REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Versione:	3.0
Anno:	2026
Approvazione	Comitato di Indirizzo – deliberazione n. 18 del 12 maggio 2026

GLOSSARIO:

Antivirus: software di protezione installato sui dispositivi informatici con lo scopo di rilevare, bloccare ed eliminare software malevoli (malware), inclusi virus, worm, ransomware e spyware. Deve essere sempre attivo, aggiornato e non può essere disabilitato dall'utente.
Autenticazione a più fattori (MFA / 2FA): metodo di verifica dell'identità dell'utente che richiede la combinazione di almeno due elementi distinti tra: qualcosa che si conosce (password), qualcosa che si possiede (dispositivo, token OTP) o qualcosa che si è (dato biometrico). Rafforza significativamente la sicurezza degli accessi rispetto alla sola password.
Backup: duplicazione di un file o di un insieme di file su un supporto esterno al computer, per avere una copia di riserva, finalizzata a garantire la disponibilità e il ripristino dei dati in caso di incidenti, guasti o eventi di sicurezza informatica.

Cloud: sistema configurato su server remoto che consente di disporre di risorse software e hardware (come memorie di massa per l'archiviazione di dati, o applicazioni), il cui utilizzo è erogato come servizio.

Download, **scaricamento**: ricevere o prelevare tramite rete telematica (ad esempio da un sito web) uno o più file, trasferendolo sul disco rigido del computer o su altra periferica.

File sharing: sistema per lo scambio di file tra utenti di Internet tramite un server comune.

Hard disk: principale unità di memorizzazione dei dati sul computer, in cui vengono memorizzati il sistema operativo, i programmi applicativi, i dati di configurazione del computer, ed eventualmente i documenti creati dall'utente.

Incidente di sicurezza informatica: evento o serie di eventi che compromettono o minacciano la riservatezza, l'integrità o la disponibilità dei sistemi informativi e dei dati. Include, a titolo esemplificativo: accessi non autorizzati, infezioni da malware, violazioni di dati personali (data breach), interruzioni di servizio. Deve essere tempestivamente segnalato all'Ufficio Sistemi Informativi secondo le procedure interne.
Instant messaging: strumenti di comunicazione on-line, simultanea ed in tempo reale, tra due o più utenti.

Intelligenza artificiale (IA): insieme di tecnologie e sistemi informatici in grado di eseguire compiti che richiedono capacità tipicamente umane, quali comprensione del linguaggio, generazione di testi o immagini, analisi di dati e supporto alle decisioni. L'utilizzo di strumenti basati su IA nell'ambito lavorativo è consentito esclusivamente nel rispetto della normativa vigente (tra cui il Regolamento UE 2024/1689 – AI Act e la L. n. 132/2025) e delle disposizioni adottate dall'Ente.
Login: procedura di accesso a un sistema informatico, che prevede l'inserimento di un codice identificativo (UserID o nome utente) e di una parola d'ordine (Password) da parte dell'utente. Nei sistemi che richiedono particolari cautele di sicurezza può essere integrata con un codice (PIN), assegnato all'utente o rilasciato in tempo reale tramite telefono cellulare (OTP).

Logout: procedura di scollegamento da un sistema informatico a cui si era avuto accesso tramite un'operazione di login.

Malware: termine generale che indica qualsiasi software progettato intenzionalmente per causare danni a sistemi informatici, reti o dati. Comprende diverse categorie, tra cui virus, worm, spyware, ransomware e trojan. È una delle principali minacce alla sicurezza informatica degli Enti pubblici.
OTP: codice numerico di sicurezza per accesso ai sistemi informatici, abbinato a nome utente e password, come il PIN, ma rilasciato tramite app o SMS sul telefono cellulare dell'utente, ed utilizzabile una sola volta per un tempo limitato.

Password: parola d'ordine dell'utente.

PEC (Posta Elettronica Certificata): sistema di posta elettronica che fornisce al mittente la documentazione elettronica attestante l'invio e la consegna del messaggio, con pieno valore legale equivalente alla raccomandata con avviso di ricevimento. Disciplinata dal D.P.R. n. 68/2005 e dal Codice dell'Amministrazione Digitale (CAD).
Phishing: tecnica di attacco informatico volta a indurre l'utente a fornire informazioni riservate o a compiere azioni dannose, mediante comunicazioni fraudolente che imitano soggetti affidabili (ad esempio email, messaggi o siti web contraffatti).

PIN: codice alfanumerico breve (di solito non più di 8 caratteri) abbinato a nome utente e password, che integra la sicurezza negli accessi ai sistemi informatici.

Ransomware: tipologia di malware che cifra i dati presenti sui sistemi informatici della vittima, rendendoli inaccessibili, e richiede il pagamento di un riscatto per il ripristino. Costituisce una delle minacce più gravi per le pubbliche amministrazioni, con potenziale impatto sulla continuità operativa e sulla protezione dei dati. Il pagamento del riscatto non è mai raccomandato dalle autorità competenti.
Server: computer di elevate prestazioni, che in una rete distribuisce un servizio (un applicativo, o l'accesso a cartelle e file di dati) agli elaboratori degli utenti collegati, detti client. rientrante tra i sistemi informativi dell'Ente.

Smart working (lavoro agile): modalità di esecuzione del rapporto di lavoro subordinato caratterizzata dall'assenza di vincoli orari o spaziali fissi, svolta anche al di fuori dei locali dell'Ente mediante l'utilizzo di strumenti informatici. Disciplinata dalla L. n. 81/2017. Ai fini del presente Regolamento, le disposizioni in materia di utilizzo degli strumenti informatici si applicano integralmente anche in modalità di lavoro agile.
Software: è l'insieme delle componenti immateriali di un sistema informatico, costituito principalmente dai programmi che vengono elaborati dal computer; è contrapposto all'hardware, cioè la parte materiale, tangibile, dello stesso sistema.

SPAM: messaggio pubblicitario non richiesto, inviato in modo massivo e ripetuto a un numero molto elevato di utenti di Internet, tramite posta elettronica.

Spyware: software scaricato, per lo più in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario, rientrante nella categoria dei software malevoli.

Virus: programma informatico malevolo in grado di replicarsi inserendo copie di sé stesso in altri file o programmi, diffondendosi tra sistemi e causando danni quali la corruzione o la perdita di dati, il rallentamento o il blocco del sistema. Si propaga tipicamente tramite allegati e-mail, download da fonti non attendibili o dispositivi rimovibili infetti.
VPN (Virtual Private Network): rete privata virtuale che consente di stabilire una connessione cifrata e sicura tra il dispositivo dell'utente e la rete informatica dell'Ente attraverso una rete pubblica (Internet). Utilizzata obbligatoriamente per l'accesso remoto ai sistemi aziendali al di fuori della sede, garantisce la protezione dei dati in transito e l'aggiornamento degli strumenti di sicurezza del dispositivo.
Worm: sottoclasse di virus, software che crea diverse copie di se stesso in uno stesso computer, diffondendosi autonomamente attraverso reti e sistemi informativi.

QUADRO NORMATIVO DI RIFERIMENTO

Il presente Regolamento è redatto e aggiornato nel rispetto del seguente quadro normativo e regolatorio (come modificato e integrato nel tempo). Restano fermi gli ulteriori obblighi settoriali eventualmente applicabili.

A) Normativa dell'Unione Europea

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR).
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (c.d. "NIS2").
- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (c.d. "AI Act"), quale riferimento generale per l'uso di strumenti di intelligenza artificiale.

B) Normativa nazionale – Cybersicurezza e resilienza

- Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e resilienza delle pubbliche amministrazioni.
- Decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 (NIS2).
- Decreto-legge 14 giugno 2021, n. 82, convertito con Legge 4 agosto 2021, n. 109, relativo all'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN).
- Legge 23 settembre 2025, n. 132 Disposizioni e deleghe al Governo in materia di intelligenza artificiale

C) Normativa nazionale – Amministrazione digitale e comunicazioni

- Decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale – CAD) e s.m.i.
- D.P.R. 11 febbraio 2005, n. 68 (Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata – PEC).

D) Protezione dei dati personali e ambito lavorativo

- Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e s.m.i.
- Decreto legislativo 10 agosto 2018, n. 101 (disposizioni per l'adeguamento della normativa nazionale al Regolamento (UE) 2016/679).
- Provvedimento del Garante per la protezione dei dati personali del 1° marzo 2007 – Linee guida su posta elettronica e Internet nel rapporto di lavoro (quale indirizzo di contesto).
- Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), art. 4, e s.m.i.
- Decreto legislativo 14 settembre 2015, n. 151, art. 23 (modifiche all'art. 4 dello Statuto dei lavoratori).

E) Sicurezza sul lavoro, condotta e corretto uso delle risorse

- Decreto legislativo 9 aprile 2008, n. 81 (tutela della salute e della sicurezza nei luoghi di lavoro) e s.m.i.
- D.P.R. 16 aprile 2013, n. 62 (Regolamento recante codice di comportamento dei dipendenti pubblici) e s.m.i., nonché Codice di comportamento dell'Ente.
- Legge 22 aprile 1941, n. 633 (protezione del diritto d'autore e diritti connessi), per i profili di utilizzo del software e dei contenuti digitali.

F) Atti di indirizzo per la sicurezza ICT nella PA

- Determinazione Agenzia Nazionale Cybersicurezza 164179 (misure di sicurezza per soggetti NIS2 importanti)
- Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015 (indirizzi per la prevenzione e reazione ad eventi cibernetici per le pubbliche amministrazioni) e relativi atti attuativi.
- Agenzia per l'Italia Digitale (AgID) – Circolare 18 aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (e successive indicazioni applicative).

ART. 1.LINEE GUIDA GENERALI

1. Con il presente Regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche e dei dispositivi fissi e mobili (personal computer, smartphone, tablet, modem/router, etc.), qualora utilizzate come strumenti informatici, che AIPo, tramite il proprio Ufficio Sistema documentale, Sistemi informativi e digitalizzazione (di seguito "Ufficio Sistemi informativi" o "Ufficio S.I."), mette a disposizione del personale dipendente e non dipendente (di seguito "Utenti") per l'esecuzione delle funzioni istituzionali di competenza, non solo all'interno dei locali dell'Ente, ma anche in modalità remota o agile (*smart working).* rispetto della normativa vigente in materia di sicurezza informatica e cybersicurezza.
2. Scopo del Regolamento è la tutela dei beni di proprietà dell'Ente consegnati in uso ai propri dipendenti, al fine di evitare condotte inconsapevoli e/o scorrette, che possono esporre l'Agenzia a rischi connessi con la sicurezza, oltre ad eventuali danni patrimoniali a terzi, o di immagine.
3. Sono disciplinate, tra l'altro, le modalità con le quali l'Agenzia può accertare e inibire le condotte illecite degli utilizzatori degli strumenti e dei servizi informatici messi a disposizione (Internet, posta elettronica e accesso alle risorse di archiviazione di massa (server, hard disk), nel rispetto delle garanzie previste dalla normativa vigente.
4. I criteri che devono essere seguiti dagli Utenti per utilizzare gli strumenti informatici ~~e~~, compresi gli apparati di telefonia mobile detti smartphone, sono:
   a) rispetto delle leggi e norme vigenti, in particolare le leggi in materia di sicurezza dei dati, tutela della privacy, tutela del copyright e modalità di accesso e uso dei sistemi informatici e telematici;
   b) rispetto delle norme e procedure lavorative generali, definite dalle strutture competenti dell'Agenzia;
   c) rispetto delle norme e procedure specifiche definite dall'Ufficio Sistemi informativi dell'Agenzia, incluse le politiche e le misure di sicurezza informatica adottate dall'Ente.
5. Gli strumenti informatici oggetto delle presenti istruzioni sono gli apparati ed i servizi di proprietà (o affidati in uso) dell'Ente, messi a disposizione degli Utenti per svolgere quotidianamente il proprio lavoro: i PC, sia fissi che portatili, gli smartphone, la connessione ad Internet e gli strumenti di scambio di comunicazioni e file, la posta elettronica e la posta elettronica certificata, i programmi e gli applicativi in uso ai dipendenti tutti, e qualunque altro strumento riconducibile ad attività informatica quali portali web, piattaforme e applicativi messi a disposizione da e per AIPo, ivi inclusi i servizi erogati tramite infrastrutture cloud autorizzate dall'Ente. Rientrano altresì tra gli strumenti informatici, ai fini del presente Regolamento, le piattaforme, le applicazioni e i servizi basati su sistemi di intelligenza artificiale, compresi quelli accessibili tramite rete Internet, qualora utilizzati per finalità istituzionali o nell'ambito dell'attività lavorativa. L'utilizzo di tali strumenti è consentito esclusivamente nel rispetto della normativa vigente, delle politiche di sicurezza informatica dell'Ente e delle eventuali disposizioni specifiche adottate da AIPo. Con specifico riferimento agli strumenti di intelligenza artificiale, si applicano inoltre le disposizioni del Regolamento interno per l'utilizzo di sistemi di intelligenza artificiale, attualmente in fase di approvazione, che disciplinerà le condizioni e i limiti d'uso di tali tecnologie nell'ambito dell'attività istituzionale.
6. Attenersi alle regole descritte in questo documento è un preciso obbligo dell'Utente che utilizza gli strumenti informatici che gli sono stati assegnati, nonché un dovere di collaborazione attiva nella tutela della sicurezza dei sistemi informativi dell'Ente.
7. I responsabili degli uffici e dei settori devono verificare la corretta e puntuale messa in pratica delle disposizioni di cui al presente regolamento, al fine di garantire sui sistemi informativi dell'Agenzia:
   a) la riservatezza dei dati;

c) l'integrità dei dati;
d) la disponibilità dei dati, anche in relazione alla prevenzione e gestione di incidenti di sicurezza informatica.

8. La precisa applicazione del presente regolamento è adeguata alle misure minime di sicurezza previste dal Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101, che si adegua alle "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

9. La puntuale applicazione del presente regolamento e delle norme da questo richiamate permette ad AIPo di garantire un uso dello strumento informatico a norma di legge, attenendosi anche a quanto riportato nella Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativa a "Misure minime di sicurezza ICT per le pubbliche amministrazioni". (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). nonché alle disposizioni introdotte dalla Legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", e dal Decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2), in qualità di soggetto classificato come "soggetto importante", e alle linee guida e indicazioni operative emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN) ivi incluso, ove applicabile, il Regolamento (UE) 2024/1689 (AI Act)

10. Condotte non conformi al presente regolamento saranno valutate dalla Direzione competente, anche ai fini disciplinari, ferme restando le ulteriori responsabilità previste dalla normativa vigente.

11. Per l'uso dei sistemi informativi e di archiviazione dell'Agenzia, nonché degli applicativi in uso presso l'Agenzia stessa, sono assegnate a ciascun Utente specifiche credenziali di accesso, se in uso a determinati uffici/dipendenti (login e password e, ove necessario, PIN o ulteriori sistemi di autenticazione previsti). L'uso di tali credenziali è strettamente individuale e non deve essere condiviso con altre persone. L'Utente è responsabile delle credenziali a lui assegnate e della segretezza della propria password. Le credenziali individuali non possono essere comunicate a terzi, in quanto associate all'identità dell'utente assegnatario, e identificative dello stesso nell'ambito dell'operatività all'interno dei sistemi informativi. L'assegnazione delle credenziali avviene, di norma, sulla base di specifica richiesta formulata dal dirigente responsabile e inoltrata all'Ufficio Sistemi Informativi.

12. Gli strumenti informatici e i dispositivi mobili sono forniti all'Utente per finalità esclusivamente lavorative. Non è quindi permesso utilizzare tali strumenti per altre finalità non connesse all'attività lavorativa o in modi che violino le leggi italiane ed europee in materia di sicurezza sul luogo di lavoro o, in generale, tutte le altre leggi applicabili alla Pubblica Amministrazione.

13. Ciascun utente è direttamente responsabile dell'utilizzo efficace, efficiente ed eticamente corretto degli strumenti, dei servizi e dei sistemi informativi. L'uso inappropriato o illegale del proprio PC e relativi strumenti, programmi e applicativi può comportare severe violazioni, anche di natura penale, con le eventuali conseguenti azioni legali nei confronti del soggetto che abbia commesso illecito, ivi incluse le responsabilità derivanti da violazioni degli obblighi di sicurezza informatica.

14. Eventuali violazioni delle procedure di accesso e sicurezza dei sistemi informativi di cui un Utente venga a conoscenza devono essere immediatamente segnalate all'Ufficio Sistemi informativi dell'Agenzia, secondo le modalità definite dalle procedure interne di gestione degli incidenti di sicurezza informatica.

ART. 2.UTILIZZO DEL PERSONAL COMPUTER

1. I Personal Computer, siano essi portatili o fissi, ed i relativi programmi e/o applicazioni affidati al dipendente sono strumenti di lavoro. Pertanto, ciascun dipendente è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ai fini del presente Regolamento, i dispositivi mobili aziendali quali smartphone e tablet, qualora abilitati all'accesso ai sistemi informativi, alle applicazioni, ai dati o alle risorse dell'Ente, sono equiparati ai Personal Computer portatili.
2. Gli Utenti sono tenuti all'applicazione delle disposizioni e delle procedure di Legge e di lavoro dell'Agenzia relativamente alla custodia delle dotazioni, al fine di proteggere le apparecchiature informatiche assegnate da furti e dall'uso da parte di persone non autorizzate. Ogni Utente è inoltre responsabile dell'adozione di precauzioni adeguate alla sicurezza e la tutela delle apparecchiature informatiche dell'Agenzia non sorvegliate. Tali disposizioni sono volte anche ad evitare accessi non autorizzati alle predette apparecchiature.
3. Gli Utenti sono altresì tenuti a rispettare le disposizioni previste dalla normativa vigente in materia di tutela della salute e della sicurezza nei luoghi di lavoro (D.lgs 9 aprile 2008, n. 81 e smi) e le indicazioni specifiche fornite dagli organi dell'Agenzia competenti in materia.
4. Il PC deve essere utilizzato dagli Utenti con la dovuta cura. In particolare, l'Utente deve:
   a) assicurarsi che il proprio PC e ogni dispositivo mobile aziendale equiparato abbia attivata una procedura di autenticazione all'accensione;
   b) non lasciare il proprio PC o dispositivo mobile equiparato acceso e incustodito quando il proprio Utente è connesso e quindi l'accesso ai dati e alle applicazioni è garantito;
   c) assicurarsi che, allontanandosi dalla propria postazione, sia attivato lo screensaver fornito dal sistema operativo che richiede una password per essere disattivato ovvero le equivalenti funzionalità di blocco automatico previste sui dispositivi mobili;
   d) eseguire il processo di logout alla fine della sessione di lavoro e spegnere il pc ogni volta a fine giornata lavorativa, per permettere gli aggiornamenti necessari;
   e) salvare obbligatoriamente il proprio lavoro (file, dati e documenti) sulle risorse cloud/server aziendali, o sulle piattaforme gestionali a disposizione di AIPo, al fine di eliminare il rischio di perdita dei dati, e di avere accesso al proprio materiale di lavoro da qualsiasi postazione dell'Agenzia;
   f) nel caso di dati che debbano indispensabilmente essere salvati sulle unità locali del PC, l'utente è tenuto ad eseguire a propria cura il backup manuali degli eventuali dati locali (che non sono sotto altre procedure di backup);
   g) non modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione da parte dell'ufficio Sistema Informativo;
   h) non utilizzare gli strumenti di archiviazione (risorse CLOUD, dispositivi USB, hard-disk removibili per fini personali;
   i) non utilizzare strumenti di archiviazione, dispositivi o servizi non autorizzati dall'Ente per la memorizzazione o il trattamento di dati istituzionali;
   j) non duplicare o diffondere software o file illegali (musica, film, ecc.) o software personali;
   k) non duplicare o diffondere il software aziendale senza specifica autorizzazione.
5. Al fine di evitare il rischio di intrusione e diffusione di malware, ovvero software creati con il solo scopo di causare danni più o meno gravi al sistema su cui vengono eseguiti (rientrano in questa categoria virus, worm, spyware e altri programmi dannosi), che costituiscono una delle minacce più frequenti alla sicurezza, è necessario che il personale si attenga alle seguenti norme:
   a) verificare periodicamente l'effettivo funzionamento dei software di protezione appositamente installati sul sistema, e non disattivarli in nessuna occasione e per nessuna ragione. I software di protezione vengono aggiornati automaticamente tramite la rete interna dell'Agenzia; **è**

indispensabile, pertanto, collegare sistematicamente, almeno una volta in ogni giornata di utilizzo, il PC alla rete aziendale, anche tramite il collegamento remoto VPN, al fine di consentire l'esecuzione dei necessari aggiornamenti;

b) evitare il download e l'esecuzione di materiale che potrebbe contenere virus o altri software dannosi;
c) non scaricare mai file provenienti da mittenti sconosciuti o sospetti e, ove necessario, effettuare sempre un controllo tramite antivirus, prima di acquisire o aprire qualunque programma o documento acquisito via posta elettronica. In caso di dubbio contattare i Sistemi Informativi.

6. L'utente è responsabile del corretto utilizzo e della diligente custodia del PC portatile e dell'eventuale smartphone o dispositivo di connettività mobile assegnatogli dall'Agenzia, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro, che si tratti di una sede dell'Ente o di una postazione di smart working. In particolare, la mancata o impropria custodia della attrezzatura informatica e/o di telefonia/connettività da parte del dipendente assegnatario può condurre ad ipotesi criminose, nel caso in cui tale attrezzatura venga sottratta, soprattutto alla luce delle disposizioni contenute in materia di trattamento dei dati personali ex D.lgs 101/2018. Anche il danneggiamento dell'apparecchiatura, che cagiona danno all'Ente, è sottoposto alla responsabilità del dipendente e passibile di richiesta di risarcimento, ai sensi della normativa vigente. Con le postazioni portatili saranno forniti e collocati presso gli uffici appositi cavi di sicurezza in acciaio, con sblocco tramite chiave o combinazione numerica, in grado di ancorare il pc alla scrivania, rendendone difficoltosa l'asportazione, così da garantire la sicurezza della strumentazione nell'ufficio, in assenza di personale in loco. Nel tragitto tra il domicilio dell'utente o la postazione di Smartworking e la sede di servizio, il pc e/o i dispositivi mobili di servizio di servizio non devono essere mai lasciati incustoditi, devono essere utilizzati esclusivamente dal dipendente ai quali sono assegnati e devono essere riposti, quando inutilizzati, in un mobile o locale chiuso a chiave, o comunque non in vista, al fine di tutelare, anche in questo caso, sia l'integrità fisica dei dispositivi che quella dei dati, programmi, applicativi ai quali i dispositivi accedono, ovvero in essi contenuti.

7. **In caso di furto o smarrimento del dispositivo (PC o dispositivo mobile) l'Utente è tenuto a presentare immediatamente denuncia alle competenti Autorità di Pubblica Sicurezza, e ad avvertire tempestivamente l'Ufficio Sistemi Informativi., al fine di consentire l'attivazione delle misure di sicurezza e di gestione dell'incidente previste dall'Ente.**

8. Alla riconsegna del PC all'Ente, l'Ufficio sistemi informativi assicura la conservazione dei dati di profilo dell'utente, e di eventuali dati o documenti salvati sulle unità locali del PC per un periodo di trenta giorni dalla riconsegna stessa; dopo di che, ai sensi delle norme di tutela dei dati e di gestione dei sistemi, procederà all'eliminazione sistematica e definitiva di tutti i dati, i documenti e gli applicativi presenti sull'unità. secondo le procedure di sicurezza e conservazione adottate dall'Ente.

ART. 3. CONTROLLO DEGLI ACCESSI

1. L'assegnazione, la gestione e la revoca delle credenziali di accesso ai sistemi informativi avvengono secondo il principio della necessità e della minimizzazione dei privilegi, in coerenza con i ruoli e le funzioni assegnate agli Utenti.

2. L'accesso alla rete aziendale ed ai sistemi aziendali è protetto da password individuale, ovvero ulteriori sistemi di autenticazione previsti dall'Ente, che hanno il compito di prevenire accessi da parte di soggetti non autorizzati ai sistemi. In relazione a ciò, allo scopo di cautelare l'Agenzia da ogni tipo di manomissione, furto o distruzione di dati e delle relative conseguenze, sia sul piano operativo che legislativo (penale e civile) nonché in attuazione delle misure di sicurezza informatica e cybersicurezza previste dalla normativa, vigono le seguenti disposizioni:

a) **è vietato** connettere in rete stazioni di lavoro diverse da quelle di proprietà dell'Agenzia, comprese quelle personali dei dipendenti, ivi inclusi dispositivi mobili personali, se non dietro esplicita e formale autorizzazione dell'Ufficio Sistemi Informativi, rilasciata nel rispetto delle politiche di sicurezza informatica dell'Ente;
b) **è vietato** condividere cartelle in rete con servizi non messi a disposizione dall'Ente, ovvero mediante piattaforme, applicazioni o servizi di terze parti non autorizzati;
c) **è vietato** monitorare ciò che transita in rete, fatta salva l'attività di monitoraggio, analisi e controllo svolta dall'Ente, direttamente o tramite soggetti autorizzati, per finalità di sicurezza informatica, prevenzione degli incidenti e tutela dei sistemi informativi, nel rispetto della normativa vigente.

ART. 4.GESTIONE DELLE PASSWORD

1. La sicurezza dei servizi e delle procedure informatiche dell'Agenzia è basata sull'uso di password e, ove richiesto, di codici di sicurezza (PIN oppure OTP), nonché su ulteriori sistemi di autenticazione forte o a più fattori adottati dall'Ente in attuazione della normativa vigente in materia di cybersicurezza.
2. Pertanto, è necessario che ciascun Utente scelga una password "robusta" e che tale password sia mantenuta rigorosamente segreta. A questo scopo è necessario scegliere la propria password seguendo i seguenti requisiti minimi, comuni a tutti i sistemi:
   a) non è possibile impostare password di lunghezza inferiore a 8 caratteri;
   b) la password deve includere, di regola, almeno tre delle seguenti caratteristiche: lettera maiuscola, lettera minuscola, cifre, caratteri speciali da selezionare fra quelli messi a disposizione dal sistema di autenticazione;
   c) la password non deve far riferimento ad informazioni personali o al servizio al quale si accede, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.
3. È necessario cambiare la password con regolarità. Ad ulteriore garanzia di sicurezza, oltre che in adempimento a specifiche disposizioni legislative, le password di accesso ai sistemi sono soggette a rinnovo obbligatorio, con cadenza predefinita, con segnalazione all'utente dell'approssimarsi della scadenza. secondo le modalità tecniche stabilite dall'Ente per i singoli sistemi. Per la gestione delle credenziali eventualmente scadute sono messi a disposizione strumenti di "self-reset", tramite i quali l'utente può autonomamente procedere a rinnovare la propria password, oltre alla possibilità di ricorrere ai servizi di assistenza informatica.
4. La password individuale deve essere riservata. L'Utente, al riguardo, deve mantenere i seguenti accorgimenti:
   a) non trascrivere la password su pezzi di carta o post-it lasciati in vista sulla scrivania, o attaccati al monitor;
   b) non comunicare a nessuno la propria password;
   c) non condividere con nessuno la propria password;
   d) assicurarsi che nessuno guardi la tastiera con l'intenzione di memorizzare la password, mentre la si digita;
   e) non inviare la password tramite e-mail e, se proprio è necessario comunicarla, farlo a voce, per telefono o a mano in una busta chiusa, secondo modalità che non ne compromettano la riservatezza;
   f) non utilizzare la stessa password per più scopi o procedure informatiche;

g) non utilizzare la funzione di memorizzazione automatica delle password inclusa nei vari browser;
h) qualora sia stato affidato all'Utente l'utilizzo di una procedura informatica con una password di default, ed il sistema non lo richieda automaticamente al primo accesso, è necessario che l'Utente provveda a personalizzarla immediatamente al primo uso cambiandola con una password di propria scelta, impostata secondo i criteri sopra indicati.

5. Sui PC in dotazione al personale dell'Agenzia è installato un programma per la gestione ed archiviazione sicura delle password, denominato "Keepass". Qualora le password vengano scritte per fini di backup su tale strumento specifico, su altri file digitali o cartacei al di fuori delle procedure di sicurezza dell'Agenzia (es: file personali , è fatto obbligo che questi documenti siano ben custoditi e ne sia inibito l'accesso agli estranei, in conformità alle politiche di sicurezza informatica dell'Ente

ART. 5.UTILIZZO DEI DISPOSITIVI MOBILI DI SERVIZIO

1. L'assegnazione e l'uso dei dispositivi di telefonia e connettività mobile (cellulari, smartphone, tablet, modem/router, etc.), come quelle dei personal computer, devono rispondere all'interesse ed alle esigenze dell'Agenzia, al fine di migliorare la qualità del lavoro e della produttività, in un quadro di economia, efficacia ed efficienza. I dispositivi possono essere utilizzati come strumento informatico, sia per la gestione della comunicazione, ad esempio a mezzo e-mail, che per la navigazione online, oppure per la connettività Internet. e, qualora abilitati, per l'accesso ai sistemi informativi, alle applicazioni e ai dati dell'Ente.
2. È fondamentale, dunque:
   a) individuare le figure aziendali che necessitano di un dispositivo mobile per l'esercizio della propria mansione;
   b) razionalizzare e controllare le spese riguardanti i servizi di telefonia e connettività mobile dell'Agenzia;
   c) rispettare regole precise riguardo all'uso appropriato dei dispositivi mobili e delle relative utenze intestate all'Agenzia, ad iniziare da quelle già illustrate all'articolo 2, in merito all'utilizzo dei PC, fissi o portatili, in quanto applicabili ai dispositivi mobili equiparati agli strumenti informatici dell'Ente.
3. Il presente articolo è conforme ai principi e alle indicazioni riportate dalla normativa nazionale e in particolare dalla Legge n. 244 del 24 dicembre 2007, art. 2, commi 594-595.
4. Il dispositivo mobile aziendale può essere utilizzato solo per ragioni di servizio, ed è obbligo di ogni assegnatario farne un uso appropriato ed averne una diligente cura, custodia e conservazione. L'apparecchio affidato al dipendente non può essere dato in uso a colleghi o terzi, né utilizzato in modo tale da compromettere la sicurezza dei dati, dei sistemi o delle applicazioni dell'Ente, anche mediante l'installazione o l'utilizzo di applicazioni, servizi o configurazioni non autorizzati che comportino rischi per la sicurezza informatica.
5. La scheda SIM aziendale assegnata, come i dispositivi, dovrà essere utilizzata solo ed esclusivamente per ragioni di servizio. Pertanto, non è consentito attivare sulla stessa dei servizi in abbonamento o traffico dati per uso personale e/o non autorizzati dall'Agenzia.
6. Il dipendente dovrà inoltre custodire la scheda ove sono riportati vari codici PIN e PUK, adottando tutte le cautele necessarie ad impedirne l'uso improprio o non autorizzato.
7. Il dispositivo mobile aziendale è dato in uso all'assegnatario che, in analogia a quanto avviene per il personal computer e gli altri dispositivi informatici, ne diventa custode e responsabile del corretto utilizzo nel rispetto del presente regolamento. L'assegnazione dà luogo, in carico al titolare, delle medesime forme di responsabilità patrimoniale previste per i consegnatari di beni dell'amministrazione, come già richiamate all'articolo 2, anche con riferimento ai rischi di perdita, compromissione o accesso

non autorizzato ai dati e ai sistemi informativi dell'Ente, nonché degli obblighi in materia di sicurezza informatica connessi all'uso del dispositivo

8. Alla consegna del dispositivo mobile aziendale, della relativa SIM card e degli eventuali accessori forniti, l'assegnatario è tenuto, obbligatoriamente, a sottoscrivere le seguenti dichiarazioni:
   - presa in consegna del telefono cellulare aziendale e degli eventuali accessori forniti; - presa in consegna della SIM card aziendale;
   - dichiarazione di conoscenza delle disposizioni previste nel presente regolamento, così come riportato all'articolo 2.
9. Analogamente a quanto già indicato all'articolo 2 con riferimento ai personal computer, **il furto o smarrimento del dispositivo** (telefono cellulare o smartphone, dispositivo di connessione remota o scheda SIM) **deve essere immediatamente denunciato alle competenti Autorità di Pubblica Sicurezza, e tempestivamente comunicato - oltre che all'Ufficio Sistemi informativi - all'Ufficio Servizi generali e Manutenzione**, per favorire le opportune segnalazioni al gestore del Servizio, e consentire l'attivazione delle misure di sicurezza e di gestione dell'incidente previste dall'Ente.

ART. 6.L'USO DELLA RETE INTERNET

1. La navigazione su Internet, attraverso cavo di rete o Wi-Fi, qualora disponibile, è un servizio che viene messo a disposizione degli Utenti a supporto delle loro attività istituzionali.
2. Gli Utenti sono tenuti a:
   a) navigare per il tempo strettamente necessario e solo per fini di natura lavorativa o professionale;
   b) non navigare su siti aventi contenuti di dubbia integrità morale, siti di hackers e siti di distribuzione di informazioni relative a software illegale, ovvero su siti che possano comportare rischi per la sicurezza dei sistemi informativi dell'Ente;
   c) non fornire dati personali, numeri di carta di credito, l'indirizzo di posta elettronica, dati dell'Agenzia, su siti sconosciuti e la cui origine e gestione non sia certa e fidata, né inserire o trattare informazioni, dati o documenti dell'Ente su piattaforme online non autorizzate;
   d) non scaricare mai nulla da siti la cui origine e gestione non sia certa e fidata ed in particolare non installare mai sul proprio computer software, giochi o screensaver non connessi con la propria attività lavorativa e scaricati da siti terzi o da fonti che non siano autorizzate o previste dalle procedure dell'Agenzia;
   e) non utilizzare servizi di scambio di informazioni disponibili su Internet (ad es. wetransfer) a meno che non siano stati autorizzati o previsti dalle procedure dell'Agenzia, in quanto tali servizi possono comportare rischi di perdita, diffusione o trattamento non autorizzato dei dati.

3. L'uso improprio della navigazione su Internet può comportare diverse conseguenze dannose, sia per l'Utente che per l'Agenzia. Inoltre, può condurre a serie violazioni delle procedure di sicurezza dell'Agenzia, ed in particolare a furti o distruzione di dati o più gravi danni patrimoniali, perseguibili a norma di Legge, in particolare:

   a) l'uso eccessivo della navigazione su Internet per fini personali o non connessi all'attività lavorativa comporta ingenti perdite di tempo, minore produttività sul lavoro e considerevole impegno delle risorse di rete messe a disposizione dall'Agenzia;
   b) l'uso inappropriato della navigazione su Internet, ad esempio la visione di siti illegali, può portare a pesanti violazioni di legge;
   c) il download di software non autorizzato o sconosciuto può portare instabilità e inaffidabilità del proprio PC con conseguente riduzione delle prestazioni e violazione delle procedure di sicurezza.

Inoltre, può comportare la diffusione di codici malevoli (virus) all'interno della rete aziendale, con conseguenti violazioni delle norme disciplinari e di sicurezza e tutela dei dati. In particolare, può provocare l'introduzione di:

- software spia (spyware) che tracciano l'attività dell'utente sul dispositivo, e la comunicano a all'esterno all'insaputa dell'Utente stesso;
- virus che compromettono l'integrità e la funzionalità del dispositivo, che possono essere trasmessi verso i sistemi di archiviazione dei dati aziendali, e che possono provocare la perdita e/o distruzione di dati, anche critici;
- software installati in maniera trasparente per l'utente, che permettono il controllo remoto del nostro dispositivo e il furto di dati;

d) il download di software illegalmente duplicato comporta l'assunzione, a totale carico dell'Utente, di tutte le responsabilità conseguenti alla violazione della normativa sul copyright.

4. Eventuali comportamenti, eventi o anomalie rilevate durante la navigazione in Internet che possano far presumere un incidente o un rischio per la sicurezza informatica devono essere tempestivamente segnalati all'Ufficio Sistemi Informativi, secondo le procedure interne vigenti.

ART. 7.SOFTWARE DI FILE SHARING

1. Non è consentito agli Utenti di fare uso di software di file sharing non preventivamente autorizzati dai Sistemi.Informativi, ivi inclusi servizi, applicazioni o piattaforme di condivisione di file basati su tecnologie cloud o accessibili tramite rete Internet.
2. A tal fine è necessario seguire le seguenti regole:
   a) non installare sui propri dispositivi software di file sharing di nessun genere a meno che non sia stato fornito dall'Agenzia;
   b) non creare librerie sui propri dispositivi di file musicali o video o che nulla hanno a che vedere con l'attività lavorativa;
   c) non utilizzare software di file sharing eventualmente fornito dall'Agenzia per condividere con Utenti esterni risorse e file dei propri dispositivi, salvo esplicita autorizzazione e nel rispetto delle procedure e delle politiche di sicurezza dell'Ente;
   d) non utilizzare software di file sharing eventualmente fornito dall'Agenzia per condividere dati che nulla hanno a che vedere con l'attività lavorativa.

3. L'uso improprio di software, servizi o piattaforme di file sharing può comportare rischi di perdita, diffusione non autorizzata o compromissione dei dati dell'Ente e costituisce violazione delle disposizioni in materia di sicurezza informatica, con le conseguenti responsabilità previste dalla normativa vigente.

ART. 8. INSTANT MESSAGING, CHAT, PIATTAFORME DI COMUNICAZIONE E COLLABORAZIONE UNIFICATA

1. Non è consentito agli Utenti di fare uso di software di instant messaging, chat, piattaforme di comunicazione e collaborazione unificata (Teams, Meet, Lifesize, ecc.) per finalità non stabilite dalle Direzioni dell'Agenzia, ovvero al di fuori delle esigenze istituzionali e delle disposizioni organizzative dell'Ente.

2. A tal fine è necessario seguire le seguenti regole:

a) non installare sui propri dispositivi applicazioni di nessun genere a meno che non siano state fornite o autorizzate dall'Agenzia;
b) non utilizzare applicazioni di instant messaging, chat, piattaforme di comunicazione e collaborazione unificata eventualmente forniti dall'Agenzia per fini personali o con Utenti che non fanno parte del personale dell'Agenzia e non hanno rapporti lavorativi o professionali con essa;
c) non aprire eventuali allegati ai messaggi istantanei la cui provenienza non sia certa e non installare mai sui propri dispositivi software ricevuto in allegati di messaggi istantanei, in quanto tali comportamenti possono costituire veicolo di malware o tentativi di compromissione dei sistemi informativi.

3. L'utilizzo improprio o non autorizzato di strumenti di instant messaging, chat o piattaforme di comunicazione e collaborazione unificata può comportare rischi per la sicurezza informatica dell'Ente, inclusa la diffusione non autorizzata di dati e informazioni, e deve essere immediatamente segnalato all'Ufficio Sistemi Informativi qualora emerga il sospetto di un evento o incidente di sicurezza.

ART. 9. LA POSTA ELETTRONICA STANDARD E LA PEC

1. La posta elettronica, sia standard che PEC (posta elettronica certificata), è uno strumento che viene messo a disposizione degli Utenti per favorire lo scambio di informazioni e per migliorare la produttività del lavoro, ma non deve essere abusato e qualora utilizzato, deve essere utilizzato in modo consapevole, corretto e sicuro e nel rispetto delle procedure stabilite dall'Agenzia e delle leggi vigenti, nonché delle misure di sicurezza informatica adottate dall'Ente.
2. **La Posta elettronica ordinaria**

Si raccomanda agli Utenti di adottare cura e attenzione, nell'utilizzo della posta elettronica. A tal fine è necessario seguire le seguenti regole:
a) non utilizzare la casella di posta elettronica fornita dall'Agenzia per fini personali;
b) non inviare o promuovere la ricezione e la diffusione, tramite la posta elettronica, nel corpo o come allegato di un messaggio, di materiale pornografico, illegale, commerciale non connesso alle attività dell'Agenzia, spam o comunque non legato all'attività lavorativa e professionale;
c) non inviare all'esterno dell'Agenzia, nel corpo o come allegato di un messaggio di posta elettronica, materiale e/o documenti di proprietà dell'Agenzia senza l'autorizzazione di un dirigente o a meno che non sia previsto dalle procedure dell'Agenzia, nel rispetto delle classificazioni e delle misure di protezione dei dati;
d) inviare i messaggi di posta elettronica solamente ai destinatari indispensabili, evitando di coinvolgere nella lettura delle e-mail Utenti non necessari, ed utilizzare in modo discreto e responsabile la rubrica degli indirizzi e-mail di tutti gli Utenti;
e) sul dispositivo fornito dall'Agenzia utilizzare sempre e solo la casella di posta elettronica fornita e conseguentemente non installare/configurare, su dispositivi forniti dall'Agenzia, account di posta elettronica personali, al fine di evitare commistioni tra comunicazioni istituzionali e personali e ridurre i rischi di sicurezza;
f) qualora si ricevano messaggi che hanno provenienza ignota, dubbia o che presentano titoli ambigui regolarsi come segue:
   - non aprire messaggi la cui provenienza non sia certa;
   - non aprire mai allegati di messaggi di posta la cui natura non sia certa;
   - non aprire messaggi il cui oggetto/titolo è dubbio, anche se appaiono ricevuti da un mittente noto;

- non fornire informazioni personali o finanziarie o password in risposte a comunicazioni di dubbia provenienza;
- se possibile visualizzare i messaggi di posta elettronica sempre in formato "testo";
- in caso di necessità, mantenere disattivata l'anteprima nel programma di posta elettronica. Una mail visualizzata in formato HTML potrebbe contenere del codice in grado di inviare il vostro indirizzo e-mail al mittente. Mantenere disattiva l'anteprima del messaggio permetterà di poter eliminare il messaggio senza aprirlo;

g) qualora si ricevano messaggi che nulla hanno a che vedere con l'attività lavorativa e che si ritiene abbiano fini pubblicitari (SPAM);
   - non rispondere a messaggi di dubbia provenienza e che nulla hanno a che vedere con l'attività dell'Agenzia (SPAM);
   - non fornire dati finanziari e password di un utente, con il rischio di essere vittima di phishing; - non cliccare su link che si trovano all'interno di mail pubblicitarie;
   - non rispondere mai alle mail degli spammer, nemmeno per rimuovere il proprio nominativo dalla loro lista;
   - spostare i messaggi nella cartella SPAM del sistema di posta, in modo che il sistema stesso possa acquisire informazioni utili a ridurre o debellare l'intrusione;
h) segnalare all'Ufficio Sistemi informativi qualunque abuso del servizio di posta elettronica di cui l'utente sia venuto a conoscenza, nonché ogni messaggio, comportamento o anomalia che possa far presumere un incidente o un rischio per la sicurezza informatica.

3. **La PEC**

La posta elettronica certificata (PEC) è stata introdotta con il DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3" in cui vengono emanate le regole per l'utilizzo della PEC e viene stabilito, tramite l'Art. 4 comma 1, che la PEC consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge. Il suo utilizzo è regolamentato anche dal CAD (Codice dell'Amministrazione digitale) all'art. 6 e smi. La PEC ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale**. Il personale che ha in uso tale tipo di posta elettronica**, sia che si tratti di un indirizzo individuale o legato ad un determinato settore/ufficio/funzione, **deve rispettare le medesime regole sopraripportate, riguardante l'uso della posta elettronica standard in dotazione**, con particolare riferimento agli obblighi di sicurezza, riservatezza, integrità e tracciabilità delle comunicazioni.

ART. 10.SOCIAL NETWORK

1. Le indicazioni del presente articolo sono rivolte non solo al personale dell'Ufficio stampa e Comunicazione che si occupa della gestione delle pagine social dell'Agenzia, ma anche al resto del personale dipendente. In generale, si fa riferimento alla puntuale applicazione di quanto prescritto

nel vigente Codice di Comportamento dell'Agenzia, o altri provvedimenti o disposizioni, interni o esterni, che ne disciplinano in particolare l'ambito.

2. Al fine di tutelare l'immagine e la reputazione di AIPO in rete e salvaguardare i dipendenti e il loro lavoro, I dipendenti che accedono ai canali social dell'Agenzia tramite l'utilizzo delle credenziali di accesso istituzionale:
   a) agiscono in nome e per conto di AIPO, sono strettamente tenuti al rispetto delle regole sopra riportate e comunque a tutto quanto riportato nel presente Regolamento;
   b) sono personalmente responsabili della tenuta dell'account e della riservatezza dei codici di accesso ricevuti che non devono essere comunicati o condivisi con soggetti non autorizzati;
   c) non possono utilizzare i profili social dell'Agenzia per scopi privati, personali, politici o commerciali, né per la diffusione di informazioni, dati o contenuti non autorizzati o non coerenti con le finalità istituzionali.
3. La mancata osservanza di quanto sopraindicato sarà soggetto di opportune sanzioni.

4. Eventuali accessi non autorizzati, compromissioni degli account social istituzionali, pubblicazioni anomale o comportamenti sospetti rilevati sui canali social dell'Agenzia devono essere immediatamente segnalati all'Ufficio Sistemi Informativi, al fine di consentire l'attivazione delle misure di sicurezza e di gestione dell'evento previste dall'Ente

ART. 11.ACCESSO AI DATI

1. Tutti i dati e le informazioni trattate dalle procedure informatiche sono di proprietà dell'Agenzia. Pertanto, qualsiasi diffusione della loro conoscenza e del loro utilizzo al di fuori delle procedure definite all'interno dell'Agenzia deve essere esplicitamente avallata dalle Direzioni competenti, nel rispetto delle disposizioni normative vigenti in materia di protezione dei dati e sicurezza informatica.
2. È necessario seguire le seguenti regole:
   a) non utilizzare la rete dell'Agenzia per scambiare e/o condividere dati che nulla hanno a che vedere con l'attività lavorativa e non salvare sui server dell'Agenzia dati o file che nulla abbiano che vedere con l'attività lavorativa al fine di ridurre i rischi di esposizione e compromissione dei sistemi informativi;
   b) non visualizzare né copiare, senza averne l'autorizzazione, file o informazioni che si trovano sui PC di altri Utenti o sui server dell'Agenzia e che non abbiano attinenza con l'attività lavorativa dell'utente in coerenza con i profili di accesso assegnati e il principio della necessità di conoscenza;
   c) seguire le procedure di archiviazione standard dell'Agenzia per eseguire il salvataggio dei dati presenti sui dispositivi assegnati agli Utenti utilizzando esclusivamente le risorse, le piattaforme e i sistemi autorizzati dall'Ente

3 Ogni accesso, utilizzo o trattamento dei dati dell'Agenzia deve essere effettuato esclusivamente nell'ambito delle funzioni assegnate e secondo le autorizzazioni ricevute. Eventuali accessi non autorizzati, anomalie o comportamenti che possano far presumere un uso improprio o un incidente di sicurezza devono essere tempestivamente segnalati all'Ufficio Sistemi Informativi.

ART. 12.VIRUS

1. Come già accennato all'articolo 2, i virus e, più in generale, i software malevoli (malware) sono una delle principali cause di danni e inefficienze dei sistemi informativi. Al fine di minimizzare il rischio di infezione e di diffusione dei software malevoli è necessario seguire le seguenti regole:

a) **non disinstallare o disabilitare il software antivirus**, che deve sempre essere presente, attivo e aggiornato sul proprio PC e su ogni altro dispositivo aziendale equiparato che acceda ai sistemi informativi dell'Ente;
b) non installare sul proprio dispositivo software di nessun genere a meno che non sia stato fornito o autorizzato dall'Agenzia e nel rispetto delle politiche di sicurezza informatica adottate dall'Ente;

c) non collegare al proprio dispositivo apparecchi removibili di scambio dei dati (chiavette usb, hard disk esterni, ecc…) la cui provenienza non sia certa e sui quali possano essere contenuti virus o file infetti ovvero altri codici malevoli potenzialmente dannosi per i sistemi informativi;
d) non aprire messaggi di posta elettronica standard o certificata la cui provenienza non sia certa, né allegati o link contenuti in tali messaggi.

2 Qualsiasi comportamento anomalo del dispositivo, sospetto di infezione, avviso del sistema di sicurezza o evento che possa far presumere la presenza di software malevolo deve essere immediatamente segnalato all'Ufficio Sistemi Informativi, al fine di consentire l'adozione tempestiva delle misure di contenimento e gestione dell'incidente.

ART. 13.AGGIORNAMENTO E REVISIONE DEL REGOLAMENTO

Il presente Regolamento è soggetto a revisione periodica con cadenza almeno annuale, a cura dell'Ufficio Sistemi Informativi, al fine di garantirne la costante aderenza al quadro normativo vigente, all'evoluzione tecnologica e alle esigenze operative dell'Ente.

La revisione è inoltre disposta in via straordinaria ogni qualvolta intervengano modifiche normative o regolamentari rilevanti, nuove minacce informatiche di rilievo, o significativi cambiamenti organizzativi o tecnologici che rendano necessario un aggiornamento delle disposizioni.