Information Security Policy

Author:	Loris Gutic
Date:	23.01.2023.
Classification:	Public
Version:	2.0

DOCUMENT SUMMARY

Summary
The purpose of this document is to define the Management Board's commitment and support for Information Security (or IS, interchangeably) in Bright Security (hereinafter: Bright). It acts as the high-level document for IS in Bright, defining requirements and principles for implementing and managing IS. IS in Bright is based on the international standards ISO27001, ISO27002, other documents from the ISO27xxx series of standards and NIST Cybersecurity Framework.

VERSION CONTROL RECORD		
Version	**Description / Relevant Changes**	**Date**
2.0	Alignment with international standards and internal developments	23.01.2023.

NEXT REVIEW LATEST ON	23.01.2024

ADDITIONAL INFORMATION

CONTENTS

DEFINITIONS

FULL NAME	TRANSLATION / CLARIFICATION / COMMENT
IS	Information security
ISMS	Information security management system
ISRM	Information security risk management
ISIM	Information security incident management
Availability	the property information and process that allows access to this information and processes, and their usefulness, ie. their availability at the request of an authorized entity ..
Integrity	the property information and processes that are unauthorized or unforeseen alterations.
Confidentiality	the property information and processes that are unauthorized or unforeseen alterations.
CISO	Chief Information Security Officer, a person appointed by Management and responsible for overseeing and managing ISMS in Bright

TERMINOLOGY

STATUS	TERMS TO BE USED IN STATEMENTS
mandatory	must shall required
recommended	should
optional	may
not recommended	should not
not allowed	must not shall not

INFORMATION SECURITY POLICY

INTRODUCTION

Bright shall establish, implement, monitor, maintain, regularly reviewed and improve process management information system in order to reduce exposure to risks, security confidentiality, integrity and availability of information and the overall information system, it is appropriate size, complexity, and scope of the Bright's operations, and the complexity of the information system.

Bright defines Information Security as follows:

Information Security (IS) is the preservation of confidentiality, integrity, and availability of information assets. In addition, and where applicable other properties, such as authenticity, non-repudiation, and reliability should also be involved.

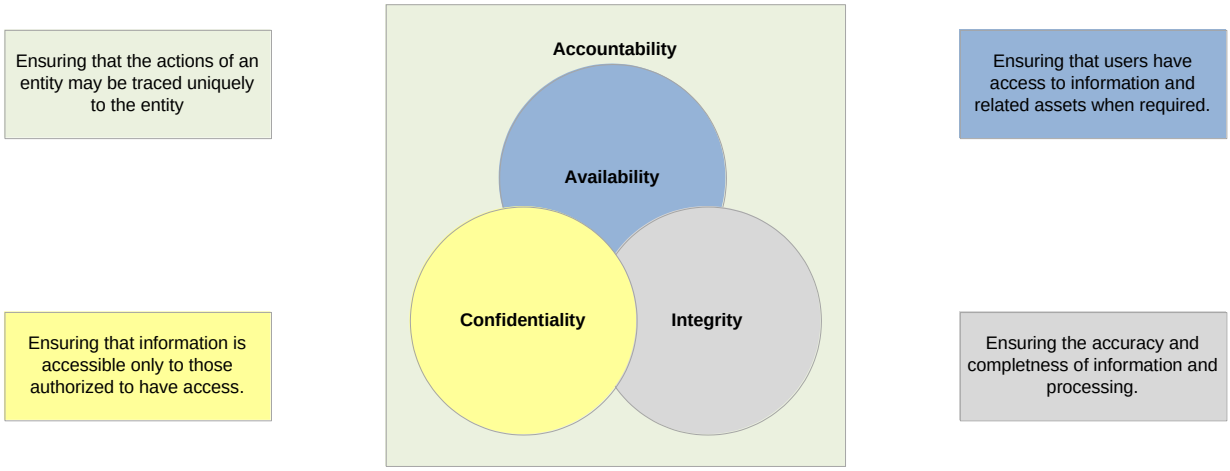

Figure 1: Definition of Information Security

Management support

Bright Management Board commits to ensuring and preserving the availability, confidentiality, integrity, and accountability of information assets of the company, customer data, and third parties. Bright is aware that the protection of information assets is one of the key Management Board responsibilities.

The implementation of the Information Security Management System is the responsibility of CISO.

Management fully supports Information Security by guaranteeing the authority and resources of the CISO. The decision-makers are constantly involved in IS processes and informed about the current IS risk profile and IS incidents.

Business success factor

Information is an asset and should be treated as such. Information Security is seen as a support and success factor for market activities and for accomplishing business goals by protecting sensitive/critical information in Bright. For this purpose, Bright commits to implement and support IS according to the risk assessment, business needs, international standards, and good practices as any other business process.

Proactive approach

A proactive approach to information protection is used to define preventive measures and safeguards for treating information risks. The main goal of IS is to manage risks related to information protection through assurance of and responsibility for the availability, integrity and confidentiality of information assets and accountability of actions.

Adequate measures for avoidance, reduction, transfer, or acceptance of risks including priorities for implementation of safeguards are based on cost-benefit analysis, international standards, good practices, and legislative requirements where applicable.

Collaboration

All Bright employees are actively involved in IS through conscientious handling of information, participation in training and core IS processes and prompt reporting of IS incidents. The collaboration of all parties and employees involved in IS processes in Bright is seen as a key success factor in achieving Bright IS strategies and guaranteeing the successful implementation of standardized and cost-efficient IS controls.

Continuous improvement

It is the goal of Bright to improve Information Security successively in accordance with industry developments, risk assessment, business needs, international standards, good practices, and legislative requirements where applicable. Key elements of ISMS shall therefore

be subjected to regular reviews, with the aim of ensuring their full alignment with the current circumstances and trends.

MOTIVATION AND GOALS

The purpose of this Information Security Policy is to prescribe high-level settings for the implementation of processes and information security management system - ISMS, define the competencies and responsibilities of participants of the process, improve the quality of operations, increase the level of protection of the information used in Bright business processes, and to meet legal and regulatory obligations.

COMPETENCIES AND RESPONSIBILITIES

Management Board is obliged to, as a minimum:

1. Develop an information system strategy, which needs to be a constituent part of the overall business strategy of Bright,
2. When circumstances so enable, ensure the selection, appointment, and authority of a qualified and competent manager who will serve as Chief Information Security Officer, and who will oversee the establishment and monitoring of the information security management processes,
3. Instruct and support CISO in developing policies for information system management, especially the information security policy, and oversee their implementation,
4. Adjust the reality of the adopted policies to the changes in the economic, market, technological and other conditions,
5. Establish the system for measurement, follow-up, control and management of risks related to the information systems security, so that it can follow the efficiency and update the given system,
6. Develop and enable the establishment of an adequate organizational structure and establishment of adequate functions and authorizations in order to secure an efficient and protected information system management,
7. Prescribe content and periods for reporting to the Management and Supervisory Board of Bright about the relevant facts related to the information system management,
8. Enable the information system management controls, as well as the information system internal control system, to be under continuous supervision and periodically subjected to external audit,
9. Appoint the security committee made of representatives of different business functions, which should meet periodically and ensure coordination of the initiatives and monitoring of the information system development activities, as well as the compliance of the information system goals with the business goals and overall business strategy,

10. Ensure that needed resources are provided for successful and uninhibited management of information system security.

CISO is obliged to, as a minimum:

1. Establish and implement the policies and the procedures for the information system management in compliance with the business goal and the business strategy,
2. Implement the system for measurement, monitoring, control, and management of the risks related to the information system,
3. Ensure that all the duties related to the information system management are clearly defined and designated,
4. Develop a plan and program for advocacy and raising awareness about the information system security,
5. Adopt methodology to define the criteria, manner and procedure for managing the risks deriving from the use of the information systems, and determine the responsibility for risk management and acceptable levels of risk,
6. In continuation analyse information system risks, take steps to decrease the risk to an acceptable level, and at least once a year report to the Management and/or Supervisory Board as needed about the risk assessment results.

CISO is also tasked with:

1. Defining, implementing, and monitoring corporate security goals, strategy and security posture, as well as overall corporate security strategic and operative processes
2. Information security system management in accordance with national and international regulation, standards, and practices
3. Data protection and privacy management in accordance with national and international regulation, standards, and practices
4. Managing fraud prevention, internal investigations, and case management in accordance with national and international regulations, standards and practices
5. Business continuity management and business impact analyses coordination
6. Monitoring, coordinating, and supporting organizational units within the company in conducting security management-related activities and processes
7. Organizing and conducting internal and/or external corporate security training, educations and awareness-raising
8. Cooperating and supporting audits, supervision, or controls in the corporate security domain
9. Submitting regular and ad hoc reports to the Management Board
10. Conducting other special corporate security activities in accordance with Management Board instructions
11. Managing, coordinating and/or supporting ongoing projects as determined by the Management Board.

INFORMATION SECURITY CORE COMPONENTS

The Management Board supports the implementation of Information Security (IS) based on international family of standards ISO/IEC 27xxx and other industry-relevant standards (e.g. NIST Cybersecurity Framework).

Therefore, specific internal documents, subordinate to this Information Security Policy, must be adopted to support the implementation of this Policy:

- Information Security Strategy and Organization Policy
- Information Security Risk Management Policy
- Information Security Incident Management Policy

INFORMATION SECURITY STRATEGY AND ORGANIZATION

The strategy of information security management should be a part of Bright strategy.

Bright is obliged to develop and monitor the implementation of the information system strategy which, at a minimum, should:

- Cover long-term and short-term initiatives related to the information security system,
- Define the relation and compliance of the goals of the information security system with the business goals,
- Develop in more detail through the development of strategic and operating plans

Bright Information Security Strategy and Organization Policy specifies the strategic direction, goals and principles, framework for implementation, management process and implementation requirements regarding Information Security in Bright. The policy also defines the functional and structural organization for Information Security in Bright and allocates roles and bodies, involved in the Information Security Management Process.

INFORMATION SECURITY RISK MANAGEMENT

Bright Information Security Risk Management Policy established basic elements required in order to have the CISO implement Information Security Risk Management and perform appropriate risk assessments.

The objective of Information Security Risk Management is to contribute to the achievement of an organization's objectives by proactively protecting the assets that support the organization's mission. This is accomplished within a structured process to identify, assess, treat, communicate, monitor, and review risks.

Information Security Risk Management is a specific part of the organization-wide risk management activities with focus on information security risks.

Information Security Risk Management can be described as a continuous process for:

- Identifying organizational needs regarding Information Security requirements
- Establish the context of threat and risk manifestations
- Identifying information assets, threats, vulnerabilities, consequences, and controls
- Analysing the risks by assigning values to the probability and consequences
- Treating the risks using a risk treatment plan to implement the controls
- Deciding on and formally accepting residual risks
- Regularly communicating risks to the decision-makers to inform them about the risk profile
- Monitoring and reviewing the approach, risk profile and related controls

The purpose of the Information Security Risk Management Policy is to define the Framework that will ensure that risks related to information assets are managed in a systematic and unified manner.

INFORMATION SECURITY INCIDENT MANAGEMENT

As a key part of Bright's overall information security strategy, controls and procedures shall be put in place to enable a structured, well-planned approach to incident management.

From the business perspective, the prime objective is to avoid or contain the impact of Information Security incidents to reduce the direct and indirect costs caused by the incidents.

The primary steps to minimize the direct negative impact of information security incidents are the following: stop and contain, eradicate, analyse and report, and follow up/lessons learnt.

To be able to do this, responsibilities, plans and procedures should be in place to handle information security events and incidents effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluation, and overall management of information security incidents.

The aim of Information Security Incident Management is to ensure that Bright reacts appropriately to any actual or suspected Information Security incident relating to information systems and data. It is essential to have a structured and planned approach to:

- Detect, report, and assess information security incidents.
- Respond to information security incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas).
- Align with existing crisis management and business continuity processes and procedures

- Report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately.
- Learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to incident management.