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

**Plant floor**

**Industrial Information Security Management System**

Rapid Adoption Instructions

Nathan Pocock

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

|  |  |
| --- | --- |
| **I-ISMS Revision** 1 (74) | Industrial Information Security Management System  Rapid Adoption Instructions  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Quality assurance**

PRIVATE

|  |  |
| --- | --- |
| 00 - Instructions.Docx  Version: 1 Revision 74  Pages: 15 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\00 - Instructions.docx  Keywords: iisms, isms, quality, implementation, wizard, instructions, howto  Last Saved by Nathan Pocock on 9/23/2016 11:49 AM |
|  | [Company]  [Company Address]  Plant floor  I-ISMS  704-491-5840  [Manager] |

Executive Summary

A simple step-by-step guide to help factory plant-floor engineers to rapidly adopt an industrial-oriented information security management system (I-ISMS), as a first-step towards a full-blown ISMS.

Revision History

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

Contents

[1 Plan 7](#_Toc462394914)

[1.1 Set Your Company Logo 7](#_Toc462394915)

[1.2 Define I-ISMS Company Policy 7](#_Toc462394916)

[1.3 Scope Definition 8](#_Toc462394917)

[1.4 Complete the Implementation Plan 8](#_Toc462394918)

[1.5 Build Asset Register 8](#_Toc462394919)

[1.6 Conduct Risk Analysis 8](#_Toc462394920)

[1.6.1 Risk Management Plan 9](#_Toc462394921)

[1.6.2 Risk Assessment 9](#_Toc462394922)

[1.7 Complete Statement of Applicability 9](#_Toc462394923)

[1.8 Define Awareness Training Plan 9](#_Toc462394924)

[2 Do 9](#_Toc462394925)

[1.1 Review Information Security Vulnerability Analysis 9](#_Toc462394926)

[1.2 Conduct Vulnerability Assessment 10](#_Toc462394927)

[1.3 Complete the Risk Treatment Plan 10](#_Toc462394928)

[1.4 Complete the Security Controls Identification and Implementation 10](#_Toc462394929)

[1.5 Complete the Business Continuity Plan (BCP) 10](#_Toc462394930)

[1.6 Complete the Metrics and Measurements 10](#_Toc462394931)

[1.7 Follow the Security Hardening Implementation Guidelines 11](#_Toc462394932)

[1.7.1 Windows Based PCs 11](#_Toc462394933)

[1.7.2 PLC Controllers / Equipment 11](#_Toc462394934)

[1.7.3 Document all changes 11](#_Toc462394935)

[1.8 Test 11](#_Toc462394936)

[3 Check 12](#_Toc462394937)

[1.1 Monitor logs 12](#_Toc462394938)

[1.2 Complete the Internal Audit checklist 12](#_Toc462394939)

[1.3 Identifying and Escalating Attacks 12](#_Toc462394940)

[4 Act 12](#_Toc462394941)

[1.1 Review the Act documentation 12](#_Toc462394942)

[1.2 Review the procedures for Responding to a situation 13](#_Toc462394943)

[5 Ongoing Maintenance 13](#_Toc462394944)

[6 Suggested Document Directory Structure 13](#_Toc462394945)

Figures

**No table of figures entries found.**

Industrial Information Security Management System Implementation Steps

This documentation library template exists to expedite the implementation of an Industrial Information Security Management System (I-ISMS) by providing document templates for rapid document development, and sample forms for expedited analysis and reporting.

This guide is split into Plan, Do, Check, and Act sections.

Estimated time to completion is provided in each section.

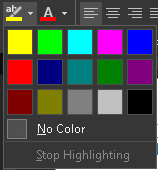
# Plan

## Set Your Company Logo

1. Replace the “CompanyLogo.jpg” graphic with your own. **Estimated time**: 1 minute

## Define I-ISMS Company Policy

The I-ISMS company policy will serve as your security framework *rulebook*. It defines the need for security, what needs to be secured, how to secure it, how to monitor the status of security, preparing for and responding to breaches/attacks.

1. Complete the [I-ISMS Company Policy](Plan%20-%2001%20--%20IISMS-CompanyPolicy.docx) document **Estimated time**: 2-4 hours
2. Open the document Properties and set the company name and author
3. Click the Custom tab and set the remaining properties before closing the window
4. Read each section and revise content as necessary  
   Note: yellow background text indicates a value set by document properties
5. Once done, select all (CTRL+A) and then press F9 (to re-paginate and tabulate) and then clear all text backgrounds by selecting “No Color”:   
   

## Scope Definition

Now to narrow down who and what will be included within the scope of the I-ISMS, and what will be excluded:

1. Complete the [Scope Definition](Plan%20-%2002%20--%20Scope%20Definition.docx) document **Estimated time**: 1-2 hours

## Complete the Implementation Plan

Prepare a plan to implement the I-ISMS **Estimated time**: 2-3 hours

1. Update [Implementation Plan](Plan%20-%2003%20--%20Implementation%20Plan.docx)

## Build Asset Register

Analyze your factory floor industrial automation equipment for devices that require cyber-security attention.

Most of the time spent completing this form will be actual investigation of equipment on the plant-floor.

1. Complete the [Asset Register](Plan%20-%2004%20--%20Asset%20Register.docx) document **Estimated time**: 2-3 days
2. Open the document Properties and set the company name and author
3. Click the Custom tab and set the remaining properties before closing the window
4. Review the instructions to understand what specifically to register

## Conduct Risk Analysis

This section consists of 2-parts; first, the definition of the risk management plan, and second, conducting an actual risk analysis.

### Risk Management Plan

1. Review the [Risk Management Plan](Plan%20-%2005%20--%20Risk%20Management%20Plan.docx) document **Estimated time**: 2-4 hours
2. Open the document Properties and set the company name and author
3. Click the Custom tab and set the remaining properties before closing the window
4. Make any changes as necessary.

### Risk Assessment

Using your asset register (on page 8) conduct a risk analysis to determine the risks that exist from a cyber-security standpoint only.

1. Complete the [Risk Register](Plan%20-%2006%20--%20Risk%20Register.docx) document **Estimated time**: 1-2 days

## Complete Statement of Applicability

The statement of applicability is a mapping of the documentation and deliverables to the I-ISMS policy.

1. Update the [Statement of Applicability](Plan%20-%2007%20--%20Statement%20of%20Applicability.docx) document **Estimated time**: 1-hour  
   Note: complete what you can; some elements will be done later

## Define Awareness Training Plan

The awareness plan is something that you will need to create. **Estimate time**: 1-2 days  
Some suggestions:

1. Define a single-page cyber-security awareness “cheat-sheet” that users can use at their desk:
   1. Customize the single-sheet to be more specific to specific roles or departments, etc.
2. Plan an introductory/training session of no more than 2-hours to train users
3. Provide the awareness sheets to HR with instructions to train new-hires and dept. transfers
4. Instruct HR to notify you whenever a plant-floor employee leaves the company.

# Do

## Review Information Security Vulnerability Analysis

In order to best-protect your systems you must be able to conduct an appropriate analysis:

1. Review the [Guide to InfoSec Vulnerability Analysis](Do%20-%2001%20--%20Guide%20to%20Infosec%20Vulnerability%20Analysis.docx) **Estimated time**: 1 hour

## Conduct Vulnerability Assessment

Obtain a baseline of the current status of equipment for vulnerabilities and weaknesses:

1. For each PC, PLC, or networked industrial device **Estimated time**: 1-2 hours
2. Scan each device
3. Create a new [vulnerability report](Do%20-%2002%20--%20Computer%20Vulnerability%20and%20Risk%20Analysis.dotx) and paste findings to it

## Complete the Risk Treatment Plan

After reviewing the risk analysis, you must complete document all decisions made:

1. Create new instance [Risk Treatment Plan](Do%20-%2005%20--%20Business%20Continuity%20Plan.docx) **Estimated Time**: 1-2 hours
2. Complete the Risk Treatment table
3. Update the document as the status of each action item is reported.

## Complete the Security Controls Identification and Implementation

Define the security controls that are available within your organization, and then specify where and when you will use them:

1. Complete the [Security Controls Identification and Implementation](Do%20-%2004%20--%20Security%20Controls%20Identification%20and%20Implementation.docx) **Estimated time**: 1-hour

## Complete the Business Continuity Plan (BCP)

Plan for the disaster scenario that causes the production process[es] to fail. One or more BCP/DRP (disaster recovery plan) may be required:

1. Create a new BCP for a given process **Estimated time**: 2-3 days  
   Use [Business Continuity Plan](Do%20-%2005%20--%20Business%20Continuity%20Plan.docx) template
2. Repeat step #1 for each additional process, e.g. paint, canning, shipping, etc.

## Complete the Metrics and Measurements

Define how you are going to measure/gauge your IISMS’s performance:

1. Modify the [Metrics and Measurements](Do%20-%2006%20--%20Metrics%20and%20Measurements.docx) document **Estimated time**: 1-2 hours

## Follow the Security Hardening Implementation Guidelines

### Windows Based PCs

For each Windows-based computer system on the network, conduct the following:

1. Follow the [Windows hardening guide](Do%20-%2007%20--%20Guide%20to%20Windows%20Hardening.docx) **Estimated time**: 1-2 hours
2. Follow the [Windows Firewall hardening guide](Do%20-%2008%20--%20Guide%20to%20Windows%20Firewall%20Hardening.docx) **Estimated time**: 1-2 hours
3. Follow the [Windows Monitoring guide](Do%20-%2010%20--%20Guide%20to%20Windows%20Monitoring.docx) **Estimated time**: 4-8 hours

### PLC Controllers / Equipment

A general framework document is provided with questions to help you identify the security capabilities provided. This is because of the wide variations in manufacturers and devices present in any production line.

1. Review the [Device hardening guide](Do%20-%2009%20--%20Guide%20to%20Device%20Hardening.docx) **Estimated time**: 1-2 hours

#### Ladder Logic Review

Conduct a review of PLC ladder logic. **Estimated time**: 4-hours

In this exercise you are specifically looking for vulnerabilities in the safety parameters of the program. Identify all variables that control machine/process safety and assure adequate input validation is present.

### Document all changes

For each PC, PLC, or networked industrial device whose configuration is modified, you must create an appropriate documentation trail to store the changes applied

1. For each PC, PLC, or device **Estimated time**: 1-2 hours
2. Edit or create a new [change-history document](Do%20-%2011%20--%20Computer%20Change%20History.dotx)

## Test

Now that you have hardened your systems you need to test them.

1. Conduct a vulnerability scan of computers and devices **Estimated time**: 1-3 hours
2. Try to bypass security, e.g. do not logon or enter a PIN etc.
3. Try to run applications that are not allowed, or install new applications etc.
4. Try to do anything/everything that you should not be able to do

# Check

## Monitor logs

The following is your frequent (daily?) chore chart: **Estimated time**: ½-1 hour

1. Review the [PC Monitoring guidance](Do%20-%2010%20--%20Guide%20to%20Windows%20Monitoring.docx) document
2. Check the logs in the centralized log monitoring server
3. Check the logs for each device that is forwarding logs to a centralized server

## Complete the Internal Audit checklist

Conduct Internal audits to determine compliance with your I-ISMS policy: **Estimated time**: 2-3 days

1. Create a new instance of the [Internal Audit checklist](Check%20-%2002%20--%20Internal%20Audit%20Checklist.docx)
2. Conduct the internal audit
3. Report all findings within the document
4. Share findings with your team
5. Plan and document your response to fix any non-compliance, risks, vulnerabilities, and improvements.
6. Assign action items to appropriate resources
7. Monitor action items for completion.

## Identifying and Escalating Attacks

1. Review the [Guide to incident handling](Check%20-%2003%20--%20Guide%20to%20Incident%20Handling.docx) document **Estimated time**: 1-hour
2. Gather details and escalate as appropriate

# Act

## Review the Act documentation

As part of your overall project management you must ensure action items are properly managed by assigning them to resources and conducting the necessary follow-ups to verify the work is complete and the issues are resolved.

## Review the procedures for Responding to a situation

Once an issue is resolved use the situation as a learning opportunity to make improvements to knowledge and capabilities. Document those lessons learned and use those lessons as improvements that can be made to the I-ISMS program, policies, procedures, guides, and training/awareness materials etc.

# Ongoing Maintenance

What do you do now that your I-ISMS is finished? You continue to use it by following the same Plan-Do-Check-Act steps.

At this point, you are trying to accomplish two things:

1. Assure the rules and infrastructure in place are working as intended and that all personnel abide by all policies
2. Find areas that can be improved and then actually improve them by enhancing existing documents and processes, or by adding new documentation and processes.

# Suggested Document Directory Structure

A great number of documents exist as part of this framework, in addition to those documents that you will create. Organizing such a library can be difficult.

Consider the following directory structure:

|  |  |  |
| --- | --- | --- |
| Directory Name / Structure | Suggested Contents | Suggested Access Rights |
| / | Root folder; contains all I-ISMS files/folders | Everyone=read Admins=modify |
| ./i-isms/ | Contains the I-ISMS deliverables, including:   * I-ISMS company policy * Scope definition * Implementation plan * Security controls identification * Business continuity plan * Metrics and measurements * Risk management plan * Statement of applicability | default |
| ./templates/ | Contains the various templates for rapid document generation, such as:   * Internal Audit Checklist * Computer Vulnerability and Risk Analysis * Risk treatment plan * Computer change history | Admins=read |
| ./guides/ | Contains the various step-by-step instruction guides, including:   * Guide to Incident Handling * Guide to Infosec Vulnerability Analysis * Guide to Windows hardening * Guide to Windows firewall hardening * Guide to Device handling | Admins=modify |
| ./register/ | Contains the asset register and other registers:   * Asset Register |  |
| ./infrastructure/ | Contains and change history for each computer system, network appliance, controller, and networked industrial device, etc.   * Asset register   For example:   * Switch #1.docx * Firewall #1.docx * SCADA PC #1.docx * SCADA PC #2.docx | Admins=modify |
| ./risks/ | Contains the risk register:   * Risk register   Also contains risk management documents, organized by year | Admins=modify |
| ./<year> | Stores the risks found, decisions made, and treatment plans:   * Risk treatment plan | Admins=modify |
| ./versioning/ | Each I-ISMS document that is revised shall be saved in its original directory with the new version in the filename. The file is then copied to this directory.  For example:   * I-ISMS Policy v1.docx * I-ISMS Policy v2.docx * Scope Definition v1.docx * Risk Management v1.docx * Risk Management v2.docx | Admins=read, add |
| ./audits/ | Directory that stores sub-directories representing the year and/or project, whichever is the most convenient. | Admins=modify |
| ./<year>/ | Contains the internal audit details for the given year, for example:   * Internal Audit Checklist * Risk Treatment Plan * Other supporting documents |  |
| ./<project>/ | (As above) |  |