Information security policy (‘ISP’)

Owner: Corporate Security Team
Distribution: Public
Date: January 2025

Table of Contents

Management declaration **2**

1. Introduction **3**

2. Information security principles **3**

3. Information Security Management System (ISMS) **4**

3.1. Information security controls 4

3.2. Continual improvement 4

4. Information security governance **4**

3.1. Roles and responsibilities 4

3.2. Information security objectives 5

3.3. Information security policies and procedures 5

3.4. Training and awareness 5

3.5. External communication 5

3.6. Information security roadmap 6

3.7. Information security meetings and reporting 6

Management declaration

BICS delivers best-in-class communication solutions, from global voice services, seamless roaming and IoT enablement to global messaging to data consumers and digitally driven enterprises worldwide. The BICS team continuously strives to provide their customers with the highest levels of quality, reliability and interoperability enabling them to maximise their end-user value.

Information systems are for our company strategic assets, essential to conduct our business and assure the satisfaction of our partners. Considering business requirements, legal, regulatory and contractual requirements, and risk assessments results, BICS has the ambition to ensure the security of information systems and the achievement of the following information security objectives:

- Protecting the confidentiality and integrity of our informational assets
- Ensuring continuity of services to our partners
- Ensuring the compliance of BICS information system to security requirements
- Ensuring a proper management of information security risks
- Choosing suppliers whose security posture fits the requirements that we have set

In order to meet these objectives, we must be committed to continuous improvement, with the aim of achieving the best security posture and the highest level of security.

This document is one of the key elements to ensure the achievement of these objectives. Its main goal is to communicate to anyone in BICS, and to any interested party from our Information Security Management System our information system ambitions, and also the main documents and processes that manage information security, and the role and responsibility of these users.

Information security is everyone's business. The effectiveness of the protection of our information systems requires the commitment of all in the implementation of this document and any related documents. In this respect:

- Each member of the personnel (employee and contractor) is responsible for the information security and the use of the systems made available
- The team leaders must ensure secure information processing in their area of activity
- The IT suppliers and developers must offer secure solutions and implement the ISP in BICS applications, systems, platforms, processes, etc.
- Management needs to provide the strategic guidance on information security and support efforts into making information security part of our BICS DNA.

We rely on the personal involvement of each person having access to BICS information system for the success of this plan and therefore to contribute to the achievement of our ambitions.

1. Introduction

BICS Corporate Security team has developed and is maintaining the present Information Security Policy (ISP) that applies to all segments of BICS' organisation and operations, in any physical location. It is the reigning document that dictates the rules and guidelines of information technology within BICS. It is one of the key elements to ensure the achievement of the security objectives defined above in the management declaration. With it, BICS increases its level of maturity in the space of information security by embedding information security within its internal operational processes as well as in its client delivery. In addition, having this central information security document, BICS is also able to communicate to any users its ambitions and the role(s) and responsibility(ies) of these users.

2. Information security principles

Information Security concerns the protection of **information** and the associated **assets** against unauthorized access, modification, or destruction.

Information exists in different forms:

- Physical, meaning written form on paper
- Electronic, meaning electronically written, saved or transmitted
- Human, meaning spoken

Assets shall be understood as:

- IT applications
- IT infrastructure
- Storage media
- Physical premises
- Human resources

Information security protection is ensured following the three key information security dimensions:

- Confidentiality
- Integrity
- Availability

Confidentiality (C)

Confidentiality means that data is not disclosed to unauthorized individuals, entities, or processes. Confidentiality is achieved by using access control techniques, need-to-have and need-to-know principles, and in respect of privacy law.

Integrity (I)

Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life cycle. Integrity controls protect an information asset against improper data modification or destruction, as well as ensuring data non-repudiation and authenticity.

Availability (A)

Availability controls ensure timely (when and where needed) and reliable access to and use of data.

3. Information Security Management System (ISMS)

BICS has implemented and is maintaining an ISMS, in order to provide an adequate level of security within BICS. BICS is working with the most recent version of the standard: **ISO27001:2022**.

3.1. Information security controls

At BICS, information security is achieved by implementing controls, which can be policies, rules, practices, and procedures, as defined by ISO 27001:2022 - Annex A.

Not all the security controls described by ISO 27001:2022 are implemented to guarantee the security of BICS. Their implementation is dependent on the risk assessment results conducted on the determined scope, and on whether the risks identified are accepted or not. Moreover, the implementation of controls is also dependent on the Proximus Group requirements, Belgium laws, EU regulation and specific country regulation determined by telecom regulator.

3.2. Continual improvement

As stated in the management declaration, BICS must guarantee the continual improvement when it comes to information security, and particularly the ISMS.

The processes implemented to manage the ISMS are built in order to work in a Plan-Co-Check-Act cycle and ensures continual improvement. Policies, procedures, security requirements, roles & responsibilities, etc. were first defined (Plan), then implemented (Do). Then the compliance is checked (regular compliance checks, internal audits, etc.) (Check), and action plans are defined in case some non-compliance is discovered (Act).

4. Information security governance

4.1. Roles and responsibilities

Roles and responsibilities have been defined within BICS, in the aim that:

- Information security objectives are met
- The necessary support from the top management is provided, with regards to information security
- Resources needed for the maintenance of the ISMS and for information security on a larger scale are available and competent
- BICS adheres to a continual improvement strategy

The main roles and responsibilities are:

- **BICS Executive Committee** (managing director and his direct reports), who validates the information security roadmap and its accompanying risk assessments and ensures adequate resources and budget are attributed to information security and to the maintenance of the ISMS.
- **Chief Information Security Officer (CISO)**, who leads the Corporate Security teams to develop and implements an information security strategy and program, which includes procedures and policies designed to protect BICS information system from both internal and external threats and aligned with business objectives.
- **Corporate Security team** (Security governance, Security engineering and Security operations), who provides information security activities such as: incident management, employee security awareness training &

adherence to security practices, identity and access management, security architecture, SIEM, vulnerability management, etc.

4.2. Information security objectives

Information security objectives are listed in the beginning of this document, in the management declaration. They have been defined by BICS top management, based on business requirements, legal, regulatory, and contractual requirements, and risk assessments results.

In order to achieve these objectives, success criteria are defined on various processes and reviewed every year, with associated ownership and deadlines. Success criteria are measured by a set of KPIs, also defined every year. The KPIs aim to provide an overall monitoring, measurement, analysis, and evaluation of the security posture at BICS, and more specifically, of the ISMS.

4.3. Information security policies and procedures

BICS Corporate Security team has developed a set of security policies and procedures, that follows the principles stated in this document. Each policy or procedure addresses a specific security domain. All these policies are available for anyone at BICS. The policy framework is reviewed at least every year, or when a need for review arises deriving, for example, from changes in organizational structure, processes or technology, or changes in industry standards and best practices that define the basis of the current document.

4.4. Training and awareness

BICS is committed to promoting an information security culture among all employees. To achieve this, throughout the year there are regularly training and awareness programs and activities to educate staff of security best practices. Moreover, more specialized training opportunities are also offered, to ensure that everyone has the best skills possible to safely conduct their responsibilities. Yearly, a security training and awareness program is developed, and it applies to everyone in BICS having access to BICS information systems (employees, contractors, etc.).

4.5. External communication

External communication is done on an ad-hoc basis, with the consultation of BICS External Communications department. Communication means is decided by external communications department. Examples of what could be communicated are:

- Results of risk assessment with a critical severity that directly impact or involve the specific internal team
- Information security objectives
- Achieved certifications
- Changes to the organizational structure of the ISMS roles
- General relevant updates to the ISMS (positive and negative)
- Major update in the security policies or other ISMS documents

External communication can be done, depending on the topics, to:

- Third parties (customers, prospects, suppliers, partners…)
- Authorities and regulators
- Auditors

Additional communication towards specific customers can be done in liaison with account managers, proactively by BICS or upon customers' requests.

4.6. Information security roadmap

The Security roadmap is defined every year and approved by the top management. It contains all the projects (potentially multi-years projects) and recurrent activities which aim to improve the security level within BICS and/or to maintain the ISMS. The security roadmap is defined and accordingly amended depending on:

- The outcome of the risk management practices
- BICS business roadmap
- Security trends and security needs observed by Corporate security team
- Legal or contractual requirements

The security roadmap is defined with the permanent objective of continuous improvement.

4.7. Information security meetings and reporting

BICS Corporate Security team regularly reports to top management, at the Exco level, via different means:

- The **Committee Security & Business continuity & Privacy (CSBP)** serves as a formal decision-making meeting, regarding information security, privacy and business continuity within BICS.
    - CSBP gathers the managing director, his direct reports, BICS CISO, BICS DPO, BICS Head of Business Continuity.
    - The CSBP is called minimum 2 times a year but can also be called whenever there is a specific need. On the security related part, the CSBP discusses the following topics:
        - Review of risks with a high severity
        - Discussion on the main security projects
        - Validation of the major changes in the security policy framework
        - Update on the main topics discussed during the last ISMS management review
- The **ISMS management review**, which aims to provide top management with relevant information related to the ISMS, so that they can ensure its continuing suitability, adequacy, and effectiveness.
    - The management review gathers BICS sponsors for the ISMS, the CISO and some team leaders in charge of the main processes of the ISMS scope.
    - The management is held minimum 2 times a year but can also be called whenever there is a specific need.
    - The management review discusses the following topics:
        - Status of actions from previous management reviews
        - Changes in external and internal issues that are relevant to the ISMS
        - Changes in needs and expectations of interested parties that are relevant to the ISMS Feedback on the information security performance, including trends in non-conformities and corrective actions, monitoring and measurement results, audit results and fulfilment of information security objectives
        - Feedback from interested parties
        - Results of risk assessment and status of risk treatment plan
        - Opportunities for continual improvement

- The **SIRT report**, which is sent by Security Operations team every month to BICS Executive committee. It gathers information regarding information security related activities:
    - Information security incidents
    - Security vulnerabilities
    - Security policies exceptions
    - Security awareness results
    - Other security activities