ISMS Management Review report

# Table of Contents

[Table of Contents 2](#_Toc453595623)

[Participants: 3](#_Toc453595624)

[1. Management Review input 3](#_Toc453595625)

[1.1. Information Security Policy 3](#_Toc453595626)

[1.2. Status of actions from previous management reviews 3](#_Toc453595627)

[Planned improvement activities related to Information Security (from Management Review 2015) 4](#_Toc453595628)

[1.3. Changes in external and internal issues that are relevant to the ISMS 4](#_Toc453595629)

[1.4 Feedback on the information security performance, including trends in: 4](#_Toc453595630)

[**1.4.1 Nonconformities and corrective actions** (by QM) 4](#_Toc453595631)

[**1.4.2 Monitoring and measurement results** (by SM) 4](#_Toc453595632)

[**1.4.3 Audit results** (by QM) 5](#_Toc453595633)

[**1.4.4** **Fulfilment of information security objectives** (by QM) 5](#_Toc453595634)

[1.5 Feedback from interested parties (by QM) 5](#_Toc453595635)

[1.6 Results of risk assessment and status of risk treatment plan (by QM) 5](#_Toc453595636)

[1.7 Opportunities for continual improvement (by MD) 5](#_Toc453595637)

[2 Management Review Output (by MD) 6](#_Toc453595638)

[2.1 Decisions related to continual improvement opportunities 6](#_Toc453595639)

[2.2 Any needed changes to the information security management system 6](#_Toc453595640)

[Revision management 7](#_Toc453595641)

[Version history 7](#_Toc453595642)

[Version control of documents 7](#_Toc453595643)

[Revision management 7](#_Toc453595644)

# Participants:

|  |  |
| --- | --- |
| **Position** | **First name, last name** |
| Managing Director |  |
| Quality Manager |  |
|  |  |

# Management Review input

## Information Security Policy

**Information Security Policy:**

“

.”

Updated to:

“

.”

## Status of actions from previous management reviews

(by QM)

# Planned improvement activities related to Information Security (from Management Review 20xx)

The following improvement activities were planned to take place:

|  |  |  |
| --- | --- | --- |
| Improvement activity | Status | Notes |
| Asset Management and Access Management process | On hold | In process again |
| Design and implement a common principle for Access Management DB | On hold | Completed |
| Assign new responsible for IS related roles | Done |  |
| Merge IS manual with Quality Manual, when the new ISO 9001 version is released | In process | Audits merged |

## Changes in external and internal issues that are relevant to the ISMS

(by MD)

* New approach for Knowledge management
* Organization structure changes.

## 1.4 Feedback on the information security performance, including trends in:

### **1.4.1 Nonconformities and corrective actions** (by QM)

For details please see the NC register.

### **1.4.2 Monitoring and measurement results** (by SM)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Metrics** | **Responsible for monitoring and measuring** | **Frequency of monitoring and measuring** | **Responsible for analysis and evaluation** | **Frequency of analysis and evaluation** | **Report** | **Conclusions** |
| Services - Patch management, Antivirus, GPO | VCOT | Permanently | TLs | Permanently | In the system | No significant deviations identified |
| Information Security Incidents monthly overview by QAT | QAT | Monthly | IS Manager | Monthly | Please see QAT monthly reports | IS Incident Management process implemented works properly |
| HR confidentiality – registered disciplinary cases. | HR BP | Annually | HR BP | Annually | Registry of disciplinary cases: 11 | Disciplinary process works properly |
| Continuity related to HR – Voluntary leaving turnover rate | HR BR | Permanently | HR BP | Permanently | HRM DB: 42,35% | Activities implemented to increase loyalty thus decreasing turnover |
| Subcontractors confidentiality – IS incidents related to subcontractors |  | Permanently | BU Manager | Permanently | In 2016 - 0 | No incidents/escalations were reported. |
| Internet up-time – 97% | IT Division Director | Permanently | IT Division Director | Permanently | 97% | Acceptable |
| Electricity up-time – all the time | IT Division Director | Permanently | IT Division Director | Permanently | 1h loss | Acceptable |
| file server availability – all the time | IT Division Director | Permanently | IT Division Director | Permanently | 1h downtime | Acceptable |
| SCSM availability – 99.47% | IT Division Director | Permanently | IT Division Director | Permanently | 99.5 | Acceptable |

### **1.4.3 Audit results** (by QM)

Please see audit results.

**Conclusions:** Continuous follow up on CAs.

### **Fulfilment of information security objectives** (by QM)

* Information management system`s goal is to protect the organizations informational assets against all internal, external, deliberate or accidental threats.
* will always strive to follow the best practices and fulfill all ISO/IEC 27001 standard requirements.
* The main objective of information security policy is to ensure the business continuity of {} and minimize the risk of damage by preventing incidents and reducing their potential impact.

|  |  |  |  |
| --- | --- | --- | --- |
| **IS Objectives** | **Responsible** | **Deadline** | **Notes** |
| Implement information security checks in the IQMS in order to merge all standards in one system | PO |  | In process |

## Feedback from interested parties (by QM)

0 Security Incidents registered based on information received from the customers. No complaints related to the IS.

## Results of risk assessment and status of risk treatment plan (by QM)

Please see Information Security Risk Assessment.

Highest risk areas:

* .

**Conclusions:** Follow-up on risk assessments and treatment.

## Opportunities for continual improvement (by MD)

* Azure services with centralized security system – in process

# Management Review Output (by MD)

## Decisions related to continual improvement opportunities

Azure services with centralized security system

Processes` improvements.

## Any needed changes to the information security management system

* Access Management and Asset Management continuous improvement.

# Revision management

## Version history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status: Main Changes** | **Changed by** | **Pages** |
| 0.1 |  |  |  |  |
| 1.0 |  |  |  |  |

## Version control of documents

The steering group of the service organization must approve all revisions to be made to the document after the document has been approved. The first approved version is v. 1.0.

Every version produced after version 1.0 requires filling in and approval of the version control form.

## Revision management

A separate revision control form is used as an instrument in revision management. Both the owner of the service or process and the management or steering group of the service organization must approve all such revisions as have an impact on the subject matter, costs, or end result.