**Information Security**  
**ObjectObjectives and Implementation Plan**

|  |  |
| --- | --- |
| DOCUMENT CLASSIFICATION | Internal Use |
| DOCUMENT REF | ISMS-DOC-06-1 |
| VERSION | 1 |
| DATED | [Insert date] |
| DOCUMENT AUTHOR | Julian VanDeventer |
| DOCUMENT OWNER | Group 3 |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | REVISION AUTHOR | SUMMARY OF CHANGES |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |
| --- | --- |
| NAME | TITLE |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | POSITION | SIGNATURE | DATE |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Introduction 8](#_Toc42602235)

[2 Information security objectives 9](#_Toc42602236)

[3 Plan to achieve objectives 11](#_Toc42602237)

[4 Resources to manage and improve the ISMS 13](#_Toc42602238)

[4.1 Human resources 13](#_Toc42602239)

[4.2 Technical resources 13](#_Toc42602240)

[4.3 Information resources 14](#_Toc42602241)

[4.4 Financial resources 14](#_Toc42602242)

[5 ISMS risks and opportunities 15](#_Toc42602243)

[5.1 Risks to the ISMS 15](#_Toc42602244)

[5.2 Opportunities for the ISMS 16](#_Toc42602245)

[6 Conclusion 17](#_Toc42602246)

Tables

[Table 1: Information security objectives 10](#_Toc42602247)

[Table 2: Plan to achieve objectives 12](#_Toc42602248)

[Table 3: Human resources required to run the ISMS 13](#_Toc42602249)

[Table 4: Risks to the ISMS 15](#_Toc42602250)

[Table 5: Opportunities for the ISMS 16](#_Toc42602251)

# Introduction

Northwoods Naturals is committed to establishing clear objectives and an effective information security plan to protect its key business activities and meet its obligations to interested parties, including customers, shareholders, employees and suppliers.

As part of this commitment, the organization has established an Information Security Management System (ISMS) that complies with the requirements of the ISO/IEC 27001 international standard for information security and will be seeking certification to this standard in the near future.

In line with the standard, it is essential that our information security objectives are consistent with our policies, measurable where practicable, communicated effectively within the organization (and outside where appropriate) and updated as part of the ISMS management review process.

Objectives will be based on a clear understanding of our information security requirements, including those from interested parties, and will consider the results of risk assessments carried out at various levels within the organization.

Northwoods Natural’s plan to meet its information security objectives is also described, including:

* What will be done
* What resources will be required
* Who will be responsible
* When it will be completed
* How the results will be evaluated

This document should be read in conjunction with other components of the ISMS, which give background information about internal and external issues relevant to the organization’s purpose, the requirements of interested parties and the organization’s information security policy.

# Information security objectives

In order to assess whether the ISMS is working as intended it is essential that clear objectives are defined, and a system of monitoring and measurement established to record progress against targets.

High-level objectives for information security are described in the ISMS document *Information Security Context, Requirements and Scope* and the overall framework for setting lower-level objectives is defined in the *Information Security Management System Manual*, also a key component of the ISMS.

Methods for determining to what extent objectives are being met are set out in the document *Process for Monitoring, Measurement, Analysis and Evaluation*.

As part of the ISMS management review process, objectives for information security are regularly set, reviewed and updated in the following major areas:

* Quality – generally how well the organization’s information security assets are protected by the ISMS
* Capability – the knowledge, skills and experience available, mainly internally but also to some extent externally to the organization
* Cost – financial resources required to maintain and improve the ISMS
* Resource utilisation – how effectively organizational resources are employed
* Risk reduction – the degree to which known risks are treated to within acceptable limits
* Other – appropriate objectives that do not fall into any of the above areas

In discussion with the management team and based upon documented requirements, Northwoods Naturals has agreed specific objectives in the area of information security as shown in Table 1 below.

Achievement against these objectives will be tracked as part of regular management reviews of the ISMS.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| REF | AREA | OBJECTIVE | MEASUREMENT METHOD | TARGET | TIMESCALE | OBJECTIVE OWNER |
| 1. | Education | All employees in Northwoods Naturals has attended and passed all required training and awareness programs listed in the policy. | Rating of reports and audits on the training and awareness | 80% | Jan 20xx | Information Security Manager |
| 2 | Education | Properly organize training for the different locations located around the world. Different time zones and personal can pose a challenge | Working closely with international management employees to ensure that all locations participate in the required training | 100% | Jan 20xx | CIO |
| 3. | Capability | Training in information security has been provided for all key resources | Number of people trained | 50 | Feb 20xx | Information Security Manager |
| 4. | Cost | Reduce amount spent on information security | Percentage reduction on last year’s budget | 5% | Apr 20xx | Information Security Manager |
| 5. | Resource utilisation | Increase number of days provided by business teams for information security activities | Percentage increase over last year’s commitment | 10% | Dec 20xx | Chief Operations Officer |
| 6. | Risk reduction | Reduce number of high priority risks on risk register via education and training of employees | Percentage reduction | 10% | Apr 20xx | Information Security Manager |
| 7. | Security | All servers have anti-virus installed | Percentage of servers with anti-virus installed | 100% | May 20xx | Chief Information Officer |

Table 1: Information security objectives

# Plan to achieve objectives

In order to achieve our objectives, it is essential that we have a clear plan that is adequately resourced and has the full support of top management. The success of this plan will determine whether Northwoods Naturals remains adequately protected against unwanted events and their potential impacts.

The plan is shown in Table 2 below. The tasks required in order to achieve each objective are listed, together with the resources required, person responsible and completion timescale for each one. The method of evaluating the success of each task will vary according to the nature of the task, but an attempt to determine this is also shown.

This plan will be managed in conjunction with background improvement activities, which may be driven by internal and external audit results, risk assessments and management reviews, amongst other sources. Additional, more detailed plans may also be created in order to control the activities required and take account of internal and external dependencies.

Progress against the plan will be tracked by the Information Security Manager and reported to top management on a regular basis. If a task is looking unlikely to be completed within the target timescale, the effect on the relevant information security objective should be evaluated. Depending on the conclusion, top management may decide whether to act, such as increasing the resources available, to improve the expected completion time.

If information security objectives are changed, the associated plan will also need to be revised.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| REF | OBJECTIVE | TASKS | RESOURCES REQUIRED | PERSON RESPONSIBLE | COMPLETION TIMESCALE | EVALUATION METHOD |
| 1 | All identified controls are in place | List controls  Implement controls  Verify controls | Specialist IT team  Internal audit | Information Security Manager | 12 months | List of signed off controls |
| 2 | All business continuity plans have been tested with the last 2 years | Agree testing schedule  Conduct tests  Produce test reports | Operational staff time | Business Continuity Manager | 12 months | Business Continuity test reports |
| 3 | Training in information security has been provided for all key resources | Identify key resources  Identify courses  Attend courses  Complete training records | Training budget  Time of attendees | Information Security Manager | 6 months | Training records |
| 4 | Reduce amount spent on information security | Review budget  Identify savings  Evaluate effect of reduction | Finance Manager | Information Security Manager | 12 months | Financial budget reports |
| 5 | Increase number of days provided by business teams for information security activities | Agree allocation with top management  Plan involvement  Conduct activities  Record days spent | Business teams | Chief Operations Officer | 12 months | Timesheets of key personnel |
| 6 | Reduce number of high priority risks on risk register | Hold workshops to identify ideas  Implement ideas  Reassess risks | Risk owners  IT team | Information Security Manager | 9 months | Risk register |
| 7 | All servers have anti-virus installed | Identify servers without AV  Install AV and verify | IT specialist | Chief Information Officer | 3 months | Reports from enterprise anti-virus software |

Table 2: Plan to achieve objectives

# Resources to manage and improve the ISMS

In addition to the specific resources required to meet the objectives set out within this document, the following resources will be required on an ongoing basis to manage and improve the ISMS.

## Human resources

The human resources needed for the ISMS are shown in Table 3 below. For more details of the specific responsibilities and authorities of the roles described here, see the document *Information Security Roles, Responsibilities and Authorities*.

|  |  |  |
| --- | --- | --- |
| ISMS ROLE | RESOURCES REQUIRED | COMMENTS |
| Information Security Manager | 1 x Full Time Equivalent | Assumed to be a full-time role |
| Information Asset Owners | 1-3 days per quarter | Depends upon nature and number of assets owned |
| Department Managers | 2 days per annum | Mainly awareness activities and participation in incident investigations |
| IT Technicians | No additional resource | Information security is already part of relevant roles |
| IT Users | 1 day per annum | Attendance at awareness events and participation in the Annual Cyber Security Training |

Table 3: Human resources required to run the ISMS

## Information resources

Additional reports and audits on the training awareness program and the implementation plan may be needed to ensure that the ISMS is properly implemented into Northwoods Naturals. These reports and audits will test if the goals if the goals established are being met within the organization.

## Financial resources

An increased budget in key departments may be required to meet all of the requirements stated in the training and awareness program and the implementation plan. These key departments can include human resources, IT department and management to ensure they have the resources necessary to accomplish their goals.

# ISMS risks and opportunities

## Risks to the ISMS

The following risks have been identified to the effectiveness of the ISMS. These will be managed and updated as part of regular management reviews and the effectiveness of the treatment actions evaluated over time.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REF | RISK | RISK OWNER | LIKE- LIHOOD | IMPACT | SCORE | RISK LEVEL | TREATMENT ACTIONS | TIMESCALE |
| 1 | Resources may not be available to take on the proactive elements of information security management that are not currently being carried out. | CISO | 3 | 2 | 6 | Low | Increase available resources for information security management by increasing funding from executives | 12/31/2025 |
| 2 | Staff fail to engage with the ISMS leading to issues with the implementation of controls | CISO | 3 | 3 | 9 | Medium | Implement enforceable actions to encourage employees to retain training and knowledge | 12/31/2025 |
| 3 | Management are not sufficiently involved in the creation of the new management system to carry it forward once certification gained | CISO | 2 | 4 | 8 | Medium | Implement enforceable action for the management to ensure they a continuously driving for maintaining the ISMS | 12/31/2025 |

Table 4: Risks to the ISMS

## Opportunities for the ISMS

The following opportunities have been identified which may assist in preventing or reducing undesired effects or achieving continual improvement within the ISMS:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| REF | OPPORTUNITY | OPPORTUNITY OWNER | POTENTIAL BENEFIT | ACTIONS | TIMESCALE |
| 1 | Recent security breaches at competitor organizations have raised the profile of information security in the industry | Information Security Manager | May make it easier to convince management of the need for additional controls | Identify controls that may have prevented the breaches at competitors | 6 months |
| 2 | Increased budget in key departments | Information Security Manager | Some of this budget could be invested in additional security controls | Discuss with department heads | 12 months |

Table 5: Opportunities for the ISMS

# Conclusion

The objectives defined within this document are critical to defining the core purpose of the ISMS and measuring its success. These objectives provide a clear answer to the question of why business resources need to be allocated to the area of information security and so go some way toward justifying the budget requested.

The objectives set for the period under consideration are intended to be challenging but achievable and will go a long way to protecting the organization from security incidents that may occur both now and in the future.

The creation of a plan to achieve these objectives is an essential part of the continual improvement of the ISMS within Northwoods Naturals Taken in conjunction with the internal audit and management review processes, this should help to ensure that we have in place an effective mechanism for managing information security in the longer term.