Information Security Policy

Responsibility for Document Issuance

Issuance Cycle	Function	Date
Developed by	ICT	02/04/2018
Checked by	Head of ICT	17/04/2018
Approved by	Compliance and AML Function	04/05/2018
	B.U. Regulation and Processes	18/04/2018
	Risk Management Function	04/05/2018
	Supervisory Board	14/05/2018

Change history

Rev	Date	Subject of revision
3	06/06/2016	Compliance to C. 285 Bank of Italy-16th update – formal review of the document, already approved by Board of Directors on 20/06/2014 and following CSI of 05/03/2015.
4	24/04/2018	Modified the cover of the present Policy, Compliance to EU Regulation 2016/679 (GDPR) and further updates in compliance to C. 285 of 17 Dec. 2013 of Bank of Italy

Table of Contents

INTRODUCTION

The Information Security Policy of Banca Farmafactoring is implemented to protect the information management system against events such as threats or incidents, external and/or internal, objective and/or subjective, which can affect the delivery of services.

The purpose of this document is to stipulate the needs, objectives, aims, and organizational models of the security strategy pursued by Bank Farmafactoring, in order to orient the development, management, control and verification of the effectiveness of its implementation.

The Security Policy Declaration is provided in Annex 1.

SCOPE OF APPLICATION

The Information Security Policy is valid for Banca Farmafactoring, for Banca Farmafactoring S.p.A. – Sucursal em Portugal and for Banca Farmafactoring S.p.A. – Sucursal en España (as well as for any further branch which may subsequently be established) and applies to all information processed by the Bank in any nature and form it had or will obtain, and to all management systems and storage media used for processing and conservation.

The recipients of the policy are all employees, contractors and consultants, full-time and for a defined time. All subjects who benefit from the information services of Bank Farmafactoring, as well as customers, are obliged to observe this policy. In particular, IT providers in respect of the typical conditions of operation directly in management information systems are obliged to observe the Security Policy.

PURPOSE

In relation to what is defined in the document **06 – SGSI Banca Farmafactoring – Information Security Manual**, the objective of the "Information Security Policy" is providing management direction and support for the proper management of information security.

Banca Farmafactoring considers the management system and the managed information an integral part of ownership. It is a goal of absolute priority to safeguard the security of the information system and to protect the confidentiality, integrity and availability of collected or otherwise processed information, against every intentional or accidental, internal or external threat.

In this extent, it is meant for:

- **Confidentiality:** guarantee that a given piece of information is secured against improper access and is used exclusively by authorized persons;
- **Integrity**: the guarantee that any information is the same originally entered into the computer system, that it has been modified in a legitimate way by authorized personnel only and any modification is tracked;

- **Availability:** the guarantee of the availability of information in relation to the requirements of continuity of delivered services and in respect of the rules imposing its safe conservation;
- **Authenticity:** the guarantee that the received information corresponds to the one generated by the person or entity who transmitted it.

Banca Farmafactoring introduces the basis for the information protection policy, as a suitable risk analysis of all resources (*Assets*), constituting the information management system, in order to understand its vulnerability, to assess the possible threats and to take the necessary countermeasures.

The awareness that the above is not possible to obtain, as is natural in the computer field, is a condition of absolute safety and implies the purpose of the Information Security Policy, that is the management of risk at an acceptable level with the design, implementation and maintenance of the Information Security Management System (ISMS) in line with the risk inclinations defined at the enterprise level, as defined in the regulation of risk management.

INFORMATION SECURITY DOMAINS

This IT Security Policy, based on ISO 27002:2013 standard, describes policies, principles, security rules and compliance requirements of particular relevance to the Company, in accordance with the following domains[1]:

- Security policies;
- Human resources security;
- Management of Company assets;
- Access management and control;
- Physical and environmental safety;
- Safety of operational activities;
- Security of communications;
- Acquisition, development and maintenance of the Information System;
- Relations with suppliers;
- Management of security incidents;
- Business continuity management.

A more detailed analysis of security audits and controls is provided in document 06 - SGSI Banca Farmafactoring – Security Operating Manual.

[1] Non-exhaustive list.

OBJECTIVES

The objectives of the Information Security Policy that the Company intends to pursue are as follows:

- Provide the staff and co-operators with respective knowledge and awareness of the concerns associated with the security of information, in order to acquire sufficient awareness of their responsibilities with regard to its processing;
- Ensure that all external suppliers are aware of the information security concerns of the Company and comply with the adopted security policy;
- Establish guidelines for the application of standards, procedures and systems to pursue the information security management system (ISMS);
- Use the standard ISO 27001:2013 "Information Security Management Systems - Requirements" and ISO 27002:2013 'Code of practice for information security management" as the guidelines of their information security and pursue compliance;
- Ensure that all Company personnel is familiar with the technical rules and organizational capabilities in the exploitation of information systems stipulated in the relevant safety procedures implemented specifically for this purpose;
- Ensure that all staff is informed about the responsibility for the management of information;
- Ensure that all employees are familiar with the "General Data Protection Regulation" on the protection of personal data" and implications, as well as the detailed rules for the application of provided measures, as defined in the operational security procedures;
- Ensure that the IT risk management process adopted by the Company is adequately monitored and periodically updated in the light of the parameters set out in the regulations constituting the ISMS.

  In this context, the controls aimed at meeting the needs of control and protection of technological risk are also regulated[2].

REVISION AND CONTROL

The CEO supported by the CISO, is responsible for the periodic review of the policy, thus it will be compliant with any significant changes in the organization and/or in the technologies used for the protection of information.

The review will be made periodically or on the occasion of significant organizational and/or technological changes relevant for the management of information. The Supervisory Board will thus approve the revised security policy.

[2] Please refer to Document "Risk Analysis" for further details.

Information Security Policy falls under the requirements stipulated by the Company of Italy (Chapter 4, Section IV, para. 2 of the Circular Informative of the Company of Italy n° 285 of 17 December 2013, "Supervisory Provisions for Companys' and subsequent updates.

FIGURES INVOLVED IN SECURITY MANAGEMENT

On the basis of the 06 - SGSI Banca Farmafactoring – Security Operating Manual and in compliance with the Regulation (EU) 2016/679 - General Regulation on data protection, the types of roles to be identified are:

- Supervisory Board;
- Chief Executive Officer;
- Risk Management Function;
- Compliance and AML Function;
- B.U. Regulation and processes;
- Internal Audit Function.

Security and Business Continuity:

- Information Security Committee (CSI);
- CISO;
- Business continuity Manager;
- System Administrators;
- Security Specialists;
- Coordination Group for restore activities.

Privacy:

- (Data) Controller;
- Controller delegate;
- Privacy Coordinator;
- Data Protection Officer;
- Head of B.U. / Function;
- External Data Processor;
- Data Processing authorized people;
- Network user.

For details of the powers and general principles of security regarding the use and management of the Information System by the Company figures mentioned above, please refer to Security Procedure PS-6.1.1. Roles and Responsibilities.

SECURITY ORGANIZATION

To ensure adequate security management, the Company has set up suitable organizational structures (see above; for further information please refer to Security Procedure PS-6.1.1. Roles and Responsibilities, par. "Operating Procedure") for the identification and control of measures to prevent and protect the confidentiality, integrity and availability of data through the ISMS.

To ensure that adequate levels of efficiency and protection are maintained, the organization of Security and the related procedures/protection measures are subject to analysis as part of the checks pertaining of the Company's Internal Control Functions.

The outsourced infrastructure and application systems are monitored by internal contacts identified from time to time, who are responsible for ensuring that suppliers operate in compliance with contractual agreements and applicable regulations.

Non-observance of the provisions set out in this Policy, as well as in the overall ISMS, means that Company's people are subject to the responsibilities arising from their conduct and may result in penalties that may go so far as to dismiss them. For further details on this liability regime, reference should be made to the document "Guidelines for Information Security".

NORMATIVE REFERENCES AND STANDARDS

Many aspects of information security are governed by the Italian and Community legislation; the following rules are considered to be the most important:

- Resolution of the Council of the European Union of 6 December 2001: common approach in the field of network and information security;
- Recommendation of the Council of the European Union of 25 July 2002: OECD guidelines on the security of information systems and networks.
- The decree of the President of the Council of Ministers 30 October 2003: Approval of the national scheme for the evaluation and certification of safety in the field of information technology, pursuant to art. 10, paragraph 1, of Legislative Decree of 23 January 2002, n.10.

SECTORAL LEGISLATION

Circular Informative of Bank of Italy n° 285 of 17 December 2013, "Supervisory Provisions for banks' and its updates.

PRIVACY

- The deliberation of the privacy guarantor number 53 of 23 November 2006: Guidelines on the treatment of personal data of workers;
- The deliberation of the privacy guarantor number 13 of 1 March 2007: use of email and the Internet;
- Measure the privacy guarantor of 13 October 2008: disposal and securely erasing data;
- Measure the privacy guarantor of 27 November 2008: System administrators; Amended on 25 June 2009;
- Measure the privacy guarantor of 8 April 2010: video surveillance;
- Requirements for the circulation of information in banking and tracking of banking transactions - 12 May 2011;
- Article 6 of the D.L. (Decree Law) 13 May 2011, n.70: "European Semester - the first urgent provisions for the economy - Decree Development" converted in Law, with amendments, by art. 1, paragraph 1, L. 12 July 2011, n. 106;
- Article 40, paragraph 2(a) and (b) of the D.L. (Decree Law) 6 December 2011, n. 201: "Urgent provisions for growth, fairness and the consolidation of public finances", converted with modifications by Law 22 December 2011, n.214;
- Article 45 of the D.L. (LAW) 9 February 2012, n.5: "Urgent provisions in terms of simplification and of development, converted in Law, with amendments, by art. 1, paragraph 1, L. 4 April 2012, n. 35;
- D. lgs. (Legislative Decree) 28-5-2012 n. 69; "Changes to the Legislative Decree 30 June 2003, n. 196 laying down the Code in matter of protection of personal data in implementation of Directives 2009/136/EC, with regard to the processing of personal data and the protection of privacy in the electronic communications sector, and 2009/140/EC in the field of electronic communications networks and services and of Regulation (EC) n. 2006/2004 on cooperation between national authorities responsible for the enforcement of legislation on consumer protection".

COMPUTER CRIME

- Law n. 547 23 December 1993: amendments and additions to the rules of the criminal code and the code of criminal procedure in the theme of cybercrime;
- Law 18/03/2008 n.48: Ratification and implementation of the Council of Europe Convention on cybercrime signed at Budapest on 23 November 2001 and regulations concerning internal adaptation;

COPYRIGHT

- L. 22 April 1941, n. 633: protection of copyright and other rights connected with its exercise;

- D. lgs. (Legislative Decree) 518/1992: implementation of Directive 91/250/EEC on the legal protection of computer programs;
- D. lgs. (Legislative Decree) 169/1999: implementation of Directive 96/9/EC on the legal protection of databases;
- D. lgs. (Legislative Decree) 10 February 2005 n.30: "Industrial Property Code";
- Decree of the Ministry of Economic Development 13 January 2010 n.33: Regulation for the implementation of the Code of industrial property.

STANDARD

The main standards for the basis of the policy of security of information, are as follows:

- ISO 9001:2008 - Quality Management Systems - Requirements;
- ISO/IEC 73:2009 - Risk management - Glossary - Guidelines for use in standards;
- UNI ISO 31000: 2010 - Risk management - Principles and guidelines;
- ISO/IEC 27001:2013 - Information security management systems - Requirements;
- ISO/IEC 27002:2013 - Code of practice for information security management,
- ISO 22301 - "Societal Security - Business continuity management systems - Requirements";
- ISO 22313 - "Societal Security - Business continuity management systems - Guidance".

USE OF INFORMATION PROCESSING SYSTEMS

Banca Farmafactoring considers information processing systems to be operational instruments for all people working at any level.

The instruments made available must be used for carrying out work in a manner strictly relevant to the specific goals of their activity in respect to the needs of functionality and security of the systems and the network.

Banca Farmafactoring will pursue the laws and the existing contract of employment with a collaborator who improperly uses the information processing systems.

SAFETY CHECKS AND INSTRUMENTATION CONTROLS

To verify the correct use of all computer facilities made available to users, Banca Farmafactoring will carry out a verification tests concerning security measures and extensive test to verify the vulnerability of this *asset* (e.g. *Penetration Test*). The broader details of the

safety checks and controls are stipulated in the "06 - ISMS Farmafactoring - Operating Manual for safety".

Additionally, the Company, at regular intervals, performs business continuity and Disaster Recovery tests to review the efficiency of their plans.

ORGANIZATION AND RESPONSIBILITY FOR SECURITY

The organization of safety is stipulated in the document "06 - ISMS Farmafactoring - Operating Manual for safety" in Chapter 6 " Safety Organization" and in the Security Procedure PS-6.1.1 roles and responsibilities.

The Supervisory Board is responsible for the content of the Information Security Policy, its adoption, implementation and upgrade.

The Supervisory Board is technically and organizationally supported by the Information Security Committee (CSI) and by the CISO; the latter is supported by the Coordination Group for restore activities and by the Security Specialists and System Administrators (roles and responsibilities are indicated in the security procedure PS-6.1.1).

The main activities of the CISO are to supervise the correct implementation and maintenance over time of the Information Security Management System, to promote and coordinate risk analysis activities, to manage relations with telecommunications operators and relevant service providers, and to verify annually the validity of the Business Continuity Plan and Disaster Recovery.

COMMUNICATION, TRAINING AND RAISING THE AWARENESS OF USERS

The Security Policy is made known to all staff and collaborators, customers and suppliers via the institutional web site.

The Security Manager via proper information sessions, informs and sensitizes internal users to the proper application of security procedures for information, stimulating them to cooperate more effectively, in order to work in an ever coordinated and exhaustive manner on this issue.

ANNEX 1

To all those responsible for corporate functions

And to all Staff

Subject: Information Security Policy

Information is an integral part of the Company's heritage.

Current technologies promote the distribution and use of information, but they expose the Company to new risks, such as fraud and computer espionage, that make information security a strategic objective to be pursued, in order to preserve its competitive advantage.

This document constitutes direction and guideline for the establishment of Information Security Management System (ISMS) and for each subsequent act or measure aiming to ensure confidentiality, integrity and availability.

The Information Security Management System provides the best international standards and ensures compliance with national regulations applicable to the sector.

The objectives that the Company intends to pursue are for the staff and co-operators to be provided with the respective knowledge and awareness of the concerns associated with the security of information, and obtained sufficient awareness of their responsibilities with regard to how it is treated; to ensure that all external suppliers are aware of the Company's information security concerns and comply with the adopted security policy; to establish guidelines for the application of standards, procedures and systems, in order to pursue the Information Security Management System (ISMS); to ensure that all staff is informed about the responsibility for information management.

All personnel should henceforth know and respect the organizational model and safety procedures, should adapt to this during the performance of their duties. In particular, personnel must have access to the information and functions that are indispensable for proper performance of tasks and duties. Access to information assets is pursuant to the obtained explicit authorization, and when such is not obtained, access cannot be allowed. Access to the Company by outside personnel must be controlled and supervised in accordance with appropriate Security Procedures.