ISO / IEC 27001: 2017 Information Security Policy

Primeur Group

Version 1.0

Approved by the General Director of Primeur Suisse SA

• 1st Edition September 2022: September 14th, 2022

The companies of Primeur Group (hereinafter also referred to as "PRIMEUR") offer *data integration* platforms and solutions to their customers and, therefore, information security is a primary goal. The purpose of this document is to describe the general principles of information security that the company has adopted to create and maintain an efficient Information Security Management System (ISMS).

The main goal of Information security is to foster a corporate culture that safeguards the protection of data (digital and analogic), of company processes, procedures and policies and, generally speaking, of all the related components of the organization.

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

- **Confidentiality**: ensure that information is available only to duly authorized subjects and/or processes.
- **Integrity**: safeguarding the reliability of information from unauthorized changes.
- **Availability**: ensure that authorized users have access to information and associated architectural elements when needed.

Lacking adequate levels of safety can entail, within the framework of any company activity, consequences both in terms of personnel responsibility (violation of company rules) and of corporate responsibility (risk of economic / financial damage, risk of lack of customer satisfaction, risk of damage to the corporate reputation as well as risk of incurring into significant sanctions related to the violation of applicable law).

The implementation of adequate levels of information security is therefore a fundamental requirement to guarantee the reliability of information processed, as well as the effectiveness and efficiency of the services provided by PRIMEUR. Therefore, 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 and voluntary rules and of contractual clauses on information security.

ORGANIZATIONAL PERIMETER

This Policy, approved by the General Director of Primeur Suisse SA (Primeur Group holding company), is aimed at all Primeur employees and personnel, as well as at all external interested parties which may be involved in the management of information handled by Group companies.

IDENTIFICATION, CLASSIFICATION AND MANAGEMENT OF ASSETS

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

- Assess and periodically update a list of all tangible and intangible assets to be secured (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, with 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 compliance with the "Principle of Least Privilege" (or "Zero trust security model" according to which an entity should be granted only the privileges it needs to get its work done), in order to ensure greater resilience in the security area and secure access to information, so as to prevent unauthorized processing of information or its viewing by users who do not have the necessary rights, the following points should be acted upon:

- Access to information by each individual user must be limited to only the information they need to carry out 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 must pass 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, to minimize the possibility of unauthorized access.

RULES OF CONDUCT TO SAFELY MANAGE COMPANY RESOURCES

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

- Work environments and corporate resources must be used in a way that is congruent with their intended purposes and ensuring 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.
- The 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 ANOMALIES AND INCIDENTS

In order to ensure that anomalies and incidents that may 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, the following applies:

- 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

To prevent unauthorized access to offices and individual company premises and to guarantee adequate levels of security for the areas and assets used to manage information:

- Security management of areas and premises must be ensured by defining appropriate levels of protection.
- Equipment security must be ensured by:
    - defining an appropriate location for information processing equipment.
    - making available the resources necessary for their operation.
    - arranging for an appropriate level of maintenance.

CONTRACTUAL ASPECTS RELATED TO INFORMATION SECURITY

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 such.
- agreements with third parties, where necessary, must guarantee compliance with the legal requirements in general and, specifically, with the protection of personal data.

BUSINESS CONTINUITY MANAGEMENT

To ensure the continuity of PRIMEUR's business and the possible timely restoration of the services provided (in case they are affected by abnormal events of a certain severity) and to reduce the consequences both within and outside the business environment:

- 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 restoration activities and their costs must be defined, as well as how best to enable the organization to address the consequences of an unforeseen event in an organized and efficient way, so that the negative consequences on the company can be reduced.

MONITORING, TRACKING AND TECHNICAL CHECKS

To ensure the timely detection of anomalous events, incidents and vulnerabilities of information systems so that the security and availability of services and related information can be ensured:

- the information systems must be periodically checked 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;
- the results of all monitoring, tracing and verification activities must be periodically analyzed to identify 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 organization'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;
    - controlled management of the documentation;
    - separation of development and test environments.
- service delivery phase, the following issues must be managed:
    - capacity management of the technology infrastructure;
    - improvement of systems and data security (configuration management, installation of anti-malware systems);
    - change management;
    - adoption of backup and restore procedures;
    - adoption of procedures for controlled decommissioning of systems;
    - systems and services monitoring;
    - user profile management;
    - performance monitoring.

COMPLIANCE WITH THE APPLICABLE LAW

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 applicable national collective labor agreement or, in the case of non-compliance by third parties, according to existing contractual relationships.

TEAM RESPONSIBLE FOR THE MANAGEMENT OF INFORMATION SECURITY

In order to make this General Security Policy consistent with the changing business environment, the Team responsible for the Information Security Management System, supported by the Management, will have to promote any actions to be taken in response to events such as:

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

Mendrisio, September 14, 2022