Policy for Security: Company guidelines for information security

1 Introduction

This document sets out the company policy defined by Benacchio Directors regarding the management of information, data and physical assets, in order to ensure the security of information and data processed by the company, in terms of confidentiality, integrity and availability.

1.1 Purpose of the document

The Security Policy defines the guidelines on the basis of which the entire System for the Management of Information Security is defined. Any plan and procedure regarding the processing of information or that may have impact with information security, must comply with the policy outlined in this document.

1.2 Scope

The Security Policy applies to all activities carried out by Benacchio, and in particular to the Product Management activity, i.e. the design, development and maintenance of software products and infrastructure management related.

1.3 Organization of the document

The document is divided into three chapters, including this introductory chapter.
Chapter 2 defines the principles that make up the Benacchio Safety Policy; in Chapter 3
the responsibilities that fall within the competence of various figures present in the organization are outlined.

2 Policy

Below are the policies defined by Benacchio regarding information security.

2.1 Acceptance

Employees, collaborators, suppliers, partners, contractors and all other third parties involved in institutional activities of Benacchio must accept their obligations and individual responsibilities in order to protect information, assets and Benacchio's resources or entrusted to Benacchio by third parties.

2.2 Access

Access to information, assets and resources of Benacchio or entrusted to Benacchio by third parties must be controlled and monitored on the basis of the following criteria:

- Access is authorized only for the necessary information (principle of minimum knowledge or need to know);
- Access is authorized only for information regarding specific activities.

2.3 Evaluation

Benacchio defines the right relationship between:

1. the expenses necessary for the implementation of measures in order to protect information, assets and resources of Benacchio or entrusted to Benacchio by third parties;
2. the risks associated with unauthorized use, modifications or destruction.

2.4 Awareness

The company management ensures that every employee, collaborator, supplier or third party is aware of Benacchio's Safety Policy and that its conduct and the tools used are adequate and in line with Benacchio's safety policy.

2.5 Training

The company management ensures that each resource is trained on the organizational policies applied and procedures related to information security.

2.6 Compliance with laws and mandatory regulations

All information processing and safety procedures of BENACCHIO SRL comply with laws and mandatory regulations. BENACCHIO SRL protects security of information in full compliance with the laws and regulations. Benacchio also undertakes to maintain an inventory of the software licenses purchased by the company and to periodically check the use of software with licensing rights by its employees and collaborators, counteracting the violation of these rights.

2.7 Protection

All information, assets and resources of Benacchio or entrusted to Benacchio by third parties are protected against risks associated with respect for confidentiality, integrity and availability in proportion to their value and in compliance with the laws in force.

Relevant records are protected from loss, destruction, falsification, unauthorized access and disclosure, in compliance with legal, regulatory, contractual and business requirements, through specific technical tools and operative procedures described in the Physical Security Plan, in the Logical Security Plan and in the Control Procedure of accesses.

IT systems that use public communication channels (e.g. Internet network) are configured to perform the encryption and decryption of transmitted information. For communication between internal systems, cryptographic keys can be generated by the systems dedicated to this operation by the Corporate Information Systems Area. The cryptographic keys used on systems that communicate with third parties, are generated and managed by external Certification Authorities. Both methods guarantee the same level of protection, guaranteeing authenticity, confidentiality and integrity of transmitted information. The process of managing the life cycle of cryptographic keys, edited by the Corporate Information Systems Area, is described in the Logical Security Plan.

The use of cryptographic tools is implemented in full compliance with current legislation and in accordance with regulations and agreements with third parties.

The systems used to manage company information are located in secure rooms with controlled access. The protection is guaranteed by appropriate countermeasures to prevent the violation of confidentiality and integrity both physical and logic, described respectively in the Physical Security Plan and in the Logical Security Plan.

Benacchio adopts a policy of separation of the IT environments dedicated to development, testing and operation of its information systems, in order to reduce the risks of unauthorized access to information and modifications or unavailability of operating systems.

The security of information that is managed outside the company information system is protected through specific behavioral policies communicated through the Company Regulations.

2.8 Security in design and development of IT solutions

Benacchio adopts a set of tools described in the Logical Security Plan and in the Physical Security Plan to ensure the safety of the development process.

2.9 Relations with suppliers

BENACCHIO SRL adopts the policy of making responsible its suppliers and third parties with whom it collaborates for its own activities, through specific non-disclosure agreements.

The SLA indicators and the NDA agreements with suppliers are periodically reviewed and in any case following each revision of risk valuation.

3 Responsibility

The responsibilities referred in this chapter are general and concern the entire Benacchio organization.
Everyone must:

- protect confidentiality, integrity and availability of information and intellectual resources of Benacchio or entrusted to Benacchio by third parties;
- protect material assets, IT systems and resources of Benacchio or entrusted to Benacchio by third parties;
- protect each information, activity and resource under its own responsibility;
- contact the Management, the competent and / or appropriate authorities in case of actual or alleged security breaches;
- contact the Management and the Head of Security, in case of any necessary modification of policy safety, safety requirements, standards, procedures.
- The violation of principles and behaviors for the protection of information security will be prosecuted by measure proportionate to the seriousness of the infringements committed and by the "Organization, Management and Control Model" that Benacchio has implemented pursuant to Legislative Decree 231/2001.

The Heads of Organizational Units must:

- be in line with the safety policy, requirements, standards and procedures defined;
- identify and define the access rights of resources for their specific activities and responsibilities;
- require third parties to be in line with confidentiality agreements (non-disclosure agreement);
- define an acceptable risk level following the implementation of a risk valuation;
- monitor the compliance with the provisions of the Safety Policy by its employees.

The Head of SGSI must:

- guarantee and monitor compliance with safety policies, requirements, rules and defined procedures;
- ensure that BENACCHIO SRL personnel are trained and aware of the Policy, requirements, standards and defined procedures to guarantee the security of information and resources.

The IT Security Manager must:

- implement safety management on the basis of the safety policies issued by BENACCHIO SRL;
- review information and physical resources under his responsibility, in order to define the adequate level of control to be implemented so that the security control is proportionate to the value of the information and the resources to be protected and in compliance with laws and mandatory regulations;
- define the safety requirements that must be taken into account when defining the maintenance budget and the development of company information systems;
- regularly check the status of company information systems to ensure compliance with standards and security policies of BENACCHIO SRL.

The Heads of the Organizational Units have the following responsibilities:

- •ensure compliance with Italian law in the activities of its Organizational Unit and in the treatment of information;
- make the human resources belonging to their Organizational Unit aware of the consequences in case of failure to comply with the security policy.
- Any change to organization or business processes, structures and processing systems of information that have an effect on information security, must be evaluated and authorized by Management.

Benacchio's approach in managing information security and its implementation (objectives of controls, controls, policies, processes and procedures for information security) is reviewed annually as part of the Management review processes, or independently of the annual frequency, when significant changes occur.