LAMBERT

MÉDICO FACTURES

Policy
Information security

Table of contents

1 PREAMBLE

In order to conduct its business, Lambert Médico Factures (hereafter "LMF") generates, stores, processes and communicates information in many forms. It recognizes that these information assets, which are essential to its business, must be evaluated, used appropriately and protected adequately throughout their life cycle. To this end, it is necessary to implement a coherent set of security measures determined by a best-practice security risk management approach, in compliance with legislative and regulatory requirements.

The information assets covered by this Information Asset Security Policy include not only information, but also equipment and media (paper or digital). They include data, documents, internal communication links, hosting sites, information technology (IT) and mobile and other portable equipment.

The policy represents an objective to be achieved by LMF within 3 years of its adoption.

2 INTRODUCTION

2.1 DEFINITIONS

Definitions of the various terms used in this policy and other related documents are available in the information security glossary.

2.2 LENS S

This document constitutes LMF's *Information Asset Security Policy* (hereinafter the "Policy"), which establishes the practices to be adopted to comply with various legal and administrative obligations and to protect all information assets and prevent potential security incidents, including fraud, information leaks, computer attacks, accidental errors, deliberate actions and privacy breaches. In this way, LMF protects its assets and mitigates the risks associated with the confidentiality, integrity and availability of information.

2.3 RANGE

This policy applies to all information assets held by LMF, including information collected in the course of contractual, regulatory and legal activities.

Without limiting the foregoing, for the purposes of this policy, LMF's employees, directors, subcontractors, suppliers and partners shall be considered LMF's stakeholders.

2.4 COMMITMENT

The present Policy is part of a context of prevention and information security awareness. To achieve this, the collaboration of all stakeholders is essential. Lambert Médico Factures undertakes to take all necessary steps to support the actions that need to be taken to implement the Policy, as well as the associated frameworks.

2.5 OWNER OF THE SUPPORTING SECURITY POLICY AND FRAMEWORK

This policy and the various associated security frameworks are the responsibility of the Information Security Manager. The Information Security Manager is responsible for its maintenance, revision and communication.

2.6 MONITORING AND CONTROL OF INFORMATION SECURITY ACTIVITIES

In order to monitor its risk exposure, LMF must have a monitoring infrastructure and processes in place. This must enable us to monitor the effectiveness of our methods, processes and protection mechanisms on an ongoing basis, and to improve them as the risks we face evolve.

LMF reserves the right, without notice, to monitor any information assets and any information held, processed and executed on its systems and mobile devices. This privilege must always be exercised in compliance with the law and when reasonable grounds recommend it.

2.7 CONSEQUENCES

Failure to comply with this policy or the associated security frameworks may result in LMF withdrawing access rights, terminating employment or contract, as well as applying disciplinary or legal measures. Any stakeholder who becomes aware of non-compliance with or omission from this policy must inform his or her manager or the Information Security Officer.

2.8 POLICY COMPLIANCE

The frameworks must be applied in support of LMF's business needs and must never become a constraint that does not add value or that prevents LMF from offering its services to its customers.

In view of the above, it is possible that, in the normal course of operations, specific situations may make it impossible to comply with certain information security requirements. In such a context, a clear procedure for managing non-compliance with security requirements is necessary to ensure that they are properly analyzed, approved and followed up.

3 GENERAL PRINCIPLES

3.1 INTERNAL ORGANIZATION

To ensure effective information security management within LMF, it is important to define the structure supporting the planning, development, implementation and control of security measures. The Management Committee is responsible for ensuring that this organizational structure is defined and implemented.

3.2 ASSESSING AND MANAGING RISKS RELATED TO INFORMATION ASSETS

In addition to corporate risk management, security measures are based on LMF's assessment, periodic analysis and treatment of risks to the confidentiality, integrity and availability of information.

A risk assessment must be carried out before acquiring new systems or making any changes that could have an impact on the security of LMF's information assets. In all cases, this assessment must be documented following a defined process.

3.3 HUMAN RESOURCES SECURITY

LMF shall establish human resources security processes to reduce the risk of human error, theft, fraud or misuse of LMF's information assets prior to hiring, during employment and after an employee's departure.

3.4 INFORMATION ASSET MANAGEMENT

In order to establish and maintain appropriate protection, each information asset must be inventoried and assigned to an owner who is aware of its value and importance to LMF. The owner will establish its classification according to its value and importance to LMF in order to establish an appropriate level of protection.

3.5 ACCESS CONTROL TO INFORMATION ASSETS

3.5.1 "NEED-TO-KNOW" PRINCIPLE

Information may only be disclosed to those persons who require such information in the course of their duties and in accordance with legal and regulatory obligations.

3.5.2 ACCESS MANAGEMENT

Access management must be carried out according to formal, agreed processes and procedures that are communicated to the people concerned.

When a user moves to a new position (e.g. redundancy, transfer, promotion or long-term leave), their manager must review their access.

Owners, in collaboration with the information security manager, must ensure that a periodic review of user accounts is carried out.

3.5.3 ACCESS CONTROLS

Any information asset that holds information not classified as public must have an active authentication mechanism to ensure that this information is not improperly disclosed, modified, deleted or made unavailable.

Users must have a unique identifier and must not share it under any circumstances.

3.6 PHYSICAL AND ENVIRONMENTAL SAFETY

All information assets must be protected by physical security measures according to their level of security, the associated risks and their value to LMF.

Access to offices and computer rooms containing information not classified as public must be physically restricted by an appropriate security mechanism.

3.7 IT AND TELECOMMUNICATIONS OPERATIONS MANAGEMENT

Unless designated as "public", all information must be protected from unauthorized disclosure to third parties. Third parties may have access to information not classified as public only if a need has been demonstrated and if such disclosure has been authorized by the owner or by law.

3.8 SYSTEMS ACQUISITION, DEVELOPMENT AND UPDATING

The security requirements to be met when acquiring, developing, implementing and maintaining an information asset must be determined. Security requirements must take account of technological developments and new security challenges.

3.9 INCIDENT MANAGEMENT

LMF *must establish and define the responsibilities and procedures to be implemented in the event of a security incident in order to guarantee an effective and relevant response, while ensuring that a team is in place to deal with incidents.*

3.10 DISASTER RECOVERY

LMF must implement an information technology recovery plan (hereinafter, "disaster recovery plan") designed to reduce the impact of the unavailability of an information asset and thus ensure the resumption of operations as quickly as possible. Recovery measures must be periodically verified to ensure their effectiveness and relevance.

3.11 TRAINING AND AWARENESS-RAISING

LMF must inform employees of the threats and consequences of a security breach so that everyone can recognize risky situations and act accordingly.

LMF must also provide specialized training in areas related to information security in order to maintain an acceptable level of risk within LMF.

An information security training and awareness program tailored to the different roles of employees must be defined.

It is LMF's responsibility to provide any person requiring access to information assets with the guidance necessary to understand their information security responsibilities.

All relevant documents must be communicated to employees, including this policy and associated guidelines.

4 R OLES AND RESPONSIBILITIES

4.1 EXECUTIVE COMMITTEE

The LMF Management Committee is responsible for ensuring that adequate safety frameworks are developed and maintained within LMF. The committee is responsible for approving this policy and taking all necessary steps to implement it and any other associated documents.

4.2 INFORMATION SECURITY MANAGER

The Information Security Manager is LMF's principal representative for all matters relating to the security of information assets.

Without limiting the generality of the foregoing, the Information Security Officer shall, among other things:

- Report annually to the Executive Committee on compliance with the policy and submit a compliance report.
- Keep the Policy up to date with LMF's needs, obligations and concerns.
- Ensure the involvement of the various stakeholders in the development of this Policy and other associated frameworks.
- Define security criteria for the technologies used within LMF.
- Provide advice on information security.
- Carry out risk and vulnerability assessments for all projects involving information assets, enabling us to define security requirements to ensure the protection of information assets.
- Make all users aware of information security.
- Ensure effective management of security incidents and maintenance of the disaster recovery plan (DRP) based on the business continuity plan (BCP).

4.3 INFORMATION ASSET OWNER

The Information Asset Owner is the person in charge of an LMF business area. He/she is responsible, from a business point of view, for the information assets that are necessary for the conduct of his/her department's activities, such as :

- Determine the value of its information assets for management purposes, and classify them accordingly.
- Identify and ensure the implementation of security measures and controls to guarantee the protection of information assets according to the assigned security level and risk assessments.
- Maintain safety measures for all our assets throughout their lifecycle (creation, maintenance, conservation, destruction, etc.).
- Approve the allocation of access rights to information assets under its responsibility, as required.

- Ensure that a disaster recovery plan, specific to its information assets, is in place and tested regularly.

4.4 USER OF AN INFORMATION ASSET

The user of an information asset (hereinafter: "user") is a person to whom an owner has granted access to one or more LMF information assets. A User may be a permanent or temporary employee, an administrator, a freelancer, a consultant or a third party.

Where justified by the value of the information asset, special arrangements with a third party (such as confidentiality agreements) must have been made prior to the award or assignment of the contract.

His role includes the following tasks:

- *Use information assets only for purposes expressly approved by the owner.*
- *Observe all safety precautions.*
- *Refrain from disclosing information in their possession (unless it has been designated as public) without prior authorization from the owner.*
- *Inform the Information Security Officer of all situations where you believe the security of an information asset is vulnerable or has been compromised.*
- *Comply with this policy and any other document that refers to or supports it.*

5 REVISION AND APPROVAL

This Policy comes into effect upon adoption by the Executive Committee and may be revised at any time by the Privacy Officer.

Changes may be proposed by various LMF stakeholders, which must be submitted in writing to the Information Security Manager.

This Policy should be reviewed at least every two years to ensure that it remains relevant to LMF's mission, the activities of its users and any substantial changes in legislation or regulatory requirements.

6 EFFECTIVE DATE

This Policy takes effect on July 1er 2023. It cancels and replaces all previous guidelines on this subject.