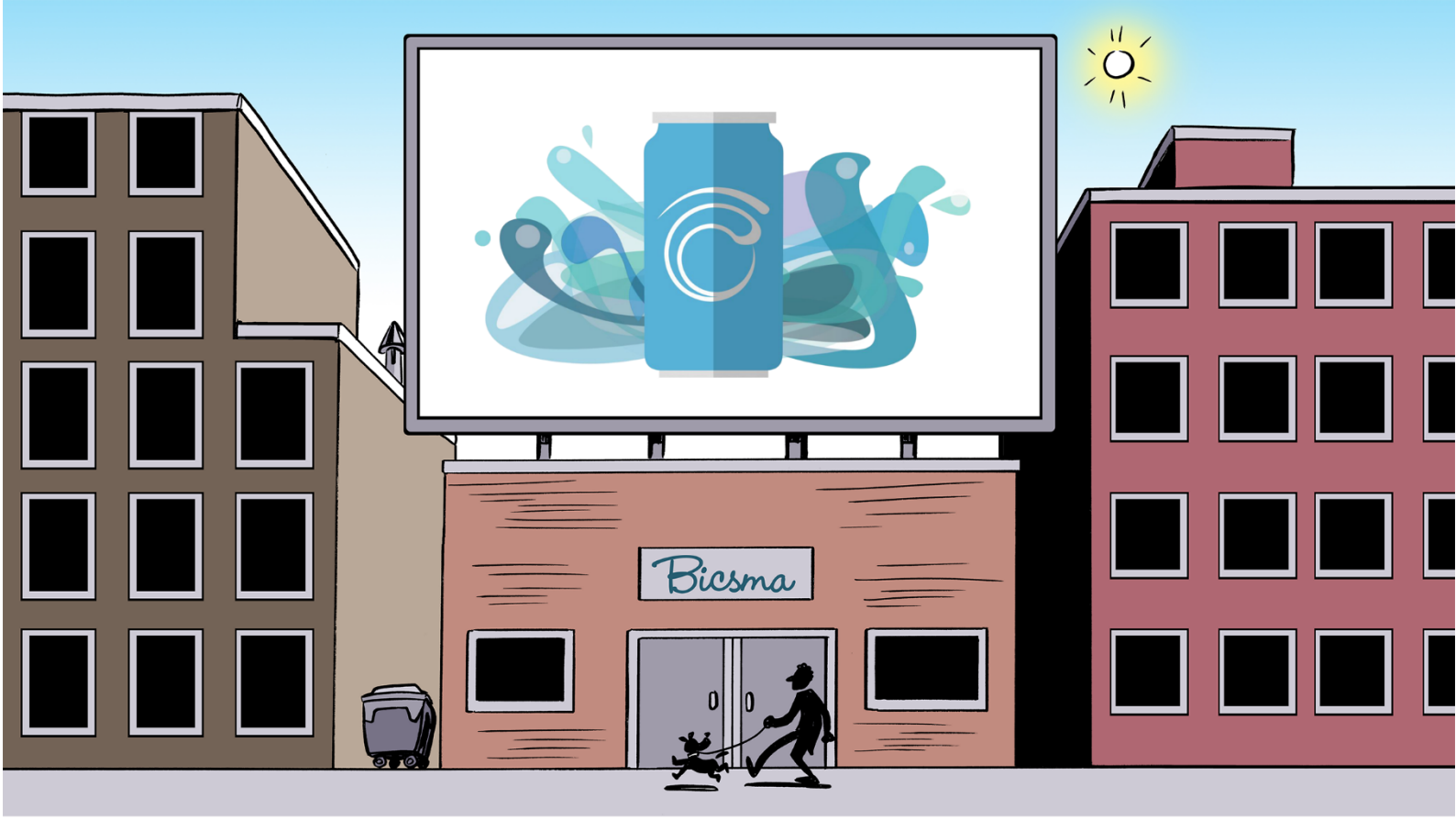


Bicsma

# BICSMA'S INFORMATION SECURITY POLICY

# Table of Contents

# 1. Document features

## 1.1 Custodian contact details

Name:
Location:
Telephone:
E-mail:
URL:

## 1.2 Reviews

Date of most recent review:

Date of next review:

| Date | Author | Version | Modifications |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## 1.3 Paragraph list

| Name | Function | Role | Date | Paragraph |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 1.4 Distribution list

| Name | Function | Role | Version | Medium/ format |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 2 Framework

## 2.1 Introduction

Bicsma BV recognises its responsibility for preserving the safety of processes, persons, resources and data within its sphere of influence. This strategic policy gives substance to that responsibility within the domain of information security.

## 2.2 Definitions

### 2.2.1 Information security

Information security is the establishment and maintenance of a coherent package of measures to guarantee the reliability of the information systems.

### 2.2.2 Reliability

Reliability is the extent to which the confidentiality, integrity and availability of the information systems is guaranteed.

### 2.2.3 Information systems

The entire range of equipment, software, data, procedures and people involved in the development, implementation and maintenance of Bicsma BV's information management.

### 2.2.4 Component of the information system

A part of the information system that can be regarded as a discrete unit from an organisational, procedural, functional, logical or physical viewpoint. Component may also refer to a composition of different underlying components.

### 2.2.5 The Bicsma BV domain

The physical and digital area in which Bicsma BV can exercise its influence. This mainly concerns the areas, buildings and IT networks managed by Bicsma BV, but also includes Bicsma domains on the internet. Home office environments fall within the Bicsma BV domain when used on behalf of Bicsma BV.

### 2.2.6 IT processes

Whether or not automated, processes that serve the development, implementation, maintenance and exploitation of the delivered IT products and services.

## 2.3 Scope

This information security policy is applicable to the computer network and the related IT processes. Interfaces with other networks, e.g. third-party networks or the internet, are also included in the scope to prevent third-party risks from affecting Bicsma BV's computer network. This does not alter the fact that third-party risks should also be addressed in their own environments. However, the way to address these risks falls beyond the scope of this document. Information stored in paper format only falls within the scope of this information security policy if relevant for guaranteeing the reliability of Bicsma BV's information systems.

## 2.4 Target group

The responsibility for preserving the security of information is shared by all Bicsma employees. Therefore, this information security policy applies to all employees of Bicsma BV and, in principle, to third parties, unless explicitly stated otherwise. Bicsma might draw up specific agreements as to how third parties should relate to this information security policy.

## 2.5 Roles and responsibilities

### 2.5.1 Management of the information security policy

The Information Security Manager acts on behalf of Bicsma BV as the owner of the information security process and is therefore responsible for managing the process. He/she is referred to as the process owner for information security. In order to ensure that this policy is up to date, a review shall take place every six months. Review are initiated by the process owner, or by a delegate of the process owner.

Developments in the environment, the business operations, the legal and regulatory requirements, the architecture, etc. might result in the need to adjust this policy. Minor adjustments can be made upon the process owner's approval. Major adjustments are submitted to the Management Team for approval before they are incorporated in the policy. Should the need arise, the process owner assesses whether the adjustment is a minor or a major one. In the event of a difference of opinion, the Management Team may be asked for advice.

### 2.5.2 Implementation of the information security policy

Every employee and partner of Bicsma BV should comply with this information security policy and the requirements resulting from this policy. The policy can only be effective if all processes, procedures and technological solutions are implemented in line with the policy and the requirements resulting from the policy. As regards processes, procedures and technological solutions in use, the process owner is accountable for complying with the information security policy. It should be pointed out that changes in the organisation might entail consequences for information security. In order to preserve control, a Change process is set up for relatively small adjustments, whereas a Project Management process is set up for relatively larger adjustments. Information security becomes an integral part of both the Change process and the Project Management process to ensure that all risks posed by any canges are properly addressed. The process owners of Change and Project Management are also obliged to comply with the information security policy.

### 2.5.3 Communication about the information security policy

The process owner informs Bicsma BV's employees of any adjustments made to this policy. The process owner ensures that everyone is aware of the current state of play in information security. Should the adjustments affect agreements made with third parties, the process owner informs the staff member(s) responsible for maintaining relationships with the third party or parties concerned, who then informs the third party or parties accordingly.

### 2.5.4 Enforcement of the information security policy

Responsibility for monitoring compliance, enforcement and reporting on the current status of information security is assigned to the staff members appointed by the process owner. The staff members in question ensure that the process owner has a proper insight into the compliance status. Should these staff members detect deviations, they shall act in accordance with the pre-established procedures and provide advice where necessary.

The continued effectiveness of the measures resulting from this information security policy is guaranteed by subjecting the policy to regular reviews. In the event that a component of the information system is adjusted or newly acquired, the review takes place as part of Change management. In addition, all measures are subjected to an annual Information Security Audit, using the Code of Practice for Information Security as a frame of reference. Where parts of the information systems are managed or used by third parties, Bicsma BV reserves the right to monitor third-party compliance with this policy and monitor the implementation of the associated security measures by performing Information Security Audits on the relevant sytems or domains of the third party in question. In the event that nonconformities are found among employees or third parties, sanctions might be imposed. In such cases, the process owner contacts the owner or owners of the affected component (s), the manager (s) of the offending employee (s) or the contract holder. The severity of the sanction should depend on the gravity of the violation and may result in contract termination and legal action.

# 3 Bicsma BV's information security policy

This information security policy is based on the legal and regulatory requirements applicable to Bicsma BV and the objectives set out in the Code of Practice for Information Security as described in ISO / IEC 27001 and 27002. These requirements translate into the policy statements included in the following paragraphs. As regards specific sub-areas, this strategic information security policy is further elaborated into issue-specific policies and guidelines. Issue-specific policies contain policy statements of a mandatory nature, whereas guidelines comprise recommendations.

## 3.1 Contractual security requirements

### Article 3.1.1

Agreeements for the delivery or purchase of services and products shall set out what information security requirements Bicsma BV's contracting partners are expected to meet. These agreements ensure that third party activities, products and services do not pose a threat to the reliability of Bicsma BV's information systems.

### Article 3.1.2

Employees of third parties performing work for BICSMA BV must comply with Bicsma BV's information security policy, including the resulting code of conduct.

### Article 3.1.3

Third parties shall openly and proactively inform Bicsma BV about developments in their environment if these developments are likely to affect the reliability of Bicsma BV's information systems.

## 3.2 Human resources security requirements

### Article 3.2.1

The human resources policy is also aimed at contributing to the reliability of the information systems. This is reflected, among other things, by a detailed description of information security-related duties and responsibilities, together with an indication of the required level of screening for each position.

### Article 3.2.2

New employees shall be screened. The level of screening depends on the classification of the processes and information new employees have access to and become involved in while performing their tasks.

**Article 3.2.3**
Employees are expected to take note of this information security policy and perform their tasks with due observance of the policy. Compliance with the information security policy plays an important part in the terms of employment. By signing an employment contract with Bicsma BV, employees automatically accept the provisions set out in the policy.

**Article 3.2.4**
All employees shall sign Bicsma BV's Code of conduct upon the start of employment. This condition also applies to contract staff or temporary employees.

**Article 3.2.5**
Employees who are likely to come into contact with sensitive information in the course of their work shall sign a confidentiality statement before gaining access to this information. The owner of the sensitive information is responsible for acquiring the employee's signature.

**Article 3.2.6**
The use of Bicsma BV's information systems is only permitted under the condition that it serves the interests of the business. This particularly applies to accessing and disseminating corporate information.

**Article 3.2.7**
Employees shall duly observe the "Clear Desk" and "Clear Screen" principle in performing their daily activities. Clear desk and clear screen significantly reduce the risk of unauthorised access to the information.

**Article 3.2.8**
In the event that an employee leaves the company, the employee's supervisor shall ensure that all access rights of the employee are revoked as set out in the relevant procedures. The supervisor also ensures that all assets that have been issued to the employee in support of his or her work are returned to the organisation. In the event that an employee's position changes, the supervisor ensures that similar measures are carried out. Access rights and assets that are no longer needed by the employee to carry out his or her duties should be revoked and returned.

## 3.3 Physical security requirements

**Article 3.3.1**
The physical and logical security of IT resources and the relevant spaces shall be arranged in such a way that preserves the reliability of the information systems.

**Article 3.3.2**
Insofar as this is possible within Bicsma BV's sphere of influence, data carriers and networks shall be physically protected against theft and unauthorised access.

**Article 3.3.3**
Data carriers that are no longer used or are no longer used for the same purpose as before will only be offered for reuse or destruction after it has been confirmed that they do not contain any confidential information. In doing so, account shall be taken of the risk entailed by so-called "data recovery" techniques.

## 3.4 Procedural security requirements

### Article 3.4.1
Information security forms an integral part of Bicsma BV's business processes. This implies that process owners are responsible for managing the risks arising from their process. Process owners shall minimise any potential adverse effects the risks originating from their process might have on the reliability of the information systems.

### Article 3.4.2
Security measures always have an owner. This owner is responsible for the implementation, documentation and monitoring of the relevant security measure (s), as well as issuing the relevant reports.

### Article 3.4.3
Every component of the information assets has an owner. The owner is responsible for ensuring that the relevant component makes a positive contribution to the reliability of the information systems. To that end, the owner shall ensure the adequate implementation of the component and the associated security measures, and the adequate documentation of the implementation and the associated operating procedures.

### Article 3.4.4
The selection, design, implementation, management, use, modification and removal of information system components shall take place in such a way that minimises information security risks. To achieve this goal, Bicsma BV benefits from risk assessments and adopts a risk-averse approach in addressing risks. In addition, newly acquired or adjusted components shall be conform to the security architecture of Bicsma BV.

### Article 3.4.5
Assets and data are classified according to reliability aspects. This results in a set of reliability requirements that need to be met at all times.

### Article 3.4.6

Where processes are sensitive to manipulation, appropriate segregation of functions is applied.

### Article 3.4.7
Data are used and processed in such a way that guarantees the privacy of employees, customers and suppliers.

### Article 3.4.8
Logical and physical access to the information systems and their individual components shall only be granted to authorised persons.

### Article 3.4.9
Should it be necessary to place a component of the information assets outside the BICSMA BV domain, the explicit and prior permission of the owner of that component is needed.

### Article 3.4.10
There shall be up-to-date reserve copies of all information relevant to the business operations. The owner of the relevant information is accountable for this information.

**Article 3.4.11**
IT resource owners shall ensure that system and user activities are recorded automatically and that the integrity of those data is monitored. This applies to the activities of system and application managers and other users with special privileges. The level of commitment depends on the classification of the IT resource in question.

**Article 3.4.12**
IT resource owners are responsible for ensuring that log files in which system and user activities are recorded are regularly checked for anomalies. Detected anomalies must be registered as incidents.

## 3.5 Technical security requirements

**Article 3.5.1**
Wherever possible, IT resources shall provide functionalities that allow for tracing activities. The information provided by this functionality shall be secured and accessible only to authorised persons. It is preferable to ensure that the manipulation of this information is impossible. It is a minimum requirement to ensure that the manipulation of this information is detected.

**Article 3.5.2**
IT resources shall allow for providing each individual user with a unique user account whereby users can be identified.

**Article 3.5.3**
The development and testing of new services, products or processes shall not take place in the production environment. Such activities shall be performed in a separate environment to prevent potential adverse effects on the reliability of production environment.

**Article 3.5.4**
Potentially sensitive data shall be exchanged in a way that ensures that the confidentiality and integrity of the data are preserved.

**Article 3.5.5**
The storage, transport, use and exchange of data shall take place in such a way that preserves the reliability of these data, including if the data carrier used falls into the hands of unauthorised persons.

## 3.6 Exceptions to the information security policy

Exceptions to the information security policy are granted under the following conditions:

**Article 3.6.1**
The asset and process owner(s) affected by the exception expressly agree to granting the exception.

**Article 3.6.2**
An owner is assigned to the exception and the owner expressly assumes responsibility for the associated risk.

**Article 3.6.3**
The exception is documented and the documentation clarifies what risks arise from granting the exception and how the risks will be handled.

**Article 3.6.4**

For minor deviations, the prior approval of the information security process owner is required. For major deviations, the prior approval of the information security process owner, the risk manager and the Management Team is required. It is up to the process owner to assess in which category the deviation falls. In the event of serious differences of opinion, the Management Team may be asked for arbitration.

# 4 Documents related to this policy

This strategic-level information security policy has been further elaborated on specific topics in tactical and operational level documents. These documents related to the information security policy are listed below and, together with this policy, are available at <location>.

## 4.1 Issue-specific information security policies

<List of information security policies used in Bicsma BV>

## 4.2 Information security guidelines

<List of information security guidelines used in Bicsma BV>

## 4.3 Codes of conduct

<List of codes of conduct used in Bicsma BV>

## 4.4 Architecture

<List of documents relevant to the security of Bicsma BV's information assets>

## 4.5 Benchmarks

<List of benchmarks used in Bicsma BV>

# 5 Explanation of terms

*Architecture*

A model of the coherence that exists between the individual components of the information assets. Different architecture models describe different aspects of the whole. In our context, the common forms of architecture are: the information architecture, the infrastructural architecture and the security architecture.

*Benchmark*

A detailed description of the technical security requirements in software and hardware installation and configuration.

*Code of Conduct*

A set of rules employees shall observe during and/or following the period of their employment. The code of conduct includes regulations on information security.

*Data carrier*

Any medium that contains data. Equipment including a data carrier shall also be regarded as a data carrier, as long as it contains the data carrier.

*IT resources/assets*

Collective name for hardware and software, IT services and products.

*Information security guideline*

A set of information security recommendations for a specific topic.

*Issue-specific information security policy*

A set of binding information security policy statements for a specific topic.

# 6 References

This information security policy is based on Bicsma BV's vision on information security and the ISO / IEC 27001 and ISO / IEC 27002 international standards. The information security process owner has drawn up a table in which the management objectives related to ISO 27001/27002 and the articles of this policy are mapped.