Politica per la sicurezza delle informazioni

Responsabilità Emissione del documento

Ciclo di emissione	Funzione	Data
Elaborata da	ICT	02/04/2018
Verificato da	Responsabile ICT	17/04/2018
Approvato da	Funzione Compliance e AML	18/04/2018
	U.O. Normativa e Processi	04/05/2018
	Funzione Risk Management	04/05/2018
	Amministratore Delegato	14/05/2018
	Consiglio di Amministrazione	23/05/2018

Oggetto della Revisione

rev	Data	Oggetto della modifica
3	06/06/2016	Adeguamenti in conformità alla C. 285 Banca d'Italia 16° aggiornamento – revisione formale del documento, già approvato in sede di CdA il 20/06/2014 e successivo CSI del 05/03/2015
4	24/04/2018	Modifica del frontespizio della Policy, adeguamento al Regolamento (UE) 2016/679 e ulteriori adeguamenti in conformità alla Circolare n. 285 del 17 dicembre 2013 della Banca d'Italia

Indice

INTRODUZIONE

La politica di sicurezza delle informazioni di Banca Farmafactoring è adottata al fine di proteggere il sistema di gestione delle informazioni da eventi quali minacce o incidenti, esterni e/o interni, oggettivi e/o soggettivi, che possono compromettere l'erogazione dei servizi.

Lo scopo di questo documento è indicare le esigenze, gli obiettivi, le finalità, ed i modelli organizzativi della strategia di sicurezza che Banca Farmafactoring persegue, al fine di orientare lo sviluppo, la gestione, il controllo e la verifica dell'efficacia della sua attuazione.

La dichiarazione della Politica della Sicurezza è riportata nell'Allegato 1.

AMBITO DI APPLICAZIONE

La politica di sicurezza delle informazioni è valida per Banca Farmafactoring, per Banca Farmafactoring S.p.A. – Sucursal em Portugal e per Banca Farmafactoring S.p.A. – Sucursal en España (nonché per le ulteriori eventuali succursali che dovessero successivamente essere stabilite) e si applica a tutte le informazioni trattate dalla Banca, qualsiasi natura e forma esse abbiano o prendano, a tutti i sistemi di gestione e a tutti i supporti di memorizzazione utilizzati per il loro trattamento e la loro conservazione.

I destinatari della politica sono tutti i dipendenti, i collaboratori o i consulenti, a tempo pieno e a tempo determinato. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di Banca Farmafactoring, nonché i clienti. In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni.

SCOPO

In relazione a quanto definito nel documento **06 – SGSI Banca Farmafactoring - Manuale Operativo per la Sicurezza**, la "Politica per la sicurezza delle informazioni" ha l'obiettivo di fornire una direttiva gestionale ed un sostegno per la corretta gestione della sicurezza delle informazioni.

Banca Farmafactoring considera il sistema di gestione e le informazioni gestite parte integrante del proprio patrimonio. È obiettivo di assoluta priorità, salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

In tale contesto, si intende per:

- **Riservatezza** la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati;
- **Integrità** la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico, che sia stata modificata in modo legittimo da soggetti autorizzati e che ne rimanga traccia;

- **Disponibilità** la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura;
- **Autenticità** la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che la ha trasmessa.

Banca Farmafactoring pone a base della politica di tutela delle informazioni, una idonea Analisi dei Rischi di tutte le risorse (*Asset*) che costituiscono il sistema di gestione delle informazioni, al fine di comprendere le vulnerabilità, di valutare le possibili minacce e di predisporre le necessarie contromisure.

La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della politica di sicurezza delle informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI) in linea con la propensione al rischio informatico definito a livello aziendale come definito nel Regolamento di gestione dei rischi.

DOMINI DI SICUREZZA DELLE INFORMAZIONI

La presente Policy di Sicurezza Informatica, ispirandosi agli Standard ISO 27002:2013, descrive le politiche, i principi, le norme di sicurezza e i requisiti di conformità di particolare rilevanza per la Banca, secondo i seguenti domini[1]:

- Politiche di sicurezza;
- Sicurezza delle risorse umane;
- Gestione degli asset aziendali;
- Gestione e controllo degli accessi;
- Sicurezza fisica e ambientale;
- Sicurezza della attività operative;
- Sicurezza delle comunicazioni;
- Acquisizione, sviluppo e manutenzione del Sistema Informativo;
- Relazione con i fornitori;
- Gestione degli incidenti di sicurezza;
- Gestione della continuità operativa.

Un maggior dettaglio delle verifiche della sicurezza e dei controlli è indicato nel documento 06 – SGSI Banca Farmafactoring – Manuale Operativo per la Sicurezza.

[1] Elenco non esaustivo.

OBIETTIVI

Gli obiettivi della Politica della sicurezza delle informazioni che la Banca intende perseguire sono:

- garantire al personale e ai collaboratori un'adeguata conoscenza e un adeguato grado di consapevolezza dei problemi connessi con la sicurezza delle informazioni, al fine di consentire a detti soggetti di acquisire sufficiente coscienza della propria responsabilità in merito al trattamento delle stesse;
- fare in modo che tutti i fornitori esterni abbiano consapevolezza dei problemi di sicurezza delle informazioni della Banca e rispettino la politica di sicurezza adottata;
- stabilire delle linee guida per l'applicazione di standard, di procedure e di sistemi per realizzare il Sistema di Gestione della Sicurezza delle Informazioni (SGSI);
- utilizzare gli standard ISO 27001:2013 "Information Security Management Systems — Requirements" e ISO 27002:2013 "Code of practice for information security management" come linee guida della propria sicurezza delle informazioni e perseguirne la conformità;
- garantire che tutto il personale della Banca abbia consapevolezza delle regole tecniche ed organizzative nell'utilizzo dei sistemi informativi indicate nelle relative procedure di sicurezza implementate appositamente a tale scopo;
- garantire che tutto il personale sia informato della responsabilità nella gestione delle informazioni;
- garantire che tutti i collaboratori siano a conoscenza del "Regolamento generale sulla protezione dei dati" e delle relative implicazioni, nonché delle modalità di applicazione delle misure previste, come richiamato nelle procedure operative di sicurezza.
- garantire che il processo di gestione del rischio informatico adottato dalla Banca sia adeguatamente presidiato e periodicamente aggiornato alla luce dei parametri contemplati all'interno della normativa costituente il SGSI.

  In tale ambito vengono altresì disciplinati i presidi volti a far fronte alle esigenze di controllo e di protezione del rischio tecnologico[2].

REVISIONE E CONTROLLO

L'Amministratore Delegato, coadiuvato dal Responsabile della Sicurezza, è responsabile della revisione periodica della politica affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni.

La revisione sarà fatta periodicamente o in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per la gestione delle informazioni. La Politica della sicurezza revisionata sarà così approvata dal Consiglio di Amministrazione.

La politica per la sicurezza delle informazioni rientra tra i requisiti indicati dalla Banca d'Italia (Capitolo 4, Sezione IV, par. 2 della Circolare di Banca d'Italia n° 285 del 17 dicembre 2013, "Disposizioni di vigilanza per le banche" e successivi aggiornamenti).

[2] Si rinvia per maggiori dettagli al Documento di "Analisi dei rischi".

FIGURE AZIENDALI COINVOLTE NELLA GESTIONE DELLA SICUREZZA

In base a quanto previsto dal Manuale Operativo per la Sicurezza e ai sensi del Regolamento (UE) 2016/679 – *Regolamento generale sulla protezione dei dati*, le tipologie di ruolo da individuare sono:

- Consiglio di Amministrazione;
- Amministratore Delegato;
- Funzione Risk Management;
- Funzione di Compliance e AML;
- U.O. Normativa e Processi;
- Funzione Internal Audit.

Sicurezza e Continuità Operativa:

- Comitato per la Sicurezza delle Informazioni (CSI);
- Responsabile della Sicurezza;
- Responsabile della Continuità Operativa;
- Amministratori di sistema;
- Specialisti della Sicurezza;
- Gruppo di coordinamento per le operazioni di ripristino.

Privacy:

- Titolare del Trattamento
- Delegato del Titolare;
- Coordinatore Privacy;
- Responsabile della Protezione dei Dati;
- Responsabili di Dipartimento/Unità Organizzativa o Owner;
- Responsabili esterni del Trattamento;
- Persone autorizzate al Trattamento;
- Utenti di rete.

Per il dettaglio delle attribuzioni e dei principi generali di sicurezza sull'utilizzo e la gestione del sistema informativo da parte dei profili aziendali sopra richiamati, si rimanda a quanto previsto nella Procedura di Sicurezza PS-6.1.1. Ruoli e Responsabilità.

ORGANIZZAZIONE DELLA SICUREZZA

Al fine di assicurare un'adeguata gestione della sicurezza, la Banca si è dotata di idonee strutture organizzative (cfr. par. sopra; per maggiori dettagli si rimanda alla Procedura di Sicurezza PS-6.1.1 Ruoli e Responsabilità, par. "Modalità Operative" e segg.) per l'identificazione e il controllo delle misure di prevenzione e protezione della riservatezza, dell'integrità e della disponibilità dei dati tramite il Sistema di Gestione della Sicurezza delle Informazioni qui definito.

A garanzia del mantenimento di adeguati livelli di efficienza e di protezione, l'organizzazione della sicurezza e le relative procedure/misure di protezione sono sottoposte ad attività di analisi nell'ambito delle verifiche di pertinenza delle funzioni di controllo interno della Banca.

I sistemi infrastrutturali ed applicativi esternalizzati sono monitorati da referenti interni di volta in volta individuati, che hanno la responsabilità di assicurarsi che i fornitori operino in conformità agli accordi contrattuali e alla normativa applicabile.

Il mancato rispetto delle previsioni contemplate all'interno della presente Policy, nonché nel complessivo SGSI comporta l'assoggettabilità da parte del personale alle responsabilità nascenti dalle condotte perpetrate e può comportare sanzioni che possono arrivare al licenziamento. Per un maggiore dettaglio relativamente a tale regime della responsabilità si rinvia al documento "Linee Guida per la Sicurezza delle Informazioni".

RIFERIMENTI NORMATIVI E STANDARD

Molti aspetti della sicurezza delle informazioni sono normati dalla legislazione italiana e comunitaria; di seguito sono indicate le norme che si ritengono più importanti.

- Risoluzione del Consiglio dell'Unione Europea del 6 dicembre 2001: Approccio comune nel settore della sicurezza delle reti e dell'informazione;
- Raccomandazione del Consiglio dell'Unione Europea del 25 luglio 2002: Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti di informazione;
- Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003: Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del D.lgs. 23 gennaio 2002, n.10.

NORMATIVA SETTORIALE

Circolare di Banca d'Italia n° 285 del 17 dicembre 2013 e s.m.i.

PRIVACY

- Deliberazione del Garante Privacy numero 53 del 23 novembre 2006: "Linee guida in materia di trattamento di dati personali di lavoratori";
- Deliberazione del Garante Privacy numero 13 del 1° marzo 2007: uso delle email e di Internet;
- Provvedimento del Garante Privacy del 13 ottobre 2008: smaltimento e cancellazione sicura dei dati;

- Provvedimento del Garante Privacy del 27 novembre 2008: amministratori di sistema; modificato dal Provvedimento del 25 giugno 2009;
- Provvedimento del Garante Privacy dell'8 aprile 2010: videosorveglianza;
- Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011;
- Articolo 6 del D.L.13 maggio 2011, n.70: "Semestre Europeo - Prime disposizioni urgenti per l'economia - Decreto Sviluppo" convertito in legge, con modificazioni, dall'art. 1, comma 1, L. 12 luglio 2011, n. 106;
- Articolo 40, comma 2, lettera a) e b) del D.L. 6 dicembre 2011, n. 201: "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici", convertito con modificazioni dalla legge 22 dicembre 2011, n.214;
- Articolo 45 del D.L. 9 febbraio 2012, n.5: "Disposizioni urgenti in materia di semplificazione e di sviluppo, convertito in legge, con modificazioni, dall'art. 1, comma 1, L. 4 aprile 2012, n. 35;
- D.lgs. 28-5-2012 n. 69; "Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori".
- Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati).

COMPUTER CRIME

- Legge n. 547 23 dicembre 1993: Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;
- Legge 18/03/2008, n.48: Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica stipulata a Budapest il 23 novembre 2001 e norme di adeguamento dell'ordinamento interno;

DIRITTO D'AUTORE

- L. 22 aprile 1941, n. 633: Protezione del diritto d'autore e di altri diritti connessi al suo esercizio;
- D.lgs. 518/1992: attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore;
- D.lgs. 169/1999: attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati;
- D.lgs. 10 febbraio 2005 n.30: "Codice della proprietà industriale";
- Decreto Ministero dello Sviluppo Economico 13 gennaio 2010 n.33: Regolamento di attuazione del Codice della proprietà industriale.

STANDARD

I principali standard posti base della politica di sicurezza delle informazioni, sono:

- ISO 9001:2008 - Sistemi di Gestione per la Qualità – Requisiti;
- ISO/IEC 73:2009 - Risk management – Vocabulary – Guidelines for use in standards;
- UNI ISO 31000: 2010 - Gestione del rischio – Principi e linee guida;
- 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".

USO DEI SISTEMI DI ELABORAZIONE DELL'INFORMAZIONE

Banca Farmafactoring considera i sistemi di elaborazione delle informazioni, come strumenti di lavoro per tutte le persone che operano in azienda a qualunque livello.

Gli strumenti messi a disposizione devono essere utilizzati per lo svolgimento dell'attività lavorativa in modo strettamente pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi stessi e della rete.

Banca Farmafactoring perseguirà a norma di legge e del vigente contratto di lavoro il collaboratore che utilizza in modo non appropriato i sistemi di elaborazione delle informazioni.

VERIFICHE DI SICUREZZA E CONTROLLI STRUMENTAZIONI

Per verificare il corretto utilizzo di tutte le strumentazioni informatiche messe a disposizione degli utenti, Banca Farmafactoring effettua dei test di verifica sia delle misure minime di sicurezza che test approfonditi per verificare la vulnerabilità dei propri *Asset* (es. *Vulnerability Assessment, Penetration test*). Il maggior dettaglio delle verifiche della sicurezza e dei controlli è indicato nel "06 – SGSI Farmafactoring – Manuale Operativo per la Sicurezza".

La Banca, con frequenza regolare, effettua delle prove di continuità operativa e di Disaster Recovery per riesaminare l'efficacia e l'efficienza dei propri piani.

ORGANIZZAZIONE E RESPONSABILITÀ DELLA SICUREZZA

L'organizzazione della sicurezza è descritta nel documento "06 – SGSI Farmafactoring – Manuale Operativo per la Sicurezza" al Capitolo 6 "Organizzazione della Sicurezza" e nella Procedura di sicurezza PS-6.1.1 Ruoli e responsabilità.

Il Consiglio di Amministrazione è il responsabile dei contenuti della politica di sicurezza delle informazioni, della sua emanazione, della sua attuazione e del suo aggiornamento.

Il Consiglio di Amministrazione si avvale del supporto tecnico ed organizzativo del Comitato per la Sicurezza delle Informazioni (CSI) e del Responsabile della Sicurezza; quest'ultimo è supportato dal Gruppo di coordinamento per le operazioni di ripristino e dagli Specialisti della Sicurezza ed Amministratori di sistema (ruoli e responsabilità sono indicate nella procedura sicurezza PS-6.1.1).

Le principali attività in carico al Responsabile della Sicurezza sono quelle di vigilare sulla corretta implementazione e sul corretto mantenimento nel tempo del Sistema di Gestione della Sicurezza delle Informazioni, di promuovere e di coordinare l'attività di analisi dei rischi, di gestire i rapporti con gli operatori delle telecomunicazioni e con i fornitori di servizi rilevanti, nonché di verificare annualmente la validità del Piano di continuità operativa e di Disaster Recovery.

COMUNICAZIONE, FORMAZIONE E SENSIBILIZZAZIONE DEGLI UTENTI

La Politica della Sicurezza è divulgata a tutto il personale, ai collaboratori, ai clienti e ai fornitori attraverso il sito internet istituzionale.

Il Responsabile della Sicurezza attraverso opportune sessioni informative e formative sensibilizza gli utenti interni ad una corretta applicazione delle procedure della sicurezza delle informazioni, stimolando gli stessi a collaborare fattivamente per una gestione sempre più coordinata ed esaustiva di tale tematica.

ALLEGATO 1

A tutti i Responsabili delle funzioni aziendali

e p.c. a tutto il Personale

OGGETTO: Politica per la sicurezza delle informazioni

Le informazioni costituiscono parte integrante del patrimonio della Banca.

Le attuali tecnologie favoriscono la diffusione e l'utilizzo delle stesse, ma espongono la Banca a nuovi rischi, come frodi e spionaggio informatico, che rendono la sicurezza delle informazioni un obiettivo strategico da perseguire nel tempo per preservare il vantaggio competitivo acquisito.

Il documento costituisce direttiva e linea guida per l'istituzione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e per ogni successivo atto o misura finalizzati a garantire la riservatezza, l'integrità e la disponibilità delle informazioni.

Il Sistema di Gestione della Sicurezza delle Informazioni recepisce i migliori standard internazionali nonché garantisce il rispetto delle normative nazionali e di settore.

In quest'ottica, la Banca adotta al suo interno un modello organizzativo per la sicurezza delle informazioni, istituendo un Comitato per la Sicurezza, nominando un Responsabile della Sicurezza e predisponendo le Procedure di Sicurezza ed i controlli necessari affinché l'intera organizzazione possa trattare in modo sicuro tutto il patrimonio informativo a disposizione, sia esso derivante da fonti interne o esterne.

Gli obiettivi che la Banca intende perseguire sono di garantire al personale ed ai collaboratori una adeguata conoscenza e un adeguato grado di consapevolezza dei problemi connessi con la sicurezza dell'informazione, al fine di acquisire sufficiente coscienza delle loro responsabilità in merito al suo trattamento; di accertare che tutti i fornitori esterni abbiano consapevolezza dei problemi di sicurezza delle informazioni della Banca e rispettino la politica di sicurezza adottata; di stabilire delle linee guida per l'applicazione di standard, procedure e sistemi per realizzare il Sistema di Gestione della Sicurezza delle Informazioni (SGSI); di garantire che tutto il personale sia informato delle proprie responsabilità nella gestione delle informazioni.

Tutto il personale è tenuto fin d'ora a conoscere e rispettare il modello organizzativo e le Procedure di Sicurezza, adeguandosi a quanto stabilito durante lo svolgimento delle proprie mansioni. In particolare, il personale dovrà poter accedere alle sole informazioni e alle sole funzioni indispensabili per il corretto svolgimento dei propri compiti e delle proprie mansioni. L'accesso ai beni informativi è subordinato all'ottenimento di un'esplicita autorizzazione, in mancanza della quale non è possibile permettere l'accesso. L'accesso alla Banca da parte di personale esterno deve essere controllato e vigilato secondo quanto previsto nell'apposita Procedure di Sicurezza.