AIFA AGENZIA ITALIANA DEL FARMACO	**DOCUMENTO DELLA QUALITA'**	Settore Information Communication Technology
		DSQ/032

DISCIPLINARE INTERNO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DELL'AIFA

REDAZIONE	DIR/SETTORE ICT	Firma	TRAPANESE MAURIZIO AIFA - AGENZIA ITALIANA DEL FARMACO Dirigente Amministrativo 28.12.2021 09:53:26 GMT+00:00	Data
PRESA VISIONE	RAQ	Firma	MARTUSCIELLO PAOLO AIFA - AGENZIA ITALIANA DEL FARMACO Dirigente Amministrativo 28.12.2021 11:37:39 UTC	Data
APPROVAZIONE	DG	Firma	MAGRINI NICOLA AIFA - AGENZIA ITALIANA DEL FARMACO 2.10.3.1 Direttore 30.12.2021 09:45:58 GMT+00:00	Data

Sommario

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete Internet dai PC fissi e portatili e dai dispositivi mobili, espone l'Agenzia Italiana del Farmaco (di seguito AIFA, Agenzia o Ente), i dipendenti, i collaboratori nonché gli utenti dei servizi offerti dall'Ente, a rischi derivanti dalla perdita totale o parziale della riservatezza, integrità e disponibilità del Sistema Informatico dell'AIFA e dei dati in esso contenuti.

Pertanto, al fine di mitigare tali rischi in relazione a eventuali comportamenti non idonei attuati da parte degli utilizzatori del Sistema Informatico dell'AIFA, che potrebbero comportare danni, anche patrimoniali o d'immagine, nonché sanzioni derivanti da violazioni di specifiche disposizioni di legge (ad es. sul diritto d'autore e sulla privacy), l'Ente ha deciso di adottare un Disciplinare interno. Tale Disciplinare è redatto in conformità alla Politica per la Sicurezza delle Informazioni dell'Agenzia, in armonia con il Codice di Comportamento dell'Agenzia Italiana del Farmaco e in ottemperanza al principio di responsabilizzazione del Titolare del Trattamento di dati personali enunciato dal Regolamento UE n. 2016/679 (di seguito anche GDPR).

Le regole contenute nel presente Disciplinare, si aggiungono ed integrano le specifiche istruzioni fornite al personale che opera per l'AIFA da parte del Responsabile dell'Area/Settore o del Responsabile dell'Ufficio, in attuazione della normativa vigente per il trattamento dei dati personali, e completano le informazioni già fornite ai suddetti interessati in ordine alle modalità con cui potranno effettuarsi i necessari controlli o ai provvedimenti disciplinari conseguenti alle violazioni.

Titolo I: Introduzione

Art. 1 Oggetto del documento

1. Il presente Disciplinare individua le regole per l'accesso e l'utilizzo del Sistema informatico dell'AIFA, per l'efficace svolgimento dei propri scopi istituzionali e dei servizi informatici ad essi correlati.
2. Il comportamento dell'utilizzatore del Sistema informatico dell'AIFA deve essere orientato agli scopi istituzionali dell'Ente.
3. Le regole riportate nel presente Disciplinare sono da intendersi come un insieme di misure minime, la cui osservanza contribuisce a ridurre i rischi correlati alla perdita totale o parziale della riservatezza, integrità e disponibilità del Sistema Informatico dell'AIFA e dei dati in esso contenuti, derivanti da comportamenti non idonei perpetrati da parte degli utilizzatori del suddetto Sistema Informatico.
4. L'accesso e l'utilizzo del Sistema informatico dell'AIFA è consentito solo nel pieno rispetto del presente Disciplinare, al fine di evitare possibili danni erariali, finanziari e di immagine all'Agenzia.
5. Gli utilizzatori del Sistema Informatico dell'AIFA sono tenuti a contattare il Responsabile della Sicurezza delle Informazioni dell'Agenzia, prima di intraprendere qualsiasi attività non esplicitamente ricompresa nelle disposizioni del presente Disciplinare, al fine di garantire che tali attività non siano in contrasto con le politiche di sicurezza informatica stabilite dall'Ente.

Art. 2 Ambito di applicazione

1. Il presente Disciplinare si applica a tutti gli utilizzatori del Sistema Informatico dell'AIFA, così come individuati all'Art. 3 let. a), n) e x).
2. Il presente Disciplinare viene pubblicato sul sito istituzionale dell'AIFA, nell'apposita sezione "*Amministrazione trasparente» Disposizioni generali » Atti generali » Atti amministrativi generali*".
3. L'Agenzia, contestualmente alla sottoscrizione del contratto di lavoro o, in mancanza, all'atto di conferimento dell'incarico, consegna e fa sottoscrivere ai nuovi assunti, con rapporti comunque denominati, copia del presente Disciplinare.

Art. 3 Definizioni

1. Ai fini dell'applicazione del presente Disciplinare deve intendersi:
   a) **Amministratore del sistema**: la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché alla protezione dei dati, quali l'amministratore di basi di dati, l'amministratore di reti e di apparati di sicurezza e l'amministratore di sistemi software complessi[1].
   b) **Archivio di rete**: le cartelle condivise nella rete locale o sui cloud di AIFA per la memorizzazione di informazioni in formato digitale a scopo esclusivamente lavorativo.

1 Definizione ai sensi del Provvedimento del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i. del 27/11/2008.

c) **Amministratore Utenze Aziendali** (di seguito **AUA):** referente nominato dalle Organizzazioni che, in qualità di Utenti di cui alla let. x) del presente articolo, interagiscono con AIFA (Azienda farmaceutica, Regione, Comitato etico, ecc..) tramite i servizi online messi a disposizione dall'Ente. L'AUA autorizza/revoca gli utenti della propria organizzazione, ad accedere ad una o più applicazioni dell'AIFA.

d) **Bring Your Own Device** (di seguito **BYOD**): qualsiasi dispositivo elettronico di proprietà, a noleggio o gestito da un Operatore dell'AIFA, in grado di memorizzare dati e di connettersi ad una rete, inclusi, a titolo esemplificativo e non esaustivo, i telefoni cellulari, smartphone, tablet, computer portatili, PC e netbook.

e) **Cartella di lavoro dell'Operatore**: la cartella denominata "Documenti" in cui sono memorizzati i documenti informatici relativi all'attività dell'Operatore.

f) **Casella di posta elettronica personale**: la casella di posta elettronica istituzionale assegnata agli Operatori dell'AIFA.

g) **Casella di posta elettronica di servizio**: la casella di posta elettronica istituzionale assegnata alle strutture o ai servizi.

h) **Casella di posta elettronica certificata**: la casella di posta elettronica certificata dell'Agenzia, della struttura o del servizio.

i) **Comunicazioni esterne**: le comunicazioni esterne al dominio di posta elettronica dell'AIFA.

j) **Dati personali**: dati personali ai sensi del GDPR.

k) **Dispositivi mobili**: qualsiasi dispositivo elettronico utilizzabile seguendo la mobilità dell'utente quali, a titolo esemplificativo e non esaustivo, telefoni cellulari, palmari, smartphone, tablet, laptop, ecc.

l) **Messaggio di posta elettronica**: messaggio inviato/ricevuto da una casella di posta elettronica personale/di servizio o attraverso un applicativo che utilizza un server e-mail.

m) **Mobile Device Management** (di seguito **MDM**): soluzione software per la gestione, il supporto, la protezione e il monitoraggio dei dispositivi mobili.

n) **Operatore**: il dipendente e il collaboratore (lavoratore parasubordinati, lavoratore somministrato, lavoratore in stage, ecc.) espressamente autorizzato dall'AIFA ad accedere ed utilizzare i sistemi informatici e telematici dell'AIFA.

o) **Rete telematica dell'Agenzia**, nel seguito semplicemente la **Rete**, l'infrastruttura fisica e logica che permette l'interconnessione degli apparati dell'Agenzia, per la trasmissione dati fra loro e con la rete Internet.

p) **Servizi informatici** si intendono:
   - posta elettronica;
   - accesso alla rete locale LAN (o Intranet);
   - accesso e navigazione Internet;
   - ogni altra applicazione informatica che l'Agenzia rende disponibile agli Operatori e agli Utenti.

q) **Sistema informatico dell'AIFA**: l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, personal computer, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'AIFA.

r) **Smartphone**: il dispositivo portatile che abbina funzionalità di gestione di dati personali e di telefono.

s) **Social Network Sites** (di seguito SNS - Sito di Social Network): servizi web (social network, newsletter, mailing list, forum, instant messaging, wiki, etc.) utilizzati per creare e mantenere reti virtuali e comunità on-line costituite da gruppi di persone che si relazionano tra loro da un qualsiasi tipo di legame (amicizia, di interessi, lavorativo, etc.). L'AIFA utilizza i SNS per comunicare con target di utenti spesso non raggiungibili con i servizi tradizionali, informare e far partecipare i cittadini alla vita istituzionale dell'Agenzia nonché per dialogare con le altre amministrazioni pubbliche presenti sui SNS.

t) **PEC**: è un sistema di comunicazione quale la posta elettronica ordinaria, a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere ai messaggi un valore legale equiparato alla Posta Raccomandata con ricevuta di ritorno (A/R). Il valore legale è assicurato dai gestori del servizio PEC del mittente e del destinatario, per le sole comunicazioni inviate da una casella PEC e ricevute da un'altra casella PEC, che certificano:
   - data e ora dell'invio del messaggio da parte del mittente;
   - data e ora dell'avvenuta consegna del messaggio al destinatario;
   - integrità del messaggio (ed eventuali allegati) nella trasmissione da mittente a destinatario.

   Le caselle PEC dell'Agenzia sono, di norma, integrate nel sistema di protocollo informatico.

u) **Rischio Informatico**: è la probabilità che minacce di natura accidentale o dolosa, sfruttino le vulnerabilità intrinseche di una risorsa informatica e quindi causare danni di varia natura (economici, reputazionali, ecc.) ad un'Organizzazione.

v) **Settore ICT**: Settore Information and Communication Technology di AIFA.

w) **SPID**: Sistema Pubblico d'Identità Digitale. Rappresenta, tramite un'unica credenziale, l'identità digitale e personale di ogni cittadino, con cui è riconosciuto dalla Pubblica Amministrazione per utilizzare in maniera personalizzata e sicura i servizi digitali messi a disposizione dalle amministrazioni centrali e locali.

x) **Utente**: il soggetto pubblico e privato esterno all'AIFA che ha con l'Agenzia rapporti diversi dall'Operatore, espressamente autorizzato ad accedere e utilizzare i sistemi informatici e telematici dell'Ente.

y) **Wi-Fi**: è una tecnologia di reti wireless che consente a dispositivi come computer fissi, dispositivi mobili e altre apparecchiature (es. stampanti e videocamere) di interfacciarsi con Internet.

Art. 4 Competenze e responsabilità

1. Per quanto concerne le responsabilità afferenti ai ruoli citati nel presente documento, nonché alla relazione tra tali i ruoli e l'organizzazione dell'AIFA, si faccia riferimento a quanto previsto nella Politica per la Sicurezza delle Informazioni di AIFA e in generale nelle politiche di sicurezza emesse dall'Ente.

Art. 5 Principi generali

1. I rapporti e i comportamenti, a tutti i livelli organizzativi, sono improntati ai principi di onestà, correttezza, trasparenza, riservatezza, imparzialità, diligenza, lealtà e reciproco rispetto.
2. I trattamenti dei dati personali effettuati durante l'accesso alla Rete e l'utilizzo del Sistema Informatico dell'AIFA, devono inoltre rispettare quanto previsto dalle normative vigenti in materia di protezione dei dati e svolgersi nell'osservanza dei seguenti principi cogenti:
   a) il **principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (artt. 5 e 6 del GDPR). Deve essere quindi garantito, per impostazione predefinita, che siano trattati solo i dati personali necessari per ciascuna finalità del trattamento (obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi (Privacy by default art. 25, comma 2 del GDPR); tutte le informazioni saranno comunque censite in un apposito Registro delle attività di trattamento effettuate dall'organizzazione (art. 30 del GDPR).
   b) i principi di **correttezza e trasparenza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 12 del GDPR). Le tecnologie dell'informazione (in modo più marcato rispetto alle apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa; ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati. I dati personali saranno trattati quindi in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5 del GDPR) nel rispetto degli obblighi di cooperazione con l'autorità di controllo quando questa ne faccia richiesta (art. 31 del GDPR).
   c) i trattamenti di dati personali devono essere effettuati per finalità determinate, esplicite e legittime, osservando il **principio di pertinenza** e non eccedenza, ovvero di limitazione delle finalità e minimizzazione dei dati (art. 5, comma 1 lett. b) e c) del GDPR). Il datore di lavoro deve trattare i dati "*nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza*" (Parere 8 giugno 2017 del EDPB[2] in merito al trattamento dei dati personali dei lavoratori, che ha integrato quanto già previsto in passato con il Parere n. 8/2001[3] ed il "Documento di lavoro sulla

2 Comitato europeo per la protezione dei dati (EDPB): è l'organismo che ha sostituito il Gruppo di lavoro articolo 29 (Working Party article 29 o WP29, appunto perché previsto dall'art. 29 della direttiva europea 95/46), col nuovo regolamento europeo, ed è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.

3 Parere n. 8/2001: Parere sul trattamento di dati personali nell'ambito dei rapporti di lavoro.

sorveglianza delle comunicazioni elettroniche sul luogo di lavoro" del 2002 del Garante per la protezione dei dati personali sul trattamento di dati personali nell'ambito dei rapporti di lavoro. I dati devono quindi essere: adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità (art. 5 del GDPR), e comunque da trattare in modo da garantirne **un'adeguata sicurezza** (artt. 24 e 32 del GDPR). Quando la violazione della sicurezza dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il datore di lavoro deve darne notizia all'interessato senza ingiustificato ritardo (art. 34 del GDPR).

d) il datore di lavoro deve distinguere i casi in cui per eseguire un trattamento di dati personali è richiesto il (previo) **consenso** dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il datore di lavoro deve essere in grado di dimostrare che il consenso è stato effettivamente prestato (artt. 6 e 7 del GDPR). Per quanto riguarda l'**informativa** invece, il datore di lavoro deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo (artt. 13 e 14 del GDPR).

e) il datore di lavoro, per procedere al trattamento dei dati personali, deve rispettare il diritto dell'Interessato a non essere sottoposto ad una decisione basata unicamente su un **trattamento automatizzato** dei dati che produca effetti che incidano significativamente sulla sua persona (art. 22 del GDPR); deve inoltre rispettare **i diritti degli interessati** in termini di accesso, rettifica, cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto di opposizione al trattamento (ove il datore di lavoro non dimostri l'esistenza di motivi legittimi cogenti), con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul datore di lavoro (artt. 15-21 del GDPR).

3. In relazione alla tutela del diritto d'autore e all'utilizzo del software e dei prodotti informatici, devono essere rispettate tutte le misure atte ad assicurare un utilizzo delle risorse conforme alle disposizioni normative che tutelano il copyright, i brevetti e la proprietà intellettuale, ai sensi della Legge 22 aprile 1941 n.633 e s.m.i.[4]. Pertanto, tutti gli Operatori e Utenti che usufruiscono del Sistema Informatico dell'AIFA devono utilizzare il software installato sulla postazione lavorativa (PC o dispositivi mobili) o disponibile attraverso la rete LAN, nel rispetto dei termini contrattuali e/o delle licenze in concessione d'uso, osservandone attentamente le limitazioni relative, ad esempio, al numero di copie riproducibili, al numero di utenti fruitori ed alle scadenze temporali delle concessioni.

Art. 6 Titolarità delle risorse informatiche

1. L'AIFA è titolare di tutte le risorse informatiche dell'Ente. Gli Operatori egli Utenti devono essere informati su quali siano gli usi consentiti e proibiti di tali risorse.
2. Ogni infrazione alle regole di cui al presente Disciplinare costituisce una violazione della sicurezza ed esporrà l'Operatore e gli Utenti ai provvedimenti previsti in tali casi, come meglio esplicitato all'Art. 51 del presente Disciplinare.

4 Legge 22 aprile 1941 n.633 : "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" e successive modifiche e integrazioni, in particolare D.lgs. n.8 del 15 gennaio 2016: Disposizioni in materia di depenalizzazione.

Titolo II: Norme per l'accesso al Sistema Informatico

Art. 7 Disposizioni generali

1. Gli Operatori e Utenti possono accedere al Sistema informatico dell'AIFA esclusivamente per lo svolgimento delle mansioni lavorative/incarichi ad essi affidati, in forza di un contratto o altro accordo in essere con AIFA, ed esclusivamente per scopi leciti.
2. Gli Operatori e Utenti possono accedere al Sistema Informatico dell'AIFA solo previa autorizzazione del Responsabile del Sistema Informatico, tramite credenziali di autenticazione (es. *username* e *password)* o altri metodi di autenticazione "forte", quali la Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE) e SPID.
3. La gestione delle credenziali di accesso deve essere conforme a quanto indicato nella specifica documentazione emessa dall'AIFA[5].
4. Gli Operatori e gli eventuali Utenti non possono cedere a soggetti terzi, le loro credenziali di accesso al Sistema informatico dell'AIFA.
5. Gli Operatori e gli Utenti possono accedere al Sistema informatico dell'AIFA, anche tramite la rete wi-fi dedicata, mediante le credenziali loro assegnate dal Responsabile del Sistema Informatico o persone da lui delegate, utilizzando i PC in dotazione dell'AIFA appositamente predisposti ovvero utilizzando proprie attrezzature preventivamente autorizzate dal Responsabile del Sistema Informatico.
6. Gli Operatori e gli Utenti si impegnano ad evitare pratiche che possono esporre l'AIFA a rischi informatici (es. possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche di proprietà dell'Ente). Laddove tali pratiche non siano evitabili, gli Operatori e gli Utenti si impegnano ad adottare comportamenti tesi a minimizzare tali rischi.
7. Gli Operatori e gli Utenti sono tenuti a segnalare presunte o accertate violazioni alla sicurezza delle risorse informatiche dell'Ente, al Responsabile del Sistema Informatico o persona da lui delegata e per conoscenza al Responsabile della Sicurezza delle Informazioni e al Responsabile dell'Ufficio.
8. Gli strumenti adottati per l'accesso Sistema informatico dell'AIFA, sono di uso strettamente personale e pertanto l'Operatore o gli Utenti sono tenuti a custodirli in modo appropriato, al fine di garantirne la riservatezza e l'integrità.
9. L'AIFA si riserva di applicare specifiche clausole contrattuali o adottare accordi di riservatezza con gli Operatori e Utenti del Sistema Informatico, per garantire la riservatezza e la non-divulgazione delle informazioni critiche di AIFA, secondo quanto previsto dalle normative vigenti. Tali accordi, devono necessariamente contemplare tutti i requisiti necessari ad assicurare la protezione del Sistema Informatico dell'AIFA.

[5] Politica "Gestione delle Utenze".

Art. 8 Attribuzione delle credenziali e dei profili di accesso

1. Il Settore Risorse Umane dell'AIFA comunica al Responsabile del Sistema Informatico, entro il 31 gennaio di ogni anno, l'elenco ufficiale del personale dipendente e dei lavoratori parasubordinati. Tale comunicazione viene effettuata anche contestualmente all'assunzione o alla cessazione del rapporto di lavoro del personale dipendente e dei lavoratori parasubordinati.
2. Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio richiedono al Responsabile del Sistema Informatico la modifica del profilo di accesso da assegnare ai propri dipendenti e i lavoratori parasubordinati di cui al comma 1 del presente articolo, coerentemente con quanto disposto nella specifica documentazione emessa dall'AIFA5.
3. Il Responsabile del Sistema Informatico provvede alla generazione delle credenziali utente associate ai dipendenti e i lavoratori parasubordinati di cui al comma 1 del presente articolo, e all'assegnazione del profilo di accesso, in base di quanto richiesto dal Settore Risorse Umane o dal Responsabile dell'Area/Settore o il Responsabile dell'Ufficio.
4. Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio richiedono l'attivazione e la modifica delle credenziali per tutte le altre categorie di Operatori non ricomprese al comma 1 del presente articolo, nonché il profilo di accesso da assegnare, coerentemente con quanto disposto nella specifica documentazione emessa dall'AIFA5
5. Il Responsabile del Sistema Informatico provvede alla generazione delle credenziali utente associate a tutte le altre categorie di Operatori non ricomprese al comma 1 del presente articolo e all'assegnazione del relativo profilo di accesso, in base di quanto richiesto dal Responsabile dell'Area/Settore o dal Responsabile dell'Ufficio.
6. L'AUA provvede ad abilitare le credenziali utente associate agli Utenti della propria Organizzazione.
7. Nell'ambito delle credenziali di accesso, la *username* attribuita dal Responsabile del Sistema Informatico è immodificabile.
8. All'atto del primo accesso al Sistema informatico dell'AIFA (*login*), con le credenziali di autenticazione, l'Operatore o l'eventuale Utente così come definito alla let. x) dell'Art. 3, deve obbligatoriamente modificare la *password* comunicatagli dal Responsabile del Sistema Informatico con una nuova *password* personale, che dovrà mantenere segreta e custodire con la massima diligenza.
9. Le *password* successive alla prima assegnata dal Responsabile del Sistema Informatico, deve essere creata esclusivamente dall'Operatore o dall'eventuale Utente, assegnatario dell'account.
10. Nessuno è autorizzato a richiedere ad un Operatore o ad un eventuale Utente la propria *username* e *password* ed ognuno di questi deve mantenere segrete le proprie credenziali di accesso.
11. Nell'utilizzo del Sistema informatico dell'AIFA ogni Operatore o Utente è identificato univocamente dalle proprie credenziali, che vengono tracciate dai vari servizi informatici (es. navigazione web, accesso a risorse condivise).
12. L'Operatore e l'eventuale Utente sono considerati gli unici responsabili dell'attività espletata tramite la propria username, la propria CNS, la propria CIE e le proprie credenziali

SPID; vige a tal fine una presunzione di corrispondenza tra l'Operatore/Utente e *username* e, laddove applicabile, la CNS, la CIE o SPID.

Art. 9 Gestione delle Password

1. Le password devono osservare le regole disposte dall'AIFA (es. lunghezza, regole di composizione, ciclo di vita, termini di scadenza, blocco automatico utenza) nella specifica documentazione emessa dall'Ente5.
2. Nel caso in cui l'Operatore o l'Utente sospetti che la propria password o quella di un altro Operatore/Utente abbia perso il requisito essenziale della segretezza, deve segnalare l'evento come possibile violazione della sicurezza informatica di cui all'Art. 7.

Art. 10 Sospensione delle credenziali

1. Il Responsabile del Settore Risorse Umane richiede la sospensione[6] delle credenziali per il personale dipendente e per i lavoratori parasubordinati, coerentemente con quanto disposto nella specifica documentazione emessa dall'AIFA5.
2. Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio, per il tramite dell'AUA, se presente, richiedono la sospensione[7] delle credenziali per gli Utenti così come definiti all'art. 3 let. x), coerentemente con quanto disposto nella specifica documentazione emessa dall'AIFA5.
3. La sospensione[8] delle credenziali di autenticazione viene effettuata dal Responsabile del Sistema Informatico, ogni qualvolta si ipotizzi un rischio di accessi illeciti o di compromissione della *password*, sia necessario per garantire la sicurezza del Sistema informatico dell'AIFA, nonché in relazione a quanto previsto all'Art. 15 del presente Disciplinare. Tale operazione avviene conformemente a quanto previsto nella specifica documentazione emessa dall'Ente5.
4. La revoca della sospensione delle credenziali viene effettuata dal Responsabile del Sistema Informatico su richiesta del Responsabile del Settore Risorse Umane per il personale dipendente e per i lavoratori parasubordinati ovvero del Responsabile dell'Area/Settore o il Responsabile dell'Ufficio per gli Utenti di cui all'art. 3 let. x).

Art. 11 Disattivazione delle credenziali

1. La disattivazione delle credenziali di autenticazione non utilizzate da almeno 90 giorni, viene garantita dal Responsabile del Sistema Informatico attraverso un meccanismo automatico, coerentemente con quanto disposto nella specifica documentazione emessa dall'Ente5.
2. Il Responsabile del Sistema Informatico, al momento della cessazione del rapporto di lavoro di un dipendente o di un lavoratore parasubordinato, comunicata dal Settore Risorse Umane, disattiva tempestivamente tutte le utenze associate allo stesso.
3. Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio richiede, al Responsabile del Sistema Informatico, la disattivazione delle credenziali per tutte le altre categorie di

[6] Si intende la disattivazione temporanea delle credenziali di autenticazione, in maniera tale che non sia possibile utilizzarle per effettuare sessioni di identificazione ed autenticazione (login).

[7] Si intende la disattivazione temporanea delle credenziali di autenticazione, in maniera tale che non sia possibile utilizzarle per effettuare sessioni di identificazione ed autenticazione (login).

[8] Si intende la disattivazione temporanea delle credenziali di autenticazione, in maniera tale che non sia possibile utilizzarle per effettuare sessioni di identificazione ed autenticazione (login).

Operatori non regolamentate al comma 2 del presente articolo, coerentemente con quanto disposto nella specifica documentazione emessa dall'AIFA5. Il Responsabile del Sistema Informatico disattiverà tempestivamente tutte le utenze associate.

4. L'AUA provvede a disabilitare le credenziali utente associate agli Utenti della propria Organizzazione, nel momento in cui non sussistano più le condizioni per il mantenimento dei delle credenziali utente e/o dei relativi profili autorizzativi (es. cambio di ruolo o mutamento delle mansioni svolte dal titolare dell'utenza, dimissioni).
5. Prima della disattivazione della casella di posta elettronica associata ai soggetti di cui al comma 2 del presente articolo, sarà possibile concordare con il Responsabile del Sistema Informatico l'eventuale invio di un messaggio di posta elettronica automatico, valido per un periodo di 30 giorni a partire dalla cessazione del rapporto di lavoro, che indichi altresì, un eventuale indirizzo di posta elettronica istituzionale alternativo, cui inviare i messaggi attinenti all'attività svolta, fermo restando la sospensione immediata di qualunque procedura atta a consentire la consultazione, da parte dei suddetti soggetti, del contenuto dei messaggi già pervenuti o che potrebbero pervenire[9].
6. Decorsi 60 giorni dalla cessazione dal rapporto di lavoro di un Operatore, il Responsabile del Sistema Informatico provvederà alla disattivazione della casella di posta elettronica personale dello stesso.
7. I contenuti della casella di posta elettronica vengono conservati sui server dell'AIFA per un anno dalla cessazione del rapporto di lavoro per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti posti dall'art. 160-bis, del Codice privacy, in base al quale "La validità, *l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali*".

Art. 12 Verifica periodica delle credenziali e dei profili di accesso

1. In linea con quanto previsto dalla politiche dell'AIFA5, al fine di ridurre le opportunità di modifica o di uso improprio e/o non autorizzato del Sistema Informatico dell'AIFA, sono avviate da parte del Responsabile del Sistema Informatico, delle verifiche periodiche (almeno annuali) in merito alla sussistenza delle condizioni per il mantenimento delle credenziali di autenticazione (utenze) e dei profili autorizzativi per l'accesso al Sistema informatico dell'AIFA, con particolare attenzione ai profili autorizzativi privilegiati (es. Amministratori del sistema). Tale attività consente di effettuare un controllo a posteriori sulle credenziali di autenticazione e sui profili autorizzativi presenti, in un determinato momento, sul Sistema Informatico dell'AIFA.
2. Le attività di verifica di cui al comma 1 del presente articolo, coinvolgono:
   a) Il Responsabile del Sistema Informatico, per l'esecuzione delle seguenti attività:
      - avvio delle verifiche periodiche;
      - estrazione dal Sistema Informatico delle utenze e dei relativi profili autorizzativi;
      - predisposizione delle liste, organizzate in base al nominativo di chi ha richiesto l'attivazione delle credenziali dello specifico Operatore o Utente (Responsabile dell'Area/Settore o Responsabile dell'Ufficio), contenenti:

9 Vedasi provvedimento del Garante per la protezione dei dati personali n° 547/2016

- lo *username* ed i relativi profili autorizzativi presenti sui vari servizi/applicativi/sistemi del Sistema Informatico dell'AIFA, afferenti allo specifico richiedente.
- la tipologia di utenza (standard, amministrativa).
- il nominativo del titolare delle credenziali di autenticazione.

- invio delle suddette liste ai richiedenti individuati, con la richiesta di conferma o meno delle abilitazioni e dei profili autorizzativi sui servizi/applicativi/sistemi interessati, dei propri collaboratori.
- ricezione dei riscontri da parte dei soggetti individuati e, laddove richieste, attuazione sui sistemi delle disattivazioni e/o delle modifiche ai profili autorizzativi sui sistemi interessati.

b) Il Responsabile dell'Area/Settore o Responsabile dell'Ufficio competente per lo specifico Operatore o Utente, per l'esecuzione delle seguenti attività:
- conferma o meno delle utenze e dei profili autorizzativi assegnati agli Operatori e agli Utenti. Tali verifiche devono essere eseguite in base al principio di necessità (need-to-know, need-to-do).
- in caso di mancata conferma di una o più utenze o profili autorizzativi, richiesta al Responsabile del Sistema Informatico, della disattivazione delle utenze e/o della modifica del profilo autorizzativo.

Art. 13 Accesso alla casella di posta elettronica personale e alla cartella di lavoro in caso di assenza del titolare

1. Fermo restando quanto stabilito all'Art. 24 del presente Disciplinare, l'accesso alla casella di posta elettronica personale e alla cartella di lavoro in caso di assenza del titolare è possibile nell'eventualità e nelle modalità previste nei commi seguenti del presente articolo.
2. L'Operatore in caso di assenza preventivata dal servizio è tenuto ad attivare il servizio di risposta automatica, anche avvalendosi di servizi webmail, al fine di avvisare i mittenti, in caso di comunicazioni attinenti all'attività lavorativa, di contattare altra persona competente ovvero l'Ufficio competente.
3. In casi assolutamente eccezionali, ove vi sia la necessità di verificare il contenuto della cartella di lavoro e della posta elettronica personale del titolare, in assenza di quest'ultimo, il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio e il Responsabile del Sistema Informatico avvieranno l'apposita POS ICT AIFA[10], redigendo apposito verbale ed informando il lavoratore con tempestività e per iscritto, trasmettendogli altresì copia del verbale redatto.
4. Per le attività di cui al punto precedente, a ciascun Operatore è preventivamente fornita un'apposita informativa in cui siano specificati i limiti e le modalità di accesso alla cartella di lavoro e alla posta elettronica istituzionale da parte del Responsabile dell'Area/Settore o del Responsabile dell'Ufficio e del Responsabile del Sistema Informatico.

[10] ICT POS 362 "Procedura di accesso alle cartelle di lavoro dell'operatore"

Art. 14 Accesso alla Posta Elettronica Certificata (PEC)

1. Le credenziali di accesso alle singole caselle di posta elettronica certificata (*username* e *password*) devono essere conosciute unicamente dal titolare della PEC e dall'addetto al protocollo della struttura di riferimento della PEC stessa; per le PEC integrate nel sistema di protocollo informatico dell'Agenzia (es. protocollo@pec.aifa.gov.it), le credenziali di accesso sono assegnate al Responsabile del Servizio di Protocollo Informatico.

Art. 15 Violazioni

1. In caso di violazione del presente Regolamento da parte dell'Operatore o dell'Utente, l'AIFA può revocare le credenziali di autenticazione e autorizzazione, ovvero sospenderne temporaneamente l'utilizzo.
2. In caso di accertate violazioni del presente Disciplinare, l'AIFA procederà all'immediata inibizione delle credenziali di accesso personali riconducibili all'Operatore o all'Utente in presunzione di reato, fermo restando ogni ulteriore provvedimento di carattere sanzionatorio, laddove applicabile ai sensi di legge.

Titolo III: Norme per l'utilizzo del Sistema Informatico

Capo I: Utilizzo delle apparecchiature informatiche e telematiche

Art. 16 Personal Computer (PC)

1. Il Responsabile del Sistema informatico provvede a:
   a) dotare tutti i PC assegnati agli Operatori, di:
      - sistema operativo e sue estensioni: antivirus, programmi di office automation (programmi per la redazione di documenti, di fogli elettronici, di gestori di database);
      - eventuale software specifico correlato alle necessità delle attività lavorative.
   b) mantenere aggiornato il sistema operativo ed i software principali (antivirus, software per la navigazione in Internet, etc.), al fine di garantire la sicurezza complessiva del PC e del Sistema informatico dell'AIFA.
2. Ogni Operatore deve tenere comportamenti tali da ridurre al minimo il rischio di attacco al Sistema informatico dell'AIFA attuati mediante virus o altro software aggressivo.
3. Nel caso di malfunzionamenti o avvisi sospetti, ogni Operatore è tenuto a comunicarli al Responsabile del Sistema Informatico, secondo quanto previsto all'Art. 22 del presente Disciplinare ed a sospendere immediatamente ogni elaborazione in corso senza spegnere il computer.
4. Gli Operatori non possono modificare le caratteristiche hardware e software impostate sui PC a loro assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi AIFA, salva autorizzazione scritta del Responsabile del Sistema Informatico.
5. Non è consentita l'attivazione della password di accensione al BIOS (Basic Input-Output System) del PC, senza preventiva autorizzazione da parte del Responsabile del Sistema Informatico.

Art. 17 PC portatili e accessori temporaneamente assegnati

1. L'Operatore è responsabile del PC portatile e/o accessori (macchina fotografica, videoproiettore) a lui temporaneamente assegnati e deve custodirli con diligenza, sia all'interno degli uffici dell'AIFA, sia durante gli spostamenti esterni, fino alla loro riconsegna.
2. Ai PC portatili dell'AIFA si applicano le regole previste dal presente Disciplinare anche al di fuori della Rete e degli Uffici dell'Agenzia.
3. Particolare attenzione deve essere prestata:
   a) nell'utilizzo e nella custodia del PC portatile al di fuori della Rete e degli uffici dell'Agenzia;
   b) nella connessione a reti telematiche esterne;
   c) nella cancellazione sicura[11] di eventuali file e dati personali memorizzati nel medesimo, prima della riconsegna.

Art. 18 Supporti e dispositivi informatici di memorizzazione

1. È vietato effettuare inutili duplicazioni di dati sui supporti e dispositivi informatici di memorizzazione, anche esterni.
2. I dati personali ai sensi del GDPR trattati nell'ambito dell'attività lavorativa possono essere replicati su supporti e dispositivi informatici di memorizzazione (dischi locali dei PC, memorie esterne), banche dati e documenti, solo previa ed esplicita autorizzazione del Responsabile dell'Area/Settore o del Responsabile dell'Ufficio e attuazione delle misure di sicurezza indicate nella documentazione AIFA[12].
3. È consentito l'utilizzo di memorie esterne (es. cd rom, dvd, hard disk portatili, chiavi usb) solo se gli strumenti di lavoro sostitutivi messi a disposizione dall'AIFA non sono disponibili o utili allo scopo.
4. In caso di utilizzo delle memorie esterne nei limiti di cui al comma 3 del presente articolo, occorre effettuare preventiva scansione antivirus e, nel caso in cui siano rilevati virus informatici, avvertire immediatamente il Responsabile del Sistema Informatico.
5. Gli Operatori devono provvedere periodicamente (almeno ogni tre mesi) alla cancellazione dei file obsoleti, dai propri supporti e dispositivi informatici.

Art. 19 Dispositivi personali (BYOD)

1. L'AIFA si riserva di poter autorizzare gli Operatori all'utilizzo dei propri dispositivi BYOD al fine di accedere, conservare e trattare informazioni e accedere ad applicazioni dell'Ente.
2. I dispositivi BYOD dovranno rispondere a un livello di sicurezza almeno pari a quello dei dispositivi dell'Agenzia.
3. L'Operatore che utilizza un dispositivo BYOD deve autorizzare l'AIFA ad accedere al proprio dispositivo per il solo scopo di proteggere i dati e il Sistema Informatico dell'AIFA. L'autorizzazione deve includere la possibilità di eliminare tutti i contenuti dal dispositivo in caso di perdita o smaltimento, ivi inclusi dati personali, rubriche ed e-mail.

[11] Secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27/11/2008: "Smaltimento e cancellazione sicura dei dati"

[12] Politica generale per il trattamento delle informazioni classificate.

4. I dispositivi BYOD, nonché quelli di proprietà dell'AIFA, per i quali è stato autorizzato l'uso promiscuo, dovranno essere gestiti in modo da evitare commistioni fra i dati di proprietà dell'utilizzatore e quelli (personali o riservati) di proprietà dell'AIFA; per questi ultimi valgono tutte le limitazioni di cui al presente Capo.
5. Sui dispositivi BYOD potranno essere installati solo software precedentemente concordati con il Responsabile del Sistema Informatico dell'AIFA.

Art. 20 Cartelle di lavoro

1. Fermo restando quanto disposto all'Art. 24 del presente Disciplinare, i documenti informatici relativi all'attività lavorativa devono essere salvati nella cartella "Documenti" del PC dell'Operatore oppure in un Sistema informatico specifico o in altra cartella condivisa messa a disposizione dal Responsabile del Sistema Informatico.

Art. 21 Dismissioni e riutilizzo di apparecchiature informatiche

1. In caso di dismissione o riutilizzo delle apparecchiature informatiche, deve essere attuato quanto previsto dalle POS ICT AIFA[13].
2. Prima della dismissione o riutilizzo, delle apparecchiature informatiche contenenti dati personali ai sensi del GDPR, devono essere attuate misure atte a garantire la cancellazione sicura di tali dati in linea con quanto previsto dalla normativa vigente[14].

Art. 22 Help desk e assistenza remota

1. Gli Operatori e gli Utenti possono inviare richieste di assistenza e segnalazioni di malfunzionamento dei servizi informatici di cui all'Art. 3 let. p), tramite il web help desk accessibile dal Portale dei Servizi AIFA https://servizionline.aifa.gov.it/.
2. Il Responsabile del Sistema Informatico attua tutte le misure tecniche e organizzative per assegnare un codice di priorità ad ogni richiesta o segnalazione di cui al comma 1 del presente articolo.
3. Gli interventi associati alle richieste o segnalazioni di cui al comma 1 del presente articolo, sono espletati sulla base del livello di priorità attribuito dal Responsabile del Sistema Informatico o da suoi collaboratori appositamente autorizzati con atto di nomina formale.
4. Nel caso di interventi, che possano essere gestiti tramite assistenza remota, il personale di cui al comma 3 del presente articolo, è autorizzato ad accedere ai PC in dotazione all'Agenzia, mediante le proprie credenziali di autenticazione, in relazione agli scopi di volta in volta identificati, avendo cura di richiedere preventivo assenso all'Operatore.

13 POS 192/2012 "Modalità di dismissione beni informatici", POS 193/2014 "Modalità di backup Utente".
14 Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008: smaltimento e cancellazione sicura dei dati e Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori - Scheda informativa del Garante per la protezione dei dati personali del 12 dicembre 2008.

Capo II: Utilizzo delle risorse di rete e dei canali di comunicazione

Sezione I: Dispositivi di comunicazione

Art. 23 Dispositivi di comunicazione

1. L'installazione sul proprio PC o il collegamento alla rete LAN, di dispositivi di comunicazione (come ad esempio modem, switch, dispositivi Wireless e Bluetooth, PC portatili non in dotazione all'Ente), è consentita solo previa autorizzazione scritta da parte del Responsabile del Sistema Informatico, su richiesta formale del Responsabile dell'Area/Settore o Responsabile dell'Ufficio.

Sezione II: Posta elettronica

Art. 24 Disposizioni generali

1. L'attivazione delle caselle di posta elettronica avviene a cura del Responsabile del Sistema Informatico, secondo le modalità di cui all'Art. 8 del presente Disciplinare.
2. L'account di posta elettronica personale (indirizzo di posta e *password*) è fornito agli Operatori del Sistema informatico dell'AIFA, così come definiti nell'Art. 3 let. n) del presente Disciplinare, insieme ad un limitato spazio di memorizzazione.
3. Possono essere attivate, inoltre, una o più caselle di posta elettronica di servizio (cfr. Art. 3 let. g) per ciascuna struttura dirigenziale dell'Agenzia (es. settoreict@aifa.gov.it, segreteriarisorseumane@aifa.gov.it), previa motivata richiesta del Responsabile dell'Area/Settore o Responsabile dell'Ufficio al Responsabile del Sistema Informatico.
4. Il formato della casella di posta elettronica personale e della casella di servizio è indicato nella IS OP 002[15].
5. Fermo restando quanto stabilito dall'Art. 40-bis del Codice dell'Amministrazione Digitale (nel seguito anche CAD), il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio devono attuare tutti quegli accorgimenti organizzativi per fare in modo che i contenuti (comunicazioni e documenti di lavoro) rilevanti per l'area/settore o ufficio, e non di esclusivo utilizzo dell'Operatore nell'ambito della propria attività lavorativa, siano resi disponibili agli altri soggetti competenti in materia, ad esempio, attraverso le seguenti modalità:
   a) per il contenuto della posta elettronica: inoltro alla posta elettronica di servizio dell'area/settore o ufficio o alla casella di posta elettronica di altro soggetto competente (es. Responsabile dell'Ufficio);
   b) per i documenti elettronici: salvataggio su cartella condivisa messa a disposizione dal Responsabile del Sistema Informatico ovvero nel Sistema informatico messo a disposizione.

[15] IS OP 002: Servizi di manutenzione logistica e assistenza informatica.

6. Il Responsabile del Sistema Informatico ha l'obbligo di adottare tutte le misure di sicurezza ritenute necessarie e sufficienti a minimizzare il rischio di perdita di informazioni. A tal fine, egli si avvale anche di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.
7. I messaggi di posta elettronica vengono conservati nei server mail dell'AIFA, finché non vengono cancellati dagli Operatori. I server sono gestiti dal Settore Informatico dell'Ente, che ne cura anche il backup periodico. Alcuni messaggi cancellati dagli Operatori potrebbero essere comunque conservati nei dispositivi di salvataggio automatico (backup) dei dati.
8. L'Operatore deve comunicare al Responsabile del Sistema Informatico qualsiasi malfunzionamento del proprio indirizzo di posta elettronica, mediante il servizio di helpdesk di cui all'Art. 21 del presente Disciplinare.
9. L'AIFA può inviare agli indirizzi di posta elettronica personali degli Operatori:
   a) comunicazioni istituzionali e di servizio.
   b) buste paga.
   c) certificazioni uniche.
10. Per le comunicazioni effettuate tramite posta elettronica, occorre osservare, oltre alle regole esposte nel presente Disciplinare, le disposizioni contenute nel "Manuale di gestione documentale dell'Agenzia Italiana del farmaco".

Art. 25 Utilizzo della posta elettronica da parte degli Operatori

1. L'Operatore è riconosciuto quale unico autore dei messaggi inviati dalla sua casella di posta elettronica personale fornitagli dall'AIFA ed è considerato, inoltre, unico responsabile dell'attività espletata tramite la propria casella di posta personale.
2. L'Operatore deve implementare, sulla propria postazione di accesso alla posta elettronica, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili e garantire la funzionalità della stessa casella.
3. L'Operatore in servizio è tenuto ad accedere alla casella di posta elettronica durante la giornata lavorativa.
4. L'Operatore deve utilizzare il servizio di posta elettronica nel rispetto della legge e del presente Disciplinare, ponendo la massima attenzione alla sicurezza del Sistema informatico e telematico dell'AIFA.
5. L'Operatore, in accordo con il Responsabile dell'Area/Settore o Responsabile dell'Ufficio, attua tutte quelle misure di carattere organizzativo procedimentale tese ad evitare l'uso della casella di posta elettronica come sistema documentale, privilegiando altresì gli strumenti istituzionali all'uopo preposti (e.g. protocollo informatico, cartelle condivise, cloud).
6. L'Operatore è responsabile dell'efficace organizzazione e gestione della propria casella di posta elettronica, attuando buone pratiche, quali a titolo esemplificativo e non esaustivo:
   a) cancellare i documenti inutili e/o che possono essere reperiti su altri sistemi istituzionali;

b) evitare di richiedere l'invio di allegati ingombranti, privilegiando modalità alternative di invio meno invasive (es. permalink, link a cartelle condivise);
c) organizzare le e-mail in cartelle per mittente/argomento, ai fini di una successiva ricerca.

Art. 26 Utilizzo della posta elettronica per comunicazioni private

1. Non è consentito agli Operatori l'uso della posta elettronica per motivi non inerenti al rapporto di lavoro in essere con l'AIFA.

Art. 27 Contenuto delle Comunicazioni

1. L'Operatore è tenuto ad osservare i seguenti divieti:
   a) divieto di utilizzare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, diffamatorio, discriminatorio, pericoloso per il Sistema informatico;
   b) divieto di utilizzare il servizio per inviare o ricevere messaggi o materiali che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
   c) divieto di utilizzare il servizio per inviare catene di lettere, comunicazioni commerciali, messaggi politici;
   d) divieto di aprire, anche mediante servizi di *webmail* personali, messaggi di posta elettronica sospetti contenenti particolari tipologie di allegati (es. files con estensione exe, bat, com e file audio, video o immagini), senza l'autorizzazione del Responsabile del Sistema Informatico;
   e) divieto di effettuare invii multipli di e-mail senza mascherare gli indirizzi delle caselle e-mail dei vari destinatari, se non strettamente necessario;
   f) divieto di sovraccaricare il sistema con l'invio di allegati di dimensioni elevate ed evitare immagini (es. sfondi) o grafismi superflui;
   g) divieto di effettuare comunicazioni inerenti all'attività lavorativa con caselle di posta elettronica diverse da quella personale, di servizio o certificata di cui all'Art. 3 lett. f), g), h) del presente Disciplinare.
   h) divieto di effettuare comunicazioni esterne così come individuate nell'Art. 3 let. i), contenenti categorie particolari di dati personali o dati personali relativi a condanne penali e reati sensi del GDPR, nonché documenti dell'AIFA per i quali l'accesso è regolato dalla Legge n. 241/1990[16], in modo particolare se riservati o protetti dal diritto d'autore[17].
2. Ogni comunicazione dovrà riportare i seguenti elementi essenziali:
   a) oggetto;
   b) contenuto (testo ed eventuale allegato/i);
   c) firma.
3. I messaggi di posta elettronica, come definiti all'Art. 3 let. l) del presente Disciplinare, inviati verso l'esterno devono riportare in calce la "firma standard", secondo il formato definito nel comma 6, let. a) del presente articolo, contenente il logo dell'Agenzia, nome e cognome del mittente, il ruolo/qualifica, il servizio/struttura di appartenenza, l'indirizzo postale, l'indirizzo del sito web dell'Agenzia e i dati di contatto (telefono/i, fax ed e-mail) ed eventuali link ai profili SNS istituzionali.
4. I messaggi di posta elettronica, come definiti all'Art. 3 let. l) del presente Disciplinare, inviati verso l'interno o inoltrati verso e-mail esterne/interne o in risposta a e-mail esterne/interne, devono riportare una "firma breve", secondo il formato definito nel comma 6, let. b) del presente articolo, contenente nome e cognome, i dati di contatto (telefono/i, fax ed e-mail), il servizio/struttura di appartenenza.

[16] Legge n. 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e s.m.i.

[17] Legge, 22/04/1941 n° 633 "Legge a protezione del diritto d'autore e di altri diritti connessi al suo esercizio" e s.m.i.

5. I messaggi di posta elettronica effettuati da un dispositivo mobile, quale ad esempio lo smartphone o il tablet, devono riportare la "firma breve" di cui al comma 6, let. b) del presente articolo.
6. Nelle comunicazioni di cui ai commi da 3 a 5 del presente articolo, gli Operatori sono tenuti ad utilizzare i seguenti formati di firma:

   a) Firma standard

   LOGO

   Mario Rossi (Font Calibri Pt 11 grassetto)
   Collaboratore amministrativo (Font Calibri Pt 10)
   Settore ICT
   Agenzia Italiana del Farmaco
   Via del Tritone, 181 - 00187 Roma
   Tel. +39 0659784NNN | Fax +39 0659784NNN | Cell. +39 33…….
   m.rossi@aifa.gov.it | www.aifa.gov.it

   b) Firma breve

   Giuseppe Bianchi (Font Calibri Pt 11 grassetto)
   Dirigente Area Amministrativa (Font Calibri Pt 10)
   Agenzia Italiana del Farmaco
   Tel. +39 0659784NNN | Fax +39 0659784NNN | Cell. +39 33…….

Sezione III: Posta Elettronica Certificata (PEC)

Art. 28 Disposizioni generali

1. Ciascun Responsabile dell'Area/Settore o Responsabile dell'Ufficio può richiedere al Responsabile del Sistema Informatico l'attivazione di una casella di posta elettronica certificata, previa autorizzazione del Direttore Generale dell'Agenzia.
2. Il formato degli indirizzi PEC dell'Agenzia è indicato nella IS OP 002[18].
3. L'elenco delle caselle di posta elettronica certificata dell'AIFA (@pec.aifa.gov.it) è pubblicato sul sito internet dell'Agenzia (http://www.aifa.gov.it).
4. Il titolare della PEC è riconosciuto quale unico responsabile dell'attività espletata tramite la casella PEC istituzionale.

Art. 29 Utilizzo della PEC istituzionale

1. Il titolare della PEC e l'addetto al protocollo della struttura di riferimento della PEC stessa devono implementare, sulla propria postazione di accesso alla PEC, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili e garantire la funzionalità della stessa casella.
2. Le caselle PEC devono essere controllate quotidianamente dagli addetti al protocollo, che provvedono a:
   a) protocollare e archiviare i messaggi (eccetto i messaggi di spam);
   b) smistarli agli Uffici competenti dell'Agenzia.
3. Non è consentito al titolare della PEC e agli addetti al protocollo della struttura di riferimento della PEC stessa, l'uso della PEC per motivi non inerenti all'attività lavorativa.
4. Per le comunicazioni tramite PEC, occorre osservare le disposizioni del "Manuale di gestione documentale dell'Agenzia Italiana del Farmaco".
5. Il titolare della PEC e l'addetto al protocollo della struttura di riferimento della PEC stessa devono utilizzare il servizio di PEC nel rispetto della legge e del presente Disciplinare, ponendo la massima attenzione alla sicurezza del Sistema informatico e telematico dell'AIFA.

Art. 30 Contenuto delle Comunicazioni tramite PEC istituzionale

1. Il titolare della PEC e l'addetto al protocollo della struttura di riferimento della PEC stessa sono tenuti ad osservare i seguenti divieti:
   a) divieto di utilizzare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, diffamatorio, discriminatorio, pericoloso per il Sistema informatico;
   b) divieto di utilizzare il servizio per inviare o ricevere messaggi o materiali che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
   c) divieto di utilizzare il servizio per inviare catene di lettere, comunicazioni commerciali, messaggi politici;

[18] IS OP 002: Servizi di manutenzione logistica e assistenza informatica.

d) divieto di aprire messaggi PEC sospetti contenenti particolari tipologie di allegati (es. files con estensione exe, bat, com e file audio, video o immagini), senza l'autorizzazione del Responsabile del Sistema Informatico;
e) divieto di sovraccaricare il sistema con l'invio di allegati di dimensioni elevate ed evitare immagini (es. sfondi) o grafismi superflui.

Sezione IV: Intranet e Internet

Art. 31 Utilizzo dell'archivio di rete

1. L'archivio di rete così come definito nell'Art. 3 lett. b) è un'area strettamente professionale e non può in alcun modo essere utilizzato per scopi diversi da quelli lavorativi. Qualunque contenuto informatico che non sia legato all'attività lavorativa non può essere memorizzato, nemmeno per brevi periodi, in questo archivio.
2. Il Responsabile del Sistema Informatico svolge sulle unità di rete attività di controllo, amministrazione e può in qualunque momento procedere alla rimozione dei contenuti informatici che riterrà pericolosi per la Sicurezza del Sistema informatico dell'AIFA.

Art. 32 Collegamento alla rete locale

1. Non è consentito collegare alcun dispositivo alla rete dell'AIFA senza la preventiva autorizzazione scritta del Responsabile del Sistema Informatico.

Art. 33 Utilizzo di Internet

1. Non è consentito agli Operatori di:
   a) accedere ad Internet per motivi privati non inerenti al lavoro d'ufficio, fatte salve le operazioni consentite nel presente Disciplinare e con i limiti ivi indicati;
   b) effettuare il download o lo scambio peer-to-peer di materiale audiovisivo, fotografico, software ed in genere di ogni altra tipologia di materiale digitale non legati ad un uso d'ufficio e che possa sottintendere presunte o palesi violazioni del copyright in ambito nazionale ed internazionale.
2. L'accesso alla rete Internet dalla rete LAN cablata e senza fili (WiFi) dell'AIFA è fornito gratuitamente.
3. Si rammenta che, limitatamente alle finalità indicate nelle specifiche Informative sulla protezione dei dati personali predisposte dall'AIFA ai sensi degli artt.13 e 14 del GDPR, i sistemi di accesso ad Internet dell'AIFA tengono traccia della navigazione degli Operatori.
4. L'AIFA fornisce libero accesso a Internet tramite la rete Wi-Fi gli Utenti di cui all'Art. 3 let. x) del presente Disciplinare, così come previsto dall' articolo 8-bis del D.lgs. 7 marzo 2005, n. 82[19].
5. Il Responsabile del Sistema Informatico produce periodicamente una statistica anonima dei siti web visitati dagli Operatori tramite la rete dell'AIFA.

[19] L'articolo 8-bis del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale (CAD)" ha previsto che le pubbliche amministrazioni, favoriscono, in linea con gli obiettivi dell'Agenda digitale europea, la disponibilità di connettività alla rete Internet presso gli uffici pubblici e altri luoghi pubblici, in particolare nei settori scolastico, **sanitario** e di interesse turistico, anche prevedendo che la porzione di banda non utilizzata dagli stessi uffici sia messa a disposizione degli utenti attraverso un sistema di autenticazione tramite SPID, carta d'identità elettronica o carta nazionale dei servizi, ovvero che rispetti gli standard di sicurezza fissati dall'AgID.

Art. 34 Responsabilità nella navigazione web

1. L'Operatore è considerato l'unico responsabile dell'attività espletata nella rete Intranet dell'AIFA e nella Internet mediante le proprie credenziali di accesso e di autorizzazione di cui all'Art. 8 del presente Disciplinare.
2. Ogni Operatore è obbligato ad utilizzare il servizio di accesso al web, ponendo la massima attenzione alla sicurezza del Sistema informatico e telematico della AIFA e nel rispetto di quanto previsto dal Codice di Comportamento dell'Agenzia Italiana del Farmaco e dalla Social Media Policy dell'AIFA.

Art. 35 Filtri web

1. Il Responsabile del Sistema Informatico provvede ad inibire, mediante appositi filtri, la consultazione dei siti web o categorie di siti web non utili alla produttività dell'Agenzia e, soprattutto, potenzialmente lesivi per la Rete dell'AIFA, in coordinamento con il Responsabile dell'Area/Settore o Responsabile dell'Ufficio.
2. Il Responsabile del Sistema Informatico si riserva di applicare per singoli e gruppi di Operatori, politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione Generale e con il Responsabile dell'Area/Settore o Responsabile dell'Ufficio, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
3. Il Responsabile del Sistema Informatico potrà autorizzare la navigazione verso siti o categorie di siti bloccati, previa richiesta motivata, da parte del Responsabile dell'Area/Settore o del Responsabile dell'Ufficio interessato, legata a specifiche ed inderogabili esigenze lavorative.

Art. 36 Attivazione di nuovi profili SNS dell'Ente

1. L'AIFA ha un proprio profilo pubblico identificabile come "AIFA". Il Direttore Generale valuta ogni richiesta, inoltrata dal Responsabile dell'Area/Settore o del Responsabile dell'Ufficio competente e autorizza l'eventuale attivazione di nuovi profili pubblici riferiti a specifici servizi secondo le effettive esigenze dell'Agenzia.
2. L' Ufficio Stampa e Comunicazione dell'Agenzia, d'intesa con il richiedente di cui al comma 1 del presente articolo, è incaricato della gestione dei contenuti del profilo pubblico di SNS attivato. Gli Operatori incaricati, a seconda dei meccanismi di accesso e gestione dello specifico SNS, utilizzano congiuntamente le credenziali di accesso del profilo pubblico assegnate all'Ente dal SNS (es. pagine Facebook, Twitter).

Capo III: Altri Dispositivi

Art. 37 Stampanti, fotocopiatrici, scanner e fax dell'Agenzia

1. È cura dell'Operatore effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
2. Non è consentito stampare documenti o file molto lunghi o di contenuto grafico su stampanti comuni, se non strettamente necessario all'attività lavorativa.
3. Non è consentito stampare, fotocopiare o scansionare documenti personali su qualsivoglia stampante e/o fotocopiatrice.
4. L'utilizzo delle memorie esterne (es. chiavetta USB) per effettuare stampe è consentito solo nel rispetto di quanto previsto dall'Art. 18 comma 4.
5. È obbligatorio effettuare le stampe in modalità fronte-retro, fatta salva documentata impossibilità tecnica o amministrativa.
6. È vietato l'utilizzo dei fax dell'Agenzia e delle stampanti di rete per fini personali, tanto per spedire quanto per ricevere documentazione.
7. L'utilizzo dei fax dell'Agenzia è consentito esclusivamente per lo scambio documentale con i privati cittadini e con i soggetti che non sono tenuti ad avere una PEC ai sensi dell'art. 47 comma 2 let. c) del CAD.
8. È fatto divieto agli Operatori effettuare la sostituzione del toner o di qualsiasi altra parte di ricambio sulle stampanti, sulle fotocopiatrici, sugli scanner e sui fax.
9. In caso di malfunzionamento delle apparecchiature in oggetto al presente articolo, gli Operatori sono tenuti a darne tempestiva comunicazione al Settore ICT.

Art. 38 Telefoni fissi

1. L'Operatore è responsabile dell'utilizzo del telefono fisso assegnato.
2. Il telefono fisso affidato all'Operatore dall'Agenzia è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali mediante il telefono fisso aziendale a disposizione è consentito solo nel caso di comprovata necessità ed urgenza e in presenza di preventiva autorizzazione scritta.

Art. 39 Telefoni cellulari e SIM

1. L'Operatore è responsabile dell'utilizzo del telefono cellulare e/o della SIM assegnati dall'AIFA.
2. Al cellulare e alla SIM assegnate si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale fisso; in particolare, è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
3. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto per motivi di necessità ed urgenza e in presenza di preventiva

autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Responsabile del Sistema Informatico e dai suoi collaboratori.

Capo IV: Smart card, Carta Nazionale dei Servizi e Firma Digitale

Art. 40 Soggetti abilitati

1. A ciascun dipendente dell'Agenzia è assegnata una smart card numerata, nominativa, con fotografia e dati anagrafici del titolare, per consentire l'accesso alle sedi dell'Agenzia e per rilevare le presenze.
2. Su ciascuna smart card di cui al comma 1 del presente articolo, possono essere installati i certificati di Carta Nazionale dei Servizi (CNS) e di firma digitale.
3. Il certificato di CNS è assegnato a ciascun dipendente dell'AIFA per accedere ai servizi online dell'AIFA e della Pubblica Amministrazione su tutto il territorio nazionale.
4. Il dispositivo di firma digitale è assegnato a:
   - Direttore Generale;
   - Dirigenti responsabili di struttura;
   - Dirigenti e funzionari individuati con specifico provvedimento dell'Agenzia.

Sezione I: Firma Digitale

Art. 41 Utilizzo della firma digitale

1. La firma digitale è utilizzata per la sottoscrizione di documenti informatici nell'ambito delle attività istituzionali dei soggetti abilitati e nel rispetto dei poteri di firma derivanti dalla legge o dai regolamenti interni dell'AIFA.

Art. 42 Definizione dei ruoli per la gestione del certificato di firma digitale

1. Operano nel processo di assegnazione e gestione del certificato di firma digitale i seguenti soggetti:
   a) Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio, che richiede il certificato a favore del titolare.
   b) Il Direttore Generale dell'AIFA provvede a fornire informazioni per ciò che attiene al ruolo e alle funzioni istituzionali dei dipendenti ai quali possono essere assegnati i certificati di firma digitale e individua e nomina gli incaricati del servizio; ai sensi dell'art. 36, comma 1 let. c) del CAD, autorizza il rilascio del certificato e ha inoltre la facoltà di richiedere la sospensione o la revoca del certificato.
   c) Il Certificatore, ovvero il soggetto che si occupa della gestione del servizio di firma qualificata nel rispetto di quanto disposto dall'art. 32, comma 3 del CAD.
   d) Soggetti nominati dal Direttore Generale e responsabili su delega del Certificatore, incaricati del servizio di firma digitale, dell'identificazione dei richiedenti, dell'attivazione delle procedure di emissione, revoca o sospensione dei certificati.
   e) Il Titolare al quale è assegnato il certificato di firma digitale. Con successiva determinazione verranno indicate le categorie che, in ragione della funzione che svolgono all'interno dell'Agenzia, potranno essere titolari di firma digitale e i soggetti che potranno autorizzarne il rilascio.

Art. 43 Compiti e responsabilità degli incaricati del servizio di firma digitale

1. Gli incaricati del servizio di firma provvedono a:

   a) verificare con certezza l'identità del titolare.
   b) rilasciare i certificati qualificati attraverso l'utilizzo dell'apposito Sistema informatico fornito dal Certificatore, seguendo le istruzioni operative previste dal Manuale Operativo del Certificatore.
   c) informare il titolare riguardo agli obblighi assunti in merito alla protezione della segretezza delle chiavi private e al trattamento dei dati personali.
   d) supportare il titolare nelle ipotesi di revoca, sospensione o annullamento della sospensione delle firme attivate.
   e) raccogliere le comunicazioni di rilascio/rinnovo, sospensione e/o revoca e conservarle con modalità sicure.
   f) individuare mensilmente i certificati la cui data di scadenza è compresa entro i trenta giorni solari successivi e, verificato il permanere delle condizioni per il rilascio, richiedere l'autorizzazione formale per il rinnovo degli stessi secondo quanto indicato al presente articolo, comma 1, let. c).
   g) rispettare le misure di sicurezza previste nel presente disciplinare.
   h) rispettare le necessarie procedure di sicurezza nell'esercizio delle proprie funzioni.
   i) compilare l'elenco dei titolari di certificato per l'identificazione.
   j) fornire istruzioni ai titolari sul corretto utilizzo del servizio di firma digitale.
   k) conservare le buste contenti i PIN - fornite dal Certificatore - in luogo sicuro e protetto, avendone accesso esclusivo.

Art. 44 Obblighi del titolare del certificato di firma digitale

1. Il titolare del certificato di firma digitale è tenuto a:

   a) adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma, che utilizzerà personalmente e per ragioni istituzionali.
   b) conservare con la massima diligenza e riservatezza i propri codici personali al fine di evitarne l'uso fraudolento da parte di terzi.
   c) comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione all'incaricato del servizio di firma digitale ed informarlo dell'eventuale variazione del rapporto contrattuale con l'Agenzia e di tutti i dati richiesti per l'emissione del certificato.
   d) informare anticipatamente gli incaricati del servizio di firma digitale di ogni circostanza che renda necessaria o, comunque, opportuna la revoca o la sospensione del certificato e del dispositivo di firma a lui assegnato; deve altresì informare tempestivamente il suddetto incaricato di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

Art. 45 Attivazione e rinnovo del certificato di firma digitale

1. Il Direttore Generale dell'AIFA, al quale spetta dare l'autorizzazione al rilascio del certificato di firma digitale ai sensi dell'Art. 42, comma 1, let. e) del presente Disciplinare invia, all'Incaricato del servizio di firma digitale, l'elenco debitamente sottoscritto, delle persone autorizzate al possesso del certificato di firma digitale.

2. L'incaricato, ricevuta la richiesta di attivazione, convoca il richiedente per lo svolgimento delle operazioni di registrazione.
3. Il richiedente deve presentarsi dall'Incaricato, nel giorno comunicatogli, munito di un valido documento di identità e del codice fiscale.

Art. 46 Causa di revoca e sospensione del certificato di firma digitale

1. La revoca di un certificato di firma digitale determina la cessazione anticipata della sua validità. La revoca ha luogo su iniziativa di Certificatore, del Titolare, del Direttore Generale che ne ha autorizzato il rilascio.
2. La revoca ha luogo, a titolo esemplificativo e non esaustivo, nelle seguenti circostanze:
   a) cessazione del rapporto di lavoro del dipendente per qualsiasi causa (es. pensionamento, dimissioni);
   b) perdita del ruolo, qualifica o funzione istituzionale che motivano l'assegnazione del certificato;
   c) smarrimento, furto o cambio del dispositivo di firma;
   d) smarrimento o furto dei codici di sicurezza;
   e) sospetta falsificazione o abusi;
   f) riscontro da parte del Certificatore o dell'Agenzia di una violazione, commessa dal titolare, delle regole di utilizzo.
3. La sospensione di un certificato di firma digitale determina l'interruzione temporanea della sua validità. La sospensione ha luogo su iniziativa del Certificatore, del titolare o del Direttore Generale che ne ha autorizzato il rilascio.
4. La sospensione ha luogo, a titolo esemplificativo e non esaustivo, nelle seguenti circostanze:
   a) la possibile perdita dei codici di sicurezza;
   b) il venir meno di uno o più requisiti che ne motivano l'assegnazione.
5. Ai sensi dell'art. 36, comma 3, del CAD la revoca o la sospensione del certificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione, a cura del Certificatore, della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

Titolo IV: Monitoraggio e controlli

Art. 47 Principi generali

1. L'AIFA adotterà ogni accorgimento tecnico necessario a tutelare l'Agenzia da eventuali comportamenti non consentiti, salvaguardando il rispetto della libertà e della dignità dei lavoratori. Gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

Art. 48 Monitoraggi

1. Il Responsabile del Sistema Informatico effettua un monitoraggio periodico del Sistema Informatico dell'AIFA, al fine di:

   a) garantire la continuità dei servizi forniti tramite il Sistema Informatico dell'AIFA, che consentono il perseguimento degli scopi istituzionali dell'Ente, anche mediante la rilevazione e la risoluzione di anomalie di funzionamento presenti o imminenti (troubleshooting);
   b) gestire le richieste di assistenza e segnalazioni di malfunzionamento dei PC e della Rete effettuate tramite il web help desk accessibile dal Portale dei Servizi online AIFA;
   c) garantire la protezione e ottimizzazione delle risorse di rete e il mantenimento di livelli ottimali di qualità dei servizi forniti tramite il Sistema Informatico dell'AIFA;
   d) garantire la protezione del patrimonio informativo, nonché l'integrità e disponibilità delle postazioni di lavoro e dei server dell'Amministrazione, rispetto a eventuali violazioni, accidentali o dolose, nel loro utilizzo;
   e) verificare la corretta applicazione del presente Disciplinare, per quanto di propria competenza.

2. Il monitoraggio di cui al comma 1 del presente articolo, può prevedere, limitatamente alle finalità indicate nelle specifiche Informative sulla protezione dei dati personali predisposte dall'AIFA ai sensi degli artt.13 e 14 del GDPR:

   a) Il monitoraggio delle applicazioni software e dei sistemi;
   b) l'analisi del traffico di rete LAN e del traffico Internet;
   c) l'Inventario Hardware e Software effettuato attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete LAN dell'AIFA.

Art. 49 Verifiche

1. È responsabilità del Responsabile dell'Area/Settore o del Responsabile dell'Ufficio verificare il corretto utilizzo delle risorse informatiche assegnate all'Area/Settore/Ufficio di riferimento ed evitarne l'uso improprio o l'accesso alle suddette risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di soggetti terzi di punti rete in luoghi non presidiati.
2. L'AIFA si riserva comunque le facoltà previste dalla normativa vigente, di effettuare controlli occasionali e puntuali, nel caso di segnalazioni di attività che hanno causato danno all'Amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.
3. I controlli di cui ai commi 1 e 2 del presente articolo, devono essere ispirati ai principi generali di cui all'Art. 5 del presente Disciplinare, e devono essere effettuati nel rispetto di quanto previsto dallo Statuto dei lavoratori[20] e dalla normativa vigente in materia di dati personali.

[20] L. 300 del 1970

Titolo V: Responsabilità e Sanzioni

Art. 50 Responsabilità

1. Per quanto di competenza l'applicazione delle disposizioni contenute nel presente Disciplinare costituisce elemento di valutazione della responsabilità dirigenziale, valutata ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili.
2. Gli Operatori e gli eventuali Utenti sono responsabili per qualsiasi utilizzo degli strumenti elettronici e informatici dell'AIFA non conforme alle disposizioni del presente Disciplinare e/o alle leggi vigenti.
3. L'AIFA monitora l'utilizzo della Rete e verifica, nel pieno rispetto della normativa vigente in tema di privacy, l'attuazione delle disposizioni del presente Disciplinare.
4. Tutte le informazioni raccolte sono utilizzabili nei limiti dello Statuto dei lavoratori[21], del Codice privacy e del GDPR e successive integrazioni e memorizzate per i periodi di tempo indispensabili al raggiungimento delle finalità perseguite.

Art. 51 Sanzioni

1. Le violazioni delle disposizioni contenute nel presente Disciplinare sono fonte di responsabilità disciplinare e sono valutate, in relazione alla loro gravità, dal Responsabile dell'Area/Settore, dal Responsabile dell'Ufficio o dalla struttura dell'Agenzia competente in materia di provvedimento disciplinare, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni a potenziale rilevanza penale ed erariale.
2. Nei casi di accertata violazione delle disposizioni contenute nel presente Disciplinare, è demandata al Responsabile dell'Area/Settore o Responsabile dell'Ufficio competente, l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituente reato.
3. L'Agenzia ha il dovere di segnalare alle autorità competenti, per gli opportuni accertamenti ed i provvedimenti del caso, gli eventuali usi illeciti dei servizi informatici e telematici, ivi compresi gli atti ed i comportamenti configurabili come "crimini informatici" perseguibili penalmente. Tali crimini informatici, possono riguardare ad esempio:
    - l'esercizio arbitrario delle proprie ragioni con violenza sulle cose (art. 392 c.p.);
    - l'attentato ad impianti informatici di pubblica utilità (art. 420 c.p.);
    - la falsificazione di documenti informatici (art. 491 bis c.p.);
    - l'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
    - la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
    - la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.);
    - la violazione di corrispondenza telematica (artt. 616 e 617 sexies c.p.);

[21] L. 300 del 1970

- l’intercettazione di e-mail (art. 617 quater c.p.);
- la rivelazione del contenuto di documenti segreti (art. 621 c.p.);
- il danneggiamento di sistemi informatici e telematici (art. 635 bis c.p.);
- la frode informatica (art. 640 ter c.p.) ovvero l’alterazione dell’integrità dei dati allo scopo di procurarsi un illecito profitto.

Titolo VI: Disposizioni finali

Art. 52 Aggiornamento e revisione

1. Tutti gli Operatori possono proporre, quando ritenuto necessario, integrazioni al presente Disciplinare.
2. Le proposte verranno esaminate dalle strutture competenti congiuntamente al Responsabile del Sistema Informatico e al Responsabile della Sicurezza delle Informazioni.
3. Il presente Disciplinare è soggetto a revisione con frequenza triennale salvo innovazioni organizzative, tecniche o normative.