ISMS guidelines

Final editing review date	11/01/2023
Author	Riccardo Poffo <poffo@mobisec.com>
Distribution list	Free
Version	1.4
Status	FINAL
Validity	Public

Summary

1. Overview

Nowadays in modern companies, most of the data are stored in IT systems. ISMS is necessary to standardize the data management in the company, identify the correct stakeholders in case of problem or necessity and guarantee the security of the information stored.

Mobisec is an IT company specialized in classic and mobile cybersecurity: the correct management and the confidentiality of the information stored in its systems is fundamental to grant the secretness of the data to prevent an unwanted access could lead to an attack to Mobisec's clients.

Despite Mobisec is trying to apply ISMS standards and concepts to every area of the company, it is focusing on particular areas of the business to define through ISO 27001 certification the high quality and validity of the company management and processes. These areas are the following:

- **Mobisec DSA**: a proprietary software developed and managed completely internally by the company and reselled to the clients as PaaS within a dedicated department of the company.
- **Web Application Penetration Testing**: the execution of a standard OWASP list of tests called WSTG to evaluate the actual security of a web application.

2. Purpose

The main purpose of setting the ISMS scope is to define which information you intend to protect. It doesn't matter whether this information is stored or is accessed. The point is that the company and its employees will be responsible for protecting this information no matter where, how, and by whom this information is accessed (or tried to be accessed).

So, for example, if you have laptops that your employees carry out of your office, this doesn't mean these laptops are outside of the scope – they should be included in the policies if through these laptops the employees can access company local network and all the sensitive information and services located there.

ISMS is also the base for ISO 27001 standards, to ensure that the services offered by Mobisec are always of a high quality and the company can provide them at their best, lowering the weight of a single employee skills (*human factor*).

3. Scope

The scope of the ISMS covers all the data managed in IT systems by any Mobisec employee or external collaborator.

ISMS covers all the internal and external needs of the company security, declining details and extra-policies on client needs when needed.

At least once a year, possibly two times, or in case of major changes in the company, all ISMS documents are checked, updated, evaluated, and – if needed – presented to Mobisec board.

The official field of application of ISO 27001 certification is the following:

> *Secure development of Mobisec DSA software for performing penetration tests on Android and iOS mobile applications.*
>
> *Provision of VA/PT cybersecurity services on Android and iOS mobile applications using the Mobisec DSA platform, and on web portals according to OWASP WSTG standard.*

4. Availability

ISMS documentation is always available to Mobisec employees on company's shared fileserver.

Master copies are stored and managed in Microsoft Sharepoint to ensure easier collaboration and ease of access to external auditors and collaborators.

5. Validity and update

The latest version of the documents is intended as the valid one. Updates usually happens during yearly checks, but they can be scheduled upon need, if a better policy is individuated or an active one is found lacking of details or use cases.

6. Risk assessment and acceptance

The risk definition is based on the CIA standard, that takes in consideration the three main pillars of the information in IT field:

- **Confidentiality** is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

- **Availability** means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

If a risk is detected, it must be evaluated using the standards available in the file "Information Asset Registry and ISMS roles and procedures".

In case of high impact, high risk, or need to provide externally to the company the result, InfoSec team should use ENISA standards to define the risk and the impact of the threat in order to ensure every detail is managed properly and the information are available at their best (https://www.enisa.europa.eu/risk-level-tool/risk).

ISMS stakeholder is required to perform an evaluation of the result and schedule a meeting with the reporter and the colleagues that better can help individuate, evaluate and find a solution to the problem.

The risk can then be managed or accepted, in the latter case it must be tracked down and the board updated about the decision.

7. Commitment to meet expectations and requirements

The commitment of the Board and of all those who are involved in the activities of the management system for various reasons is to ensure the quality and security of the company's own data, of its employees, customers, and all the external agencies and companies involved in the very existence of Mobisec. In addition to this, the company is committed to complying with all the requirements of the International Standard ISO 27001:2017 for its activities that are in scope of the certification.

For this reason, the Board undertakes to exercise leadership, directly or delegated, according to the provisions of the ISO 27001 set of rules.

8. Commitment to continuous improvement

The client's information assets and that relating to the know-how of our organization will henceforth constitute the focal points of everyone's commitment.

This commitment will be manifested through continuous "security performances" checks capable of showing how effective the organization and the ISMS are in recording continuous improvement.

9. Definition and Terms

Acronym	Description
ISMS	Information Security Management System

DSA	Mobisec's Dynamic Security Analysis software
PaaS	Product as a Service
VA/PT	Vulnerability Assessment & Penetration Testing
WAPT	Web Application Penetration Testing
OWASP	Open Web Application Security Project – See link
WSTG	Web Security Testing Guide – See link

10. Revision History

Date of Change	Responsible	Summary of Change
Jan 2023	Riccardo Poffo	Update scope as in ISO 27001 official certification documents
Dec 2022	Riccardo Poffo	Declaration of ISO 27001 scope, document improvement
Jul 2022	Riccardo Poffo	Company overview, path updates, declaration of will of improvement.
Jan 2022	Riccardo Poffo	Release of the ISMS scope and guidelines as a document.