Information Security Policy 🇬🇧

1. Statement

As of 25 May 2018, the Personal Data Protection Act will be replaced by the General Data Protection Regulation (GDPR). In addition, the Netherlands Authority for the Financial Markets published the Principles for Information Security on 19 December 2019.

The information below follows the requirements that GDPR imposes on a financial service provider in compliance with the Netherlands Authority for the Financial Markets Principles for Information Security.

2. Introduction

Managing information security risks is becoming increasingly important. This is due to the increasing digitization of companies and the increasing threat of cybercrime.

Information security is important for both LMIS and its customers. After all, customers must be able to rely on the services provided. In addition, companies must treat their data with integrity and confidentiality. The legislator and the Netherlands Authority for the Financial Markets therefore expect companies to handle information security risks with care.

LMIS has taken appropriate measures to ensure the continuity and reliability of information technology, information received and with regard to the provision of information, as well as limiting the impact of any information security incidents to an acceptable level.

3. The 11 AFM Principles

The AFM published on 19 December 2019 11 principles for information security to provide guidance to financial undertakings. With this policy statement, the AFM outlines its expectations about the desired behaviour of financial undertakings in the field of information security. These 11 principles are now final. The principles offer tools to financial companies that contribute to the development of the sector. The principles do not replace legal GDPR requirements.

The eleven principles are:

I. Ensure an up-to-date information security policy

An up-to-date information security policy describes a coherent set of measures, procedures and processes with which information security risks are managed.

In this information security policy, LMIS sets out its objectives for information security and the way in which these objectives are achieved. LMIS considers cyber security to be an integral part of information security. The information security policy applies to the IT resources and processes under management, personal data carriers, digital products of the organization and IT resources and processes that have been outsourced.

This information security policy is kept up-to-date due to threats and risks are periodically evaluated. In the event of new risks, additional evaluations will take place.

II. Set up the governance structure in

LMIS establishes a governance structure that enables effective information security. The board of LMIS Global (Europe) B.V. is responsible for information security. The board is aware of the most important information security risks, threats and incidents.

If parts of LMIS do not comply with the information security policy, additional measures will be taken, or the risks of non-compliance will be accepted after careful consideration. The implementation of the organizational structure for information security is proportionate to the business model of LMIS, the size and complexity, the characteristics of the information and data created or processed and the related information security risks.

A clear division of tasks and the availability of sufficient expertise and experience are crucial for the quality of risk assessments and the effectiveness of information security measures. The roles and responsibilities in organizing, managing and controlling information security are therefore clearly assigned. LMIS has sufficient capacity, knowledge and experience in the field of information security to fulfil these roles and responsibilities.

III. Identify threats and assess risks

Information security is designed based on an up-to-date understanding of existing threats and risks, the potential impact of existing threats on LMIS and the risk appetite of the company.

Information security is designed based on an up-to-date understanding of existing threats and risks, the potential impact of existing threats on LMIS and the company's risk appetite.

When implementing the information security policy, measures are taken based on a good understanding of existing threats and risks according to principles 4 to 8.

Information security is dynamic. Technology and threat factors are constantly evolving. This creates new risks. LMIS therefore periodically updates its risk assessment based on an up-to-date insight into information security threats that are relevant to the company.

One way to gain insight into existing risks is to test the effectiveness of the risk management measures based on known threats. Both internal and external sources can provide added value in determining these threats.

The frequency and depth of the risk assessment shall be proportionate to the business operations, size and complexity, and characteristics of the information and data created or processed. In its risk assessment, LMIS takes into account both its own interests and those of stakeholders, such as customers and business partners in the sector in which it operates.

IV. Recognize the importance of people and culture

LMIS recognizes the risk of human action for information security and creates and supports a culture in which employees are aware of the risk of information security incidents and communicate openly about them. People are an important link in information security.

Irresponsible or unthinking behavior can lead to information security incidents. This is recognized and mitigated by LMIS through effective measures. LMIS uses processes in such a way that people effectively contribute to adequate information security and to properly handle incident reports from employees.

In addition, LMIS implements measures such as awareness programmes and training courses. The effectiveness of these measures is periodically tested in combination with other information security measures.

LMIS recognizes the risks that human activity entails for the effectiveness of the information security policy and takes appropriate measures to limit these risks. Such risks include risks that can be attributed to internal factors (internal fraud, for example) and that are attributable to external factors (such as phishing via email). To mitigate these risks, companies can take technological, procedural, and physical measures that support employees in fulfilling their information security responsibilities. Any residual risks have been weighed against the costs and impact of intended additional measures they mitigate.

The management of LMIS promotes the importance of information security, making employees aware of existing threats. All employees are actively made aware of their responsibilities in the field of information security and are trained accordingly.

V. Secure technology

In the implementation and maintenance of systems, the principle of 'secure by design' is applied.

LMIS uses technology standards to embed information security in the design of IT architecture and systems. LMIS recognizes the risks associated with the use of new and outdated technology and has taken measures to mitigate these risks. Changes in the IT infrastructure have been implemented in such a way that information risks are reduced to an acceptable level in accordance with policy and risk appetite.

VI. Set up processes well

The design of business processes guarantees the availability, integrity and confidentiality of processes and the systems used in them.

All processes of LMIS are designed in such a way that they contain safeguards to guarantee their confidentiality, integrity and availability. Processes and systems (and processed data) are in line with the policy and risk appetite of LMIS. Information security is an integral part of administrative organization and internal control. The effectiveness of the measures is periodically tested in combination with the other information security measures.

VII. Ensure physical security

The design and layout of the company's facilities and equipment is in line with information security requirements.

LMIS has taken physical measures to supplement technical and procedural measures. Measures, such as restrictions on access to facilities and equipment. Physical measures have been taken to protect facilities and equipment. An analysis of the risks of external factors (such as the likelihood of natural disasters), human factors (e.g., unauthorized access) and crisis situations (such as a power failure) is part of these measures.

The information security risks of facilities and equipment are mitigated in accordance with the information security policy. The effectiveness of this is periodically tested in accordance with the inherent risk of the facility and/or equipment and in combination with the other information security measures.

VIII. Secure the data

Throughout the entire lifecycle of data and information, measures have been taken to meet the relevant security requirements.

These measures relate to the storage, use and transport of data through communication channels. The effectiveness of these measures is periodically tested in collaboration with other information security measures taken by LMIS.

LMIS takes into account the integrity and availability of data. This also applies to system conversions and data migrations, so that historical data and the relationship between data elements remains available in accordance with the requirements arising from the legislation and the objectives arising from this information security policy.

IX. Ensure effective incident response and recovery

LMIS is prepared for information security incidents to limit their impact on the company's business operations. We have an effective information security management system based on the fundamental pillars of people, processes, and technology. When an information security incident occurs, the company shall take timely and effective response and remedial action.

LMIS will implement processes and plans that are triggered when an information security incident is detected. These future processes and plans include minimal measures to (1) stop the incident, (2) limit the negative impact, (3) repair the damage, and (4) communicate effectively with stakeholders.
Assessments are carried out during and after the recovery activities. The insights gained are incorporated into the information security policy, existing processes and systems and the communication to and training of employees.

X. Also take your responsibility when outsourcing

LMIS is responsible for the information security of outsourced processes and systems. LMIS remains responsible for the information security of processes and systems outsourced to another company in the same group or to an external party. Prior to outsourcing IT infrastructure and/or processes, LMIS conducts a thorough investigation into the information security of the supplier, in which the scope and depth of the research are aligned with the risks to the information security of LMIS.

The firm is aware of the implications of outsourcing for the relevant international distribution of roles and responsibilities, as well as for risk management and chain integration. The analysis of these risk factors is regularly updated by LMIS.

LMIS makes clear legally binding agreements about the cooperation and division of tasks in the field of information security. This also concerns the right to carry out audits at the supplier.

XI. Chain perspective

LMIS applies an integrated chain approach in determining information security risks and the necessary control measures. Through this approach, LMIS is aware of the dependence of chain parties in safeguarding information security of its own IT environment. The chain consists of various links of internal and external parties, including customers and supervisory authorities.

LMIS applies an integrated chain approach where it takes into account its position in the chain and its dependencies on other parties in the chain. As a starting point, LMIS assumes that other companies in the same sector and within the same chain are coalition members in protecting the sector against external information security risks. Weaknesses of a party in the chain can have consequences for other parties in the same chain.