing history and cache is not permitted

# Equipment security

## Equipment sitting and protection

Industrial equipment is expensive, complex, and dangerous. To protect personnel and factory investments the following applies to all equipment, devices, PLCs/controllers, computer systems, and peripherals, etc.:

* must be physically secured to a stable surface to assure safety, to prevent theft, and to assure continuous production
* all available security controls that exist to protect the equipment are utilized, e.g. lockable doors/panels, security coded screens, etc.

## Power supplies

The power to equipment may vary from small electronics utilizing mAmps to heavy equipment using 480v or more. Power supply is essential and therefore:

* All power-outlets must be secured for authorized personnel only
* All power-connectors to devices must be secured for authorized personnel only
* All power cables must be anchored to stable surfaces to eliminate any movement
* All power cables must be shielded to prevent damage or disruption
* All power adapters, cables, and plugs must be cataloged in the asset register

## Network security

The communications platform required by the plant-floor computer systems, controllers/PLCs, and machines/devices etc., must be secured as follows:

* Network infrastructure components (routers, switches, firewalls, etc.) are accessible to authorized personnel only, is sufficiently hardened to reduce attack surfaces, and is physically protected in a safe location (room or rack, etc.)
* Network cabling is secured from accidental damage
* Network access is restricted to authorized users only, and authorized equipment only
* Network communications (protocols) are limited to authorized applications and systems only, and inter-device communications are controlled
* External network access, if required, is highly restrictive and limited to authorized personnel and systems only
* All network activities are logged

## Operational security

The successful operations of production are dependent on numerous systems which must be secured as follows:

* Network infrastructure (see *Network security*, above) and computer systems (see *Physical security*, on page 10 and *Computer Usage*, on page 12) are adequately secured from unauthorized access or re-configuration
* Device/Machine/Equipment access and configuration is secured (see *User access control*, on page 15)
* Device configuration is documented (see *System documentation*, on page 19)
* Device configuration is reviewed by a change-review board and is approved for use (see *Configuration Management*, below)
* Device configuration is backed-up (see *\*Data and Configuration Backup*, on page 14)

## System documentation

Documentation of systems is required to eliminate risk of knowledge loss, and to assure knowledge transfer to authorized employees. Systems documentation may be required by factory floor personnel or contractors.

All systems must be documented and stored in an approved document library:

* secured for read-only access to authorized personnel only
* secured for modification access to authorized personnel only
* structured to provide versioning control

Documentation must include:

* factory processes and the equipment needed
* system configuration
* user access
* integration and relationship of components, systems, and devices

# Configuration Management

Industrial equipment requires significant effort, skill, and time to define and test and must be protected from accidental loss or intentional destruction etc.:

* A change-review board must be established and take responsibility for configuration settings management, review, approval, and documentation of requests, risk analysis, recommendations, and decisions made etc.
* Changes to configuration settings must go through a review process with the change-review board to assure safety, accuracy, and efficiency, while reducing risk
* Only approved personnel may change configuration settings after receiving written approval from the change-review board
* Any changes made to configuration settings must be documented.
* Configuration settings must be backed-up (see *\*Data and Configuration Backup* on page 14)

# Monitoring and Continuous Improvements

The implementation of an I-ISMS will not eliminate the potential of cyber-attacks or sabotage from malicious employees. Therefore, monitoring of the complete program is required in order to improve the effectiveness of the controls put in place.

* Supervision of overall monitoring assigned to a principal engineer

The following is required for monitoring processes and logs to detect breaches:

* Daily reviews of computer system security information (alerts, logs, emails, on-screen reports etc.) by minimum; assigned to a competent and responsible engineer
* Frequent reviews of industrial equipment access and logs (where possible) with a minimum of 1 review per week.
* Summary reports to be provided in regular engineering team meetings

The monitoring of the I-ISMS program is described in section *Review and audit*, on page 6.

# Security Breach & Incident Management

Security breaches vary by type, such as the unauthorized access to data/systems, theft or modification of information, sabotage from an employee, or virus/malware attack.

The detection of a security breach requires:

* immediate attention and escalation to the principal engineer in charge
* immediate attention and escalation to the most senior person available
* Follow the plan in the risk register, as appropriate

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Change** | **Section** | **Approver** |
| 1 | 2-Sep-16 | Initial Creation | n/a |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |