Azienda Farmacie e Servizi S.p.A. Sesto Fiorentino
FARMACIE COMUNALI

AFS SPA V. CAVALLOTTI, 46 SESTO F.NO

DLgs.231/01MOD.ORG.vo GEST.le&CONTROLLO

ALLEGATO 02

AZIENDA FARMACIE E SERVIZI S.P.A.

D. LGS. 8 GIUGNO 2001, N.231

REATI INFORMATICI

Approvato dall'Amministratore Unico
con Determina N° 29 del 15/09/2018

PARTE SPECIALE

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI art. 24 bis

Questa categoria di reati trova il suo presupposto nella gestione ed utilizzo dei sistema informato aziendale e nel trattamento dei dati recepiti in occasione dell'esercizio dell'attività aziendale.
Nell'ambito della Società sono considerate funzioni a rischio reato tutte le aree aziendali che utilizzano sistemi informatici e che recepiscono dati.

01) Frode informatica: prevista dall'art. 640-*ter* c.p., 2° comma, e costituita dalla condotta di chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a esso pertinenti, procura a sé o ad altri un ingiusto profitto con danno dello Stato o di altro ente pubblico;

02) Accesso abusivo ad un sistema informatico o telematico: previsto dall'art. 615 - *ter* c.p. e costituito dalla condotta di chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo;

03) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici: prevista dall'art. 615 – *quater* c.p. e costituita dalla condotta di chi, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico protetto da misure di sicurezza o comunque fornisce indicazioni o istruzioni idonee al predetto scopo;

04) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico: prevista dall'art. 615 – *quinquies* c.p. e costituita dalla condotta di chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici;

05) Intercettazione, impedimento o interruzione illecita di comunicazione informatiche o telematiche: prevista dall'art. 617 - *quater*. c.p. e costituita dalla condotta di chi fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o le interrompe;

06) Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche: prevista dall'art. 617 – *quinquies* c.p. e costituita dalla condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;

07) Danneggiamento di informazioni, dati e programmi informatici: previsto dall'art. 635-*bis* c.p. e costituito, salvo che il fatto costituisca più grave reato, dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui;

08) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità: previsto dall'art. 635 – *ter* c.p. e costituito, salvo che il fatto costituisca più grave reato, dalla condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o

comunque di pubblica utilità;

09) ***Danneggiamento di sistemi informatici o telematici***: previsto dall'art. 635 – *quater* c.p. e costituito, salvo che il fatto costituisca più grave reato, dalla condotta di chi, tramite condotte di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati e programmi informatici altrui o con l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende in tutto o in parte inservibili i sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento;

10) ***Danneggiamento di sistemi informatici o telematici di pubblica utilità:*** previsto dall'art. 635-*quinquies* c.p. ed integrato se il danneggiamento di sistemi telematici o informatici è diretto a distruggere, a danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o tematici di pubblica utilità o ad ostacolarne gravemente il funzionamento;

11) ***Frode informatica del soggetto che presta servizi di certificazione di firma elettronica:*** prevista dall'art**.** 640-*quinquies* c.p. e costituita dalla condotta del soggetto che presta servizi di certificazione di firma elettronica che, per procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato;

In base all'art. 491-*bis* c.p. le fattispecie di reato di Falsità in atti si applicano anche ai documenti informatici pubblici e privati aventi efficacia probatoria come se si trattasse di atti pubblici o scritture private.

FUNZIONE DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere, nell'ambito della gestione ed utilizzo di sistemi informatici e nel trattamento dei dati, dai Dipendenti e dagli Organi Societari, nonché dai suoi Collaboratori Esterni e Partner, come già definiti nella Parte Generale.

L'obiettivo che si intende perseguire è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto nel Codice Etico e dalle regole sopra descritte al fine di prevenire il verificarsi dei reati.

1. Nello specifico, il presente Parte Speciale ha lo scopo di:

a) indicare i principi che informano le procedure che i Dipendenti, Organi Societari, Collaboratori Esterni e Partner della Società sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo, come già definito nella Parte Generale, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

Le regole e i principi generali di comportamento, nonché le procedure specifiche disciplinati nel presente paragrafo richiamano, focalizzandoli ai fini della prevenzione dei delitti informatici e del trattamento illecito dei dati ed integrandoli, quelli previsti nel Codice Etico e nelle procedure aziendali interne, a suo tempo adottati dalla Società ed attualmente in vigore, quali individuati nella Parte Generale del presente Modello.

2.Gestione della Sicurezza informatica ed Aree Sensibili.

Devono essere definiti e monitorati criteri di assegnazione degli strumenti di firma di documenti informatici aziendali.

Nell'ambito delle regole aziendali per la gestione della Sicurezza Informatica devono essere fornite precise e chiare indicazioni su:

i riferimenti di tutti coloro che a vario titolo accedono all'interno del sistema informatico aziendale, ivi compresi i soggetti esterni;

a) limiti di utilizzo del Personal Computer e delle risorse di rete da parte di ciascun dipendente;

b) divieto di installazione personale di *software* sui *personal computer* di ciascun dipendente, ma solo tramite intervento degli addetti al sistema informatico;

c) indicazioni specifiche circa l'uso di codici di accesso e loro modalità di conservazione;

d) modalità di distribuzione di codici di accesso ai siti della PA.

- Sono previste modalità di utilizzo del sistema informatico basate su adeguato riscontro delle *password* di abilitazione per l'accesso ai sistemi informativi della P.A. eventualmente posseduti da determinati dipendenti appartenenti a specifiche funzioni o strutture aziendali.
- E' prevista la dotazione di opportuni programmi antivirus il cui funzionamento e la corretta applicazione dovrebbe essere tolta al libero arbitrio dei singoli dipendenti (aggiornamenti periodici);
- Devono essere verificati i livelli di permission concessi a tutti coloro che operano all'interno Sistemi informativi e che hanno accesso a sistemi, applicativi o apparati di comunicazione elettronica al fine di evitare operazioni di controllo e/o tracciamento illecito di dati.
- Devono essere effettuate delle analisi periodiche sulle installazioni presenti in azienda, con particolare attenzione a tutti gli strumenti che possono attuare un controllo e/o un tracciamento di dati.

La suddetta relazione deve essere inviata all'OdV.