
# Information Security Objectives Plan - 2023

Reference: RECOBJ-2023-2022

Version: 2

Owner: James Pobgee

First Issued Date: 29/09/2023

Revision Issued Date:

**Prepared for:**
All Employees, select Contractors, Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

FISCAL TECHNOLOGIES

# 1 CONFIDENTIALITY



# Table of Contents

# 2 DOCUMENT CONTROL

| Item | Description |
|---|---|
| Document Title: | Information Security Objectives Plan - 2023 |
| Associated Controls: | 10.1 4.1 4.2 5.1 6.1 6.1.1 6.2 7.1 7.2 9.1 9.3.1 9.3.2 9.3.3 |
| Reference ID: | RECOBJ-2023-2022 |
| Version: | 2 |
| Status: | Draft |
| Approver: | |
| Approval Date: | |
| First Issued Date: | 29/09/2023 |
| Revision Issued Date: | |
| Reference Documents: | Linked Policies:<br>• Information Security Governing Policy<br>Linked Procedures:<br>Linked Records: |

## 2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

| Version | Date | Author |
|---|---|---|
| 1 | 09/05/2023 | Marius Vanaswegen |
| 2 | | James Pobgee |

# 3 INTRODUCTION

FISCAL technologies are 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 organisation 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 organisation (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. They will consider the results of risk assessments carried out at various levels within the organisation.

To meet our information security objectives, we will describe:

- **What will be done?**
- **What resources will be required?**
- **Who will be responsible?**
- **When will it 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 organisation's purpose, the requirements of interested parties and the organisation's information security policy.

These include:

- Information Security Context, Requirements and Scope
- Information Security Roles, Responsibilities and Authorities
- Information Security Monitoring, Measurement, Analysis and Evaluation

# 4 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.

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 organisation'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 organisation.

Risk reduction – the degree to which known risks are treated to within acceptable limits.

Cost – financial resources required to maintain and improve the ISMS.

Other – appropriate objectives that do not fall into any of the above areas.

In discussion with the management team and based upon documented requirements, FISCAL technologies have 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 monthly, quarterly, and regular management reviews of the ISMS.

| REF | AREA | OBJECTIVE | MEASUREMENT METHOD | TARGET | TIMESCALE | OBJECTIVE OWNER |
|---|---|---|---|---|---|---|
| 1. | Quality & Information Security | Improve Security Controls in place inline with current recommended practices | Percentage of controls in place | 60% | June 2023 | IT Director |
| 2. | Quality & Information Security | All business continuity plans have been tested with the last 1 year. | Percentage of plans tested within 1year | 90% | Nov 2023 | IT Director |
| 3. | Capability | Training in information security has been provided for all key resources | Number of people trained with allocated training resources | 95% | Nov 2023 | IT Director |
| 4. | Risk reduction | Reduce number of high priority risks on risk register | Percentage reduction | 15% | June 2023 | IT Director & COO |
| 5. | Risk Reduction | Improvement of Supplier Management | All Suppliers Reviewed for Risk and documented | 95% | Nov 2023 | COO |
| 6. | Other | All servers have anti-virus installed and up to date patch management | Percentage of servers with anti-virus and up to date with patches | 100% | Nov 2023 | IT Director |
| 7. | Other | All End User Computers are managed and have security protections, policies and patch managed up to date | Percentage of EUC in Intune, Compliant, anti-virus configured and up to date with patches | 100% | Nov 2023 | IT Director |
| 8. | Other | Provide Internal Support in line with support SLA's | Helpdesk Support SLA Success per month | 90% | Nov 2023 | IT Director |

*Table 1: Information security objectives*

# 5 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 FISCAL technologies remain 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, the 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 | Improve Security Controls in place in line with current recommended practices | List controls.<br>Select controls for improvement.<br>Implement improvement to controls.<br>Verify controls. | Specialist IT team<br><br>Internal audit | IT Director | 12 months | List of signed off controls |
| 2 | All business continuity plans have been tested with the last 1 year | Agree on the testing schedule.<br>Conduct tests.<br>Produce test reports | Operational staff time | IT Director<br><br>Senior Developer | 12 months | Disaster Recovery test reports |
| 3 | Training in information security has been provided for all key resources | Identify key resources.<br><br>Identify courses.<br><br>Attend courses.<br><br>Complete training records | Training platform<br><br>Time of attendees | IT Director | 12 months | Training records |
| 4 | Reduce number of high priority risks on risk register | Hold workshops to identify ideas.<br>Implement ideas.<br>Reassess risks. | Risk owners<br>IT team | Chief Operations Officer / IT Director | 12 months | Completed Risk Reviews |
| 5 | Improvement of Supplier Management | Agree allocation with top management.<br>Plan involvement<br>Conduct supplier reviews.<br>Record findings | Asset owners<br>IT team | Chief Operations Officer | 12 months | Completed supplier management documentation. |
| 6 | All servers have anti-virus installed and up to date | Identify servers without AV and incomplete patching. | IT team | IT Director | 12 months | Monthly Report |

| | | | | | | |
|---|---|---|---|---|---|---|
| | patch management | Apply AV / Patching | | | | |
| 7 | All End User Computers are managed and have security protections, policies and patch managed up to date | Identify unmanaged EUC devices without AV and / or incomplete patching. Apply Management / AV / Patching. | IT team | IT Director | 12 months | Monthly Report |
| 8. | Provide Internal Support in line with support SLA's | Manage Support incidents. Monitor and report on successful SLA completion | IT Team | IT Director | 12 months | Monthly Report |

*Table 2: Plan to achieve objectives.*

# 6 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.

## 6.1 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 Steering Group | 1 day per quarter for each member | Assuming quarterly meetings |
| IT Director | Half Time Equivalent | Assumed to be a half-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 | 1 additional resource | Information security is already part of relevant roles |
| IT Users | 1 day per annum | Attendance at awareness events |
| Development Users | 5 days per annum | Depending on testing requirements for DR testing. |

*Table 3: Human resources required to run the ISMS.*

## 6.2 TECHNICAL RESOURCES

- Hardware:
    - Laptops, tablets or mobile devices for employees.
    - Servers for storing and processing data.
    - Firewall devices for network security.
    - Backup servers and storage devices for disaster recovery
- Software:
    - Antivirus and anti-malware software for protecting against security threats.
    - Data encryption software to ensure confidentiality of sensitive data.
    - Authentication and access control software to manage user access and permissions.
    - Intrusion detection and prevention software to monitor network activity and prevent attacks.
    - Vulnerability Management software to actively monitor vulnerabilities.
- Cloud Resources:
    - Cloud storage for backup and disaster recovery purposes
    - Cloud-based security services for network security
    - Cloud-based collaboration and communication tools for remote working
- Networking Equipment:
    - Switches, routers, and firewalls for network connectivity
    - Network monitoring and analysis tools to detect and prevent network attacks.

These are just some of the technical resources that may be needed to run the ISMS effectively and is not limited to these resources.

## 6.3 INFORMATION RESOURCES

Reports from existing systems:

- Access logs from servers and network devices to monitor user activity and detect potential security breaches.
- Incident reports from the helpdesk and IT staff to track and investigate security incidents.
- Vulnerability assessment reports from automated tools or external auditors to identify potential weaknesses in systems and applications.
- Patch and software update reports to ensure that systems are up-to-date and protected against known vulnerabilities.

External sources:

- Subscriptions to relevant organisations or security news feed to stay up to date with the latest threats and vulnerabilities
- External threat intelligence services to provide early warning of potential security threats.
- Access to industry-specific regulatory guidance and standards to ensure compliance with relevant regulations and requirements.
- Legal advice and support to ensure that the organisation is aware of legal obligations and liabilities related to data protection and security.

## 6.4 FINANCIAL RESOURCES

Capital expenses:

- Upgrading hardware and software to support the implementation of security controls and procedures.
- Investing in specialised security tools and technologies, such as firewalls, intrusion detection systems, and vulnerability scanners.

Revenue expenses:

- Hiring additional IT and security personnel to manage and maintain the ISMS.
- Ongoing training and development for staff to ensure they have the necessary skills and knowledge to implement security controls and procedures effectively.
- Conducting regular security audits and assessments to identify vulnerabilities and weaknesses in the ISMS.
- Maintaining and renewing subscriptions to external security services or software.

Timing and budget:

- The budget for financial resources will depend on the organisation's specific needs and circumstances. However, it is important to allocate sufficient resources to support the ISMS effectively.
- Capital expenses may be required at the start of the implementation phase, while revenue expenses will be ongoing.
- Regular reviews of the budget and spending will be necessary to ensure that the ISMS remains effective and up to date.

# 7 CONCLUSION

The objectives set for the period under consideration are intended to be challenging but achievable and will go a long way to protecting the organisation 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 FISCAL technologies help to ensure that we have in place an effective mechanism for managing information security in the longer term.