ISO / IEC 27001: 2022 Information Security Policy

Primeur Group

Version 2.0

Approved by the Managing Director of Primeur Suisse SA

• 2ndt Edition December 2024

The companies of the Primeur Group (subject to the management and coordination of Topicus.com Cooperatief U.A.-NL., hereinafter also referred to as "PRIMEUR") offer *data integration platforms and solutions* to their customers and, therefore, the objective of information security is primary. The purpose of this document is to describe the general principles of information security that the company has adopted in order to create and maintain an efficient Information Security Management System (ISMS).

Information security has as its primary objective the promotion of a corporate culture that protects the protection of data (digital and analogue), of company processes, procedures and *policies* and, in general, of all the related components of the organization.

In particular, pursuing information security means defining, achieving and maintaining the following objectives:

- **Confidentiality** : ensure that information is accessible only to duly authorized subjects and / or processes;
- **Integrity** : safeguarding the consistency of information from unauthorized changes;
- **Availability** : ensure that authorized users have access to information and associated architectural elements when they request it;

The lack of adequate levels of safety can entail, in the context of any company activity, consequences both in terms of personnel responsibility (violation of company regulations) and from the company point of view (risk of economic / financial damage, lack of customer satisfaction, damage to the corporate image as well as to incur significant sanctions related to the violation of current regulations).

The adoption of adequate levels of information security is therefore a fundamental requirement to guarantee the reliability of the information processed, as well as the effectiveness and efficiency of the services provided by PRIMEUR; consequently, it is essential to identify security needs through the following activities:

- risk analysis and treatment, which allow the company to acquire awareness and visibility on the level of risk exposure of its organization;
- application of related internal *policies and procedures;*

- application of mandatory, voluntary legislation and contractual clauses on information security.

ORGANIZATIONAL PERIMETER

This Policy, approved by the Managing Director of Primeur Suisse SA, the Primeur Group holding company (under the management and coordination of Topicus.com Cooperatief U.A.-NL.), is aimed at all employees and collaborators of PRIMEUR, as well as all external interested parties involved in the management of the information handled by the companies of the Group.

IDENTIFICATION, CLASSIFICATION AND MANAGEMENT OF ASSETS

In order to ensure full knowledge of the information managed in PRIMEUR and the assessment of their criticality and in order to facilitate the implementation of adequate levels of protection, PRIMEUR undertakes to:

- survey and periodically update a list of all tangible and intangible assets to be protected (information, hardware, software, paper documents and storage media);
- associate each resource (tangible / intangible asset) with a specific manager;
- classify information according to its level of criticality, in order to manage it with consistent and appropriate levels of confidentiality and integrity. The criticality of the information must be assessed as objectively as possible, through the use of adequate working methods;
- define management methods and protection systems for the information and the *assets* on which they reside, consistent with the level of criticality identified.

SECURE ACCESS MANAGEMENT

In accordance with the "principle of least privileges" *(or " Least privilege "* or, again *" Zero trust security model ":* an entity should be granted only the privileges it needs to complete its work *)* , in order to ensure greater resilience in the field of security and secure access to information, in order to prevent unauthorized processing of the same or their vision by users who do not have the necessary rights, it is necessary to act in accordance with the following points:

- Access to information by each individual user must be limited to only the information they need for the performance of their duties. The communication and transmission of information internally, as well as externally, must be based on the same principle.
- Access to information in digital format by authorized users and systems must be subject to authorization and subsequently to the passing of an identification and authentication procedure.
- Authorizations for access to information must be differentiated on the basis of the role and positions held by individuals and must be periodically reviewed and managed through unique credentials;
- The systems and services used by PRIMEUR must be suitably protected, segregated and periodically checked, in order to minimize the possibility of unauthorized access.

RULES OF CONDUCT FOR THE SAFE MANAGEMENT OF COMPANY RESOURCES

In order to ensure that PRIMEUR employees and collaborators adopt behavior models aimed at guaranteeing adequate levels of information security:

- the work environments and company resources must be used in a manner consistent with the purposes for which they were made available and guaranteeing the security of the information processed;
- appropriate procedures are defined for the management and use of information, both digitally and on paper;
- the systems and services used must be used by employees and collaborators according to shared and approved procedures.

PERSONNEL AND SECURITY

In order to ensure that the personnel working on behalf of PRIMEUR (employees and collaborators) are fully aware of the issues relating to information security:

- during their stay in PRIMEUR, staff must receive adequate and periodic training on data security issues;

- *management* must ensure and verify that personnel have relevant knowledge of the security of the information and systems they develop or maintain . Personnel involved in the life cycle of information systems development must be aware of their responsibilities regarding system and information security.
- in the phases of selection and insertion of personnel in PRIMEUR, the levels of knowledge of company safety issues must be assessed according to the activities to be carried out;
- the safety measures relating to teleworking / agile / remote work and the use of portable devices and those relating to the optimization of the work area must be envisaged in a specific procedure;
- the procedures for closing the employment relationship with PRIMEUR must be consistent with the corporate safety objectives.

MANAGEMENT OF ANOMALY EVENTS AND ACCIDENTS

In order to ensure that anomalies and incidents that could have repercussions on the information system and on corporate security levels are promptly recognized and correctly managed through efficient prevention, communication and reaction systems in order to minimize the impact on the business, it is necessary that :

- all employees and collaborators are required to detect and notify, according to the procedures, any problems related to information security;
- accidents that may have an impact on safety levels must be detected and any damage, potential or otherwise , must be managed, where possible, in a short time according to specific procedures, also involving external suppliers and third parties.

PHYSICAL SECURITY MANAGEMENT

In order to prevent unauthorized access to offices and individual company premises and to guarantee adequate levels of security for the areas and assets through which the information is managed:

- the management of the safety of the areas and premises must be guaranteed through the definition of adequate levels of protection.
- the safety of the equipment must be guaranteed by:

- the definition of an adequate location for information processing equipment;
- the provision of the resources necessary for their operation;
- the provision of an adequate level of maintenance.

CONTRACTUAL ASPECTS RELATED TO INFORMATION SECURITY

In order to ensure compliance of contracts with third parties with the legal requirements and principles related to information security, in accordance with the specific characteristics of the relationship that PRIMEUR must establish with the third parties themselves:

- agreements with third parties (customers and suppliers) who access the information and / or the tools that process it, must be based on formal contracts containing appropriate security requirements that have been assessed as appropriate;
- agreements with third parties, where necessary, must guarantee compliance with the legal requirements in general and, specifically, with regard to the protection of personal data.

BUSINESS CONTINUITY MANAGEMENT

In order to guarantee the continuity of PRIMEUR's activity and the possible timely restoration of the services provided that may be affected by anomalous events of a certain gravity, reducing the consequences both inside and outside the company context:

- all the events that could lead to an interruption in the business continuity must be carefully identified and evaluated in terms of probability of occurrence and possible consequences;
- the timing of the restoration activities and the related costs and the most suitable methods to allow the organization to deal with the consequences of an unforeseen event in an organized and efficient way must be defined, in such a way as to allow the reduction of negative consequences about the company.

MONITORING, TRACKING AND TECHNICAL CHECKS

In order to ensure the timely detection of anomalous events, accidents and vulnerabilities of information systems, in order to ensure the security and availability of services and related information:

- the information systems must be periodically checked in order to assess the correct functioning of the security systems, *hardware* and *software* , implemented, as well as the possible presence of vulnerabilities not found or known in the past;
- in view of the results of all monitoring, tracing and verification activities, periodic analysis must be carried out, aimed at identifying critical areas and appropriate corrective and improvement actions;
- periodic *audit activities* of the information security management system must be planned.

LIFE CYCLE OF SYSTEMS AND SERVICES

In order to ensure that safety aspects are included in all phases of design, development, operation, maintenance, assistance and decommissioning of the organisation's systems and services:

- the guarantee and safety requirements must be respected at the beginning of each development project, to ensure that they are effective and that there are no negative repercussions on the project or product;
- the safety requirements are in no case considered separately from the functional requirements of the systems. To effectively consider security, it must be planned from the very beginning of the development and / or maintenance process to ensure that it fits into the context of the system.
- in the design and development phase the following issues must be managed:
    - inclusion of safety requirements in the functional specifications of services and systems;
    - adoption of *best practices* and recognized *standards for software* development and maintenance ;
    - management controlled of the documentation ;

- separation of development and test environments.
- service delivery phase, the following issues must be managed:
  - *capacity management* infrastructure technological ;
  - improvement of systems and data security (*configuration management* , installation of *anti-malware systems*);
  - management of the changes ;
  - adoption of *backup* and *restore procedures* ;
  - adoption of procedures for controlled decommissioning of systems;
  - systems and services monitoring;
  - management utilities ;
  - *performance monitoring* .

COMPLIANCE WITH THE APPLICABLE LAW

In order to ensure compliance with current legislation, contractual obligations and all information security requirements, minimizing the risk of legal or administrative sanctions, significant losses or reputational damage :

- all regulatory and contractual requirements regarding the organization's security and having an impact on the Information Security Management System must be identified and analyzed, in order to assess their impact on the organization and information systems;
- the managers of the various areas must ensure, each within their area of responsibility, that all policies, procedures, standards and in general all documentation relating to information security are applied, respected and verified;
- failure to comply with what is indicated in this document, and in all others deriving from it, will be managed in compliance with the provisions of the CCNL or, in the case of non-compliance by third parties, according to existing contractual relationships.

TEAM RESPONSIBLE FOR THE MANAGEMENT OF INFORMATION SECURITY

The Team responsible for the Information Security Management System, supported by the *management* , will have to act as promoter, in order to make this General Security

Policy consistent with the evolution of the company context, of any actions to be taken in response to the occurrence of events Which:

- new threats or changes to those considered in previous risk analysis activities;
- significant security incidents ; _
- evolution of the regulatory and legislative context on information security;
- results of analysis on the costs, impacts, effectiveness and efficiency of the Information Security Management System.

Mendrisio , December 23, 2024