Sistema Socio Sanitario
Regione Lombardia
ASST Ovest Milanese

DELIBERA 230 DEL 04/04/2025

OGGETTO: APPROVAZIONE DEL REGOLAMENTO PER L'ULIZZO DEI SISTEMI INFORMATIVI AI SENSI DELL'ART.32 DEL REGOLAMENTO UE 2016/679"

DELIBERAZIONE ADOTTATA DAL DIRETTORE GENERALE DOTT. FRANCESCO LAURELLI

SU PROPOSTA DEL DIRETTORE
SC AFFARI GENERALI E LEGALI

che, accertata la propria competenza, sottopone l'allegata proposta di deliberazione in ordine all'oggetto sopra specificato, attestando la legittimità e la regolarità tecnico amministrativa della stessa.

Il Direttore
SC AFFARI GENERALI E LEGALI
Avv. Giacomo Rossi

Attesta, altresì, che il presente provvedimento non comporta né oneri né introiti.

Il Direttore
SC AFFARI GENERALI E LEGALI
Avv. Giacomo Rossi

Vista l'attestazione di legittimità del presente atto

Il Direttore
SC AFFARI GENERALI E LEGALI
Avv. Giacomo Rossi

IL DIRETTORE GENERALE

RICHIAMATI:

- il D.Lgs. n. 502 del 30/12/1992 e ss.mm.ii., recante norme per il riordino della disciplina in materia sanitaria;
- la L. R. n. 33 del 30/12/2009 e ss.mm.ii. avente ad oggetto: "Testo unico delle leggi regionali in materia di sanità";
- la D.G.R. n. X/4476 del 10/12/2015 avente ad oggetto: "Attuazione L.R. 23/2015: costituzione dell'Azienda Socio Sanitaria Territoriale (ASST) Ovest Milanese";
- la deliberazione del Direttore Generale n. 1 del 02/01/2024, con la quale è stato preso atto della D.G.R. n. XII/1642 del 21/12/2023 con cui Regione Lombardia ha nominato il Dott. Francesco Laurelli Direttore Generale dell'Azienda Socio Sanitaria Territoriale Ovest Milanese, con decorrenza dal 1° gennaio 2024;
- la deliberazione del Direttore Generale n. 589 del 14/11/2024 "Presa d'atto della D.G.R. n. XII/3284 del 31/10/2024 ad oggetto: "Aggiornamento del Piano di Organizzazione Aziendale Strategico (POAS) 2022 - 2024 dell'Azienda Socio Sanitaria Territoriale (ASST) Ovest Milanese";
- la D.G.R. n. XII/3720 del 30/12/2024 avente ad oggetto: "Determinazioni in ordine agli indirizzi di programmazione del SSR per l'anno 2025 – (di concerto con il Vicepresidente Alparone e gli Assessori Lucchini e Fermi)";

PREMESSO che il Direttore proponente ha attestato la legittimità e regolarità tecnico amministrativa del presente provvedimento e riferisce in merito ai presupposti a fondamento dell'adozione dello stesso, come specificatamente di seguito argomentato;

RICHIAMATA la seguente normativa:

- D.Lgs 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" e ss.mm.ii.;
- Delibera del Garante della Privacy n. 13 del 1° marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e Internet";
- D.Lgs. 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale e ss.mm.ii;
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
- Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS);
- Circolare 18 aprile 2017, n. 2 dell'Agenzia per l'Italia digitale 'Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»';
- D.P.R. 13 giugno 2023, n. 81 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165»;
- Garante per la protezione dei dati personali - Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati;
- LEGGE 28 giugno 2024, n. 90 Disposizioni in materia di rafforzamento della cybersicurezza

nazionale e di reati informatici;

- Garante per la protezione dei dati personali - Provvedimento del 17 luglio 2024 sull'accesso alla posta elettronica da parte del datore di lavoro;
- Decreto Legislativo 4 settembre 2024, n. 138 - Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;
- Framework della Cybersecurity rilasciato da US National Institute of Standards and Technology (NIST);

EVIDENZIATO che:

- la progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'ASST Ovest Milanese a rischi di attacchi informatici, oltre che alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa;
- l'utilizzo delle risorse informatiche e telematiche deve quindi sempre ispirarsi al principio della diligenza e correttezza, e che il presente Regolamento interno è diretto a evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati e alla continuità operative;
- gli strumenti informatici costituiscono i veicoli dell'informazione aziendale e sono, a tale titolo, oggetto di controllo, sia per quanto riguarda l'accesso, sia relativamente al loro utilizzo, per garantirne integrità, disponibilità, corretto uso e sicurezza. Un uso corretto delle risorse informatiche a disposizione, dunque, è un dovere di ciascun operatore, nell'interesse di tutti.

DATO ATTO che, in attuazione della normative sopra richiamata, la Responsabile della S.C. Sistemi Informativi ha, pertanto, predisposto apposito regolamento che contiene le misure minime di sicurezza di cui al Regolamento UE/2016/679, oltre che le prescrizioni relative alle modalità ed ai doveri che ciascun operatore dell'ASST deve osservare nell'utilizzo della strumentazione informatica a disposizione;

DATO ATTO che il suddetto testo regolamentare è stato illustrato e, successivamente – in data 25 febbraio 2025 - inviato, da parte dell'Ufficio Relazioni Sindacali della S.C. Gestione Risorse Umane alle Organizzazioni Sindacali del Comparto, dell'Area Sanità e della PTA e che lo stesso ufficio ha comunicato, con nota conservata agli atti, di non avere ricevuto alcuna osservazione in merito;

RITENUTO, pertanto, di procedere all'approvazione del "*Regolamento per l'utilizzo dei Sistemi Informativi ai sensi dell'art. 32 del Regolamento UE 2016/679*", allegato alla presente deliberazione quale parte integrante e sostanziale;

EVIDENZIATO che Il nuovo regolamento entra in vigore a partire dalla data di pubblicazione del presente provvedimento e che da tale momento tutte le disposizioni in precedenza adottate in materia, devono intendersi abrogate e sostituite dalle prescrizioni di cui all'allegato regolamento;

DATO ATTO che il presente provvedimento non comporta né oneri di spesa a carico del bilancio aziendale, né introiti;

ACQUISITA l'attestazione di legittimità della presente deliberazione da parte del Direttore della SC Affari Generali e Legali tramite firma apposta alla stessa da parte del proponente;

ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario, del Direttore Socio Sanitario, resi per quanto di competenza, ai sensi dell'art. 3 del D.Lgs. n. 502/1992 e ss.mm.ii.;

DELIBERA

Per i motivi in premessa indicati e che si intendono qui integralmente richiamati:

1. di approvare il *"Regolamento per l'utilizzo dei Sistemi informativi ai sensi dell'art. 32 del Regolamento UE 2016/679"* allegato alla presente deliberazione quale parte integrante e sostanziale della stessa;

2. di dare atto che il suddetto Regolamento entra in vigore a partire dalla data di pubblicazione del presente provvedimento e che da tale momento tutte le disposizioni in precedenza adottate in materia, devono intendersi abrogate e sostituite dalle prescrizioni di cui all'allegato regolamento;

3. di dare atto che il Regolamento oggetto del presente provvedimento verrà pubblicato, oltre che nella sezione Amministrazione Trasparente del sito aziendale, anche nella intranet aziendale e ne verrà data ampia diffusione agli utenti;

4. di dare atto che il presente provvedimento non comporta né oneri di spesa né introiti;

5. di dare atto che l'esecuzione del presente provvedimento è affidata al Responsabile del procedimento il quale ne comunicherà l'avvenuta approvazione alle Strutture interessate per l'adempimento delle rispettive competenze così come individuate dal P.O.A.S.;

6. di dare atto che ai sensi dell'art. 17 comma 4 L.R. n. 33/2009 e ss.mm.ii. il presente provvedimento non è soggetto a controllo ed è immediatamente esecutivo ai sensi dell'art. 17, comma 6, L.R. n. 33/2009 e ss.mm.ii;

7. di disporre la pubblicazione del presente provvedimento all'Albo Pretorio online aziendale, ai sensi dell'articolo 17, comma 6, della L.R. n. 33/2009, e ss.mm.ii.

IL DIRETTORE GENERALE

(Dott. Francesco Saverio Laurelli)

IL DIRETTORE AMMINISTRATIVO	IL DIRETTORE SANITARIO	IL DIRETTORE SOCIO SANITARIO
(Dott.ssa Maria Luigia Barone)	(Dott. Valentino Lembo)	(Dott. Giovanni Guido Guizzetti)

SC AFFARI GENERALI E LEGALI
Responsabile del procedimento amministrativo: Brera Fiona Silvia
Addetto all'istruttoria: Brera Fiona Silvia
Allegati n. 1

Sistema Socio Sanitario

Regione Lombardia

ASST Ovest Milanese

REGOLAMENTO PER L'ULIZZO DEI SISTEMI INFORMATIVI

AI SENSI DELL'ART.32 DEL REGOLAMENTO UE 2016/679

Sistema Socio Sanitario
Regione Lombardia
ASST Ovest Milanese

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'ASST Ovest Milanese a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, il presente Regolamento interno è diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e alla continuità operativa.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Reg. UE 2016/679 contenente le misure minime di sicurezza.

Considerato inoltre che l'ASST Ovest Milanese, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti, sono state inserite nel regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione. A tal proposito si richiama anche quanto stabilito dal DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 giugno 2023, n. 81 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165».

Gli strumenti informatici costituiscono i veicoli dell'informazione aziendale e sono, a tale titolo, oggetto di controllo sia per quanto riguarda l'accesso sia relativamente al loro utilizzo, per garantirne integrità, disponibilità, corretto uso e sicurezza. Un uso corretto delle risorse informatiche a disposizione, dunque, è un dovere di ciascuno, nell'interesse di tutti.

2. Abbreviazioni

SISS : Sistema Informativo Socio Sanitario

UO: Unità Operativa

SIA: Sistemi Informativi Aziendali

PC: Personal Computer

VPN: Virtual Private Network

NIS: Network and Information Security

3. ENTRATA IN VIGORE DEL REGOLAMENTO E DIFFUSIONE

3.1. Il nuovo regolamento entra in vigore a partire dalla data di pubblicazione del provvedimento di adozione;

3.2. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

3.3. Il presente regolamento viene pubblicato sulla intranet aziendale e diffuso agli utenti.

4. CAMPO DI APPLICAZIONE DEL REGOLAMENTO

4.1. Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori coordinati e continuativi, collaboratori a progetto, in stage, volontari, ecc.).

4.2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore coordinato e continuativo, collaboratore a progetto, in stage, volontario, ecc.) in possesso di specifiche credenziali di autenticazione o autorizzato ad effettuare operazioni sui sistemi informativi dell'azienda. Ognuno, in relazione al proprio ruolo e responsabilità, dovrà informare adeguatamente i terzi circa gli obblighi richiesti dal presente documento, esigerne l'applicazione, segnalare eventuali violazioni e adottare gli opportuni provvedimenti.

5. UTILIZZO DEL PERSONAL COMPUTER

5.1. Il PC affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento o furto.

5.2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'ASST Ovest Milanese solo attraverso specifiche credenziali di autenticazione come meglio descritto successivamente nel presente Regolamento.

5.3. Salvo preventiva espressa autorizzazione del personale dei Sistemi Informativi non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

5.4. Ogni utente deve prestare la massima attenzione ai supporti rimovibili, avvertendo immediatamente il personale SIA nel caso in cui siano rilevati virus ed adottando quanto previsto dal capitolo relativo alle procedure di protezione antivirus.

5.5. Le postazioni devono essere, per quanto possibile, costantemente sorvegliate. In caso di allontanamento dalla propria postazione di lavoro, l'utilizzatore deve provvedere all'attivazione di tutte le cautele necessarie ad impedire l'accesso alle informazioni al personale non autorizzato. In particolare, si consiglia di bloccare l'accesso alla macchina mediante le apposite funzioni del sistema operativo o degli applicativi, e comunque effettuando la disconnessione dagli applicativi.

5.6. Il PC deve essere, se possibile, spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, poiché lasciare un elaboratore incustodito connesso alla rete espone al rischio di utilizzo da parte di terzi non autorizzati.

6. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI E PC PORTATILI

6.1. Tutti i PC portatili e i supporti magnetici rimovibili (CD e DVD, supporti USB, ecc.), contenenti dati personali nonché informazioni aziendali, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Dove tecnicamente possibile, applicare la cifratura al dispositivo mobile. I sistemi informativi si riservano di inibire l'utilizzo di supporti removibili mettendo a disposizione altre modalità di condivisione dati.

6.2. In ogni caso, i PC portatili e i supporti magnetici devono essere dagli utenti adeguatamente custoditi, anche riponendoli in armadi chiusi a chiave.

7. UTILIZZO DI PC PORTATILI, TABLET E SMARTPHONE

7.1. L'azienda può, per esigenze organizzative, consegnare ai lavoratori uno smartphone o un computer portatile o un Tablet ad uso lavorativo. I dispositivi affidati, devono essere utilizzati solo per lo svolgimento delle attività lavorative, non è quindi consentito l'utilizzo a carattere personale.

7.2. E' vietato effettuare la copia del contenuto della SIM affidata.

7.3. Per lo smartphone e il tablet è obbligatorio l'uso del PIN di sicurezza e l'uso di crittografia a protezione delle informazioni ivi memorizzate. Allo stesso modo, per il PC portatile è obbligatoria la crittografia del disco.

7.4. Non è possibile apportare modifiche alle impostazioni e misure di sicurezza attivate sullo smartphone ed al suo relativo profilo, così come sull'eventuale computer portatile e/o tablet.

7.5. In caso di cessazione del rapporto di lavoro, i dispositivi affidati dovranno essere restituiti alla proprietà e dovranno essere cancellati – prima della restituzione – tutti i dati ivi presenti sia sul telefono che sul pc come ad es. rubrica dei numeri di telefono, app e programmi installati, chat di messaggistica, cartelle di dati e documenti, cartelle di archiviazione di posta.

7.6. Il lavoratore è responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante le trasferte e gli spostamenti, sia durante l'utilizzo nel luogo di lavoro; deve sempre essere adottata ogni cautela per evitare danni o sottrazioni. In caso di furto, il lavoratore dovrà fare riferimento a quanto previsto dal documento aziendale 'Regolamento relativo alla violazione dei dati personali – data breach' e avvisare immediatamente il proprio responsabile.

7.7. L'azienda può, per esigenze organizzative e in accordo con il lavoratore, permettere allo stesso di utilizzare uno smartphone o un computer portatile personale ad uso lavorativo previa verifica dei criteri di sicurezza da parte dei sistemi informativi aziendali che si riservano la facoltà ad installare/rimuovere applicazioni sul dispositivo propedeuticamente al rilascio dell'autorizzazione all'utilizzo.

8. UTILIZZO DI STRUMENTI PER LA STAMPA DEI DOCUMENTI AZIENDALI

8.1. Tutti i documenti prodotti con sistemi di stampa comuni ossia stampanti, fax, fotocopiatrici in rete non devono essere lasciati incustoditi e devono essere immediatamente distrutti ove non più utili, avendo cura di impedire la ricostruzione delle informazioni ivi riportate.

9. UTILIZZO DELLA RETE E GESTIONE DELLE CARTELLE DIGITALI CONDIVISE

9.1. Per l'accesso alla rete, al pc, agli applicativi e alle cartelle digitali dell'ASST Ovest Milanese ciascun utente deve essere in possesso della personale credenziale di autenticazione.

9.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vengono comunicate esclusivamente e direttamente all'utente interessato.

9.3. L'eventuale reset delle credenziali avviene su richiesta scritta da parte dell'utente interessato, corredata da un documento di identità. Il reset avviene in orari lavorativi da parte di personale specifico dei sistemi informativi.

9.4. Le cartelle digitali presenti nei server o nel cloud dell'ASST Ovest Milanese sono aree di condivisione di informazioni strettamente professionali. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. A tal proposito potranno essere svolte dai sistemi informativi delle verifiche nel rispetto del principio di pertinenza e non eccedenza, con modalità graduale, secondo quanto stabilito dalle vigenti normative. Il personale SIA può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC sia sulle unità di rete.

9.5. Tutti i dischi o altre unità di memorizzazione locali (es. disco C:) ivi incluse le unità di memorizzazione a corredo degli apparati elettromedicali, non sono soggette a backup. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente utilizzatore.

9.6. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti (secondo il Massimario di Scarto) o inutili. Particolare

attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

9.7. Ogni Direttore/Responsabile di U.O. può richiedere l'accesso o la revoca per sé o per i propri collaboratori ad una serie di cartelle che permettano di tenere ordinate e strutturate le informazioni (files, documenti, foto …) all'interno di un'area esclusivamente dedicata al suo Servizio.

9.8. Gli utenti accedono ai servizi informatici, alle cartelle e agli applicativi per i quali sono stati espressamente autorizzati ed utilizzano gli stessi unicamente per scopi connessi all'attività lavorativa svolta per l'ASST Ovest Milanese.

9.9. Si precisa che le cartelle assegnate non sono da ritenersi cartelle personali, ma cartelle funzionali poste sotto il controllo della funzione medesima e del diretto superiore. È, pertanto, vietato rinominarle con Nome + Cognome o simili. Al termine del rapporto di lavoro queste cartelle restano nella disponibilità dell'ASST in qualità di Datore di Lavoro; l'utilizzatore ha l'obbligo di cancellare qualunque dato strettamente personale sia stato per errore ivi archiviato, lasciando nella cartella tutto il resto del materiale, a garanzia della continuità lavorativa dell'azienda.

9.10. Il Servizio Risorse Umane comunica tempestivamente al SIA l'avvenuta cessazione o l'interruzione temporanea del rapporto di lavoro dell'utente tale da consentire la disattivazione dell'utenza di dominio che è alla base di ogni accesso ai servizi informatici.

I Direttori/Responsabili di ciascuna U.O. verificano periodicamente e in corrispondenza di eventuali variazioni del proprio organico, le autorizzazioni concesse e i privilegi consentiti a ciascun utente che opera sotto la sua supervisione, comunicando tempestivamente ai Sistemi Informativi le eventuali modifiche/disabilitazioni da apportare alle autorizzazioni. Le autorizzazioni di accesso devono tenere conto del ruolo e dell'ambito di trattamento dei dati personali concesso alla propria U.O.

In caso di mobilità di un utente da un servizio ad un altro, il responsabile della U.O. cedente comunica a Sistemi Informativi la richiesta di disabilitazione degli accessi precedentemente richiesti specificandone la tipologia, es. nome delle cartelle condivise, applicativi, caselle di posta di ufficio.

10. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

10.1. L'accesso ai sistemi aziendali è basato su credenziali personali. Previa formale comunicazione del:

- Servizio Risorse Umane in caso di nuove assunzioni o interruzioni dei rapporti di lavoro;
- Responsabile della U.O. in caso di attivazione/disattivazione dell'utenza per l'accesso agli ambiti applicativi e alle cartelle condivise a supporto delle aree di propria competenza;

esse possono essere assegnate/revocate:

- Dai Sistemi Informativi nei casi di accesso ai servizi informativi della rete aziendale e degli applicativi gestiti direttamente (inclusa attivazione smart card o credenziali di operatore SISS)
- Dalle Direzioni dei servizi di riferimento (es. Direzioni Mediche; Servizi Amministrativi, Direttori U.O.C ecc.) per Siti, Portali di Informazione e Gestione, sistemi regionali e nazionali

- Dal fornitore di software e applicativi o portali on-line.

I metodi di autenticazione possono consistere nel:

- codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata, oppure
- autenticazioni con un terzo fattore basato su utilizzo di token o app su cellulare
  oppure
- utilizzo della smart-card operatore SISS o altri metodi di autenticazioni previsti dal sistema SISS
- utilizzo di SPID/CIE/CNS

10.2. Le password devono essere formate da lettere (maiuscole o minuscole) e/o numeri o caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno 14 caratteri e non deve contenere riferimenti agevolmente riconducibili all'utente. Il grado di complessità deve ricomprendere nella password: almeno una lettera maiuscola, almeno una lettera minuscola, almeno una cifra, almeno un carattere non alfabetico (es.! $, #, %).

10.3. L'utente procede alla modifica della parola chiave al primo utilizzo e, successivamente, almeno ogni 90 giorni e comunque ogni volta che ritenga vi siano rischi di riservatezza dei dati o rischi di sicurezza. A tal proposito i sistemi informativi si riservano di effettuare, anche senza preavviso, il reset della password e/o la disabilitazione prolungata ai servizi informatici aziendali nei casi in cui vengano rilevate situazioni di vulnerabailità.

10.4. Inoltre, le password scelte devono avere le seguenti caratteristiche:

- Non consentire il riconoscimento diretto e l'identificazione certa dell'utente (es. evitare di utilizzare username contenenti nome, cognome, data di nascita o comunque dati riferibili all'utente);
- Essere differenti dalle ultime tre password utilizzate sul medesimo account;
- Non devono mai essere rese leggibili al di fuori dei computer;
- Non devono essere conservate vicino al pc d'accesso alla quale fa riferimento;
- Non devono essere conservate nella custodia del computer portatile usato per collegarsi in remoto alla rete;
- Non devono essere mai conservate o memorizzate all'interno di programmi di connessione (es. browser di navigazione internet) o di altro genere.

10.5. Gli utenti sono responsabili per tutte le attività riguardanti gli accessi eseguiti utilizzando il proprio profilo.

10.6. Gli utenti non devono permettere ad altri di effettuare alcuna attività con il proprio profilo, così come agli utenti è proibito svolgere attività con profili di altri utenti.

11. PROTEZIONE ANTIVIRUS E SICUREZZA

11.1. Il sistema informatico dell'ASST Ovest Milanese è protetto da software antivirus installato su pc e server.

11.2. Nel caso il software antivirus rilevi la presenza di un virus o comunque in caso di sospetti di infezione ed anomalie, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso;
- scollegare il cavo di rete o disattivare la connessione wifi in essere;
- spegnere il computer in caso di impossibilità a procedere alla disconnessione della rete;
- segnalare prontamente l'accaduto ai Sistemi Informativi e all'help desk dell'assistenza tecnica informatica.

11.3. A tutela della sicurezza, si raccomanda di prestare la massima attenzione nell'apertura degli allegati dei messaggi di posta elettronica ed adottare comportamenti attenti seguendo regole di base tra cui:

- non aprire mail che provengono da mittenti sconosciuti, non sono attese o, comunque, hanno un carattere di anormalità;
- non aprire allegati se non si è certi della loro origine;
- non cliccare su link presenti nella mail, se non si è certi della provenienza;
- non eseguire file allegati alle mail se non si è certi della loro provenienza;
- non eseguire macro presenti in file allegati nella mail se non si è certi della provenienza;
- in caso di sospetti, prima di aprirla, accertarsi con il mittente sull'effettivo invio della mail;
- in caso di apertura dell'allegato scollegare immediatamente il pc dalla rete e spegnerlo avvisando l'help desk dell'assistenza tecnica.

Il sistema antivirus aziendale e i sistemi di prevenzione delle intrusioni sono dotati di un cruscotto di monitoraggio e controllo centralizzato dei rischi di vulnerabilità di ogni postazione e di ogni server che segnala anche la presenza di file infetti specificandone nome e percorso al fine di una precisa individuazione degli stessi. Qualora venga rilevato qualunque tipo di infezione o rischio, anche solo sospetto, i sistemi informativi si riservano ogni necessario intervento a garanzia della sicurezza aziendale, ivi incluse eventuali immediate disabilitazioni di utenze e di servizi applicativi coinvolti nonchè rimozione di file infetti provvedendo ad avvisare gli utenti interessati nei tempi, nelle modalità e nei contenuti consentiti dal contesto e dalle situazioni di urgenza.

12. APPLICATIVI SOFTWARE A SUPPORTO DEI PROCESSI AZIENDALI

12.1. I software sono applicazioni mediante le quali ogni utente può trattare e gestire le informazioni aziendali. Ogni utente in relazione alle responsabilità e all'attività lavorativa che svolge per conto dell'ASST Ovest Milanese può accedere con credenziali personali, se previamente autorizzato e abilitato, alle specifiche applicazioni a supporto dei processi aziendali.

12.2. Ogni forma di implementazione e/o attivazione di soluzione applicativa, soluzione hardware, soluzione medicale che preveda la gestione di dati, immagini o segnali deve essere preventivamente e per tempo sottoposta al vaglio del SIA e, per le soluzioni elettromedicali, anche a quello dell'Ingegneria Clinica.

12.3. Con riferimento alla finalità sopra descritta e al fine di meglio garantire il corretto utilizzo delle applicazioni in questione, non è consentito:

- utilizzare le applicazioni aziendali per scopi personali estranei all'attività lavorativa svolta per conto dell'ASST Ovest Milanese;
- copiare i dati aziendali e i dati personali, consultabili dalle applicazioni in oggetto, qualora tali operazioni non siano strettamente necessarie all'attività lavorativa svolta per conto dell'ASST Ovest Milanese;
- usare programmi diversi da quelli ufficialmente installati per conto della ASST Ovest Milanese né procedere in autonomia all'installazione di programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza della presente disposizione espone la stessa ASST Ovest Milanese a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, possono essere sanzionate.

13. USO DELLA POSTA ELETTRONICA

13.1. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

13.2. È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. L'utente deve essere consapevole che egli è responsabile, non solo per quello che può scrivere nelle e-mail, ma anche dell'uso dello strumento lavorativo messo a disposizione dall'azienda. L'invio di qualsiasi messaggio o documento allegato (archivio collegato) e l'utilizzo o il reinvio di qualsiasi messaggio o documento allegato ricevuti, impegna la responsabilità personale del mittente.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- diffondere tramite tale servizio contenuti che possono risultare offensivi o discriminatori per genere, orientamento sessuale, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- esprimere nei messaggi di posta elettronica opinioni di natura politica, religiosa, filosofica o di altro genere senza indicare espressamente che trattasi di opinioni personali, al fine di evitare che esse siano interpretate quali posizioni ufficiali dell'ASST Ovest Milanese;
- diffondere a soggetti indeterminati dati riservati e dati personali;
- diffondere opere protette dal diritto d'autore, siano esse di proprietà dell'ASST Ovest Milanese di terze parti;
- inviare intenzionalmente molteplici messaggi indesiderati (Spam), diffondere messaggi riportanti notizie false e inoltrare messaggi che invitano i destinatari ad inviare, a loro volta, questi ultimi ad altri indirizzi;
- utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mailing-list non attinenti all'attività lavorativa;
- configurare e installare sul dispositivo in dotazione sistemi di posta elettronica diversi da quelli autorizzati dai sistemi informativi aziendali;

- inviare messaggi di posta elettronica utilizzando false generalità;
- prendere visione della posta altrui se non previamente autorizzati per iscritto dall'interessato.

13.3. Messaggi di posta elettronica diretti all'esterno potrebbero, per errore, essere inviati a un destinatario errato o non conosciuto. Pertanto, si consiglia di verificare sempre attentamente che l'indirizzo di posta corrisponda effettivamente al destinatario e che eventuali file allegati siano intestati e destinati al ricevente. Inoltre, si raccomanda di proteggere con password documenti o fascicoli contenenti dati "sensibili" che vengono allegati ai messaggi di posta.

13.4. La casella di posta elettronica, sia essa personale o di ufficio, NON è un sistema di archiviazione dati ed è pertanto da considerarsi solo come sistema per gestire le comunicazioni. I documenti di rilevanza aziendale devono essere opportunamente archiviati, fascicolati e gestiti sul sistema di gestione documentale e protocollo generale.

13.5. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, superati e soprattutto allegati ingombranti. E' responsabilità dell'utente provvedere alla cancellazione di messaggi ed informazioni presenti nella casella di posta e/o nel dispositivo/PC assegnato il cui tempo di conservazione risulti sproporzionato agli scopi di utilizzo.

13.6. Il sistema informativo aziendale è dotato di un sistema antispam centralizzato che previene la ricezione di messaggi di posta indesiderati da parte degli utenti. Qualora dovessero comunque pervenire messaggi anomali o sospetti, occorre darne comunicazione immediata al personale SIA. Non si dovrà in alcun caso procedere all'apertura di eventuali file allegati a tali messaggi o dare seguito ai contenuti dei messaggi.

13.7. Qualora, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'utente sia impossibilitato ad accedere al contenuto dei messaggi della posta elettronica d'ufficio (es. segreteria@asst-ovestmi.it), dovrà avvisare il proprio responsabile che potrà autorizzare la delega ad un altro lavoratore (fiduciario) a verificare il contenuto di messaggi.

13.8. In caso di assenza programmata, l'utente deve impostare messaggi di risposta automatici contenenti i riferimenti (email e/o telefono) di un altro soggetto o altre modalità utili per contattare la struttura o il servizio.

13.9. A garanzia della continuità operativa dei servizi si raccomanda di evitare l'utilizzo di caselle di posta personali ma privilegiare le caselle di posta di ufficio in modo da consentire la tempestiva ed opportuna condivisione delle informazioni tra gli operatori.

13.10. Le utenze di accesso ai servizi aziendali e gli account email personali (es. xxxx.yyyyy@asst-ovestmi.it) saranno disattivati entro 5 gg dall'inizio dell'assenza per incarico full time presso altro ente o cessazione del rapporto di lavoro, in entrambi i casi previa comunicazione da parte del servizio Risorse Umane ai Sistemi Informativi .

13.11. Le caselle di posta elettronica sono archiviate su sistemi centralizzati protetti che possono risiedere nel data center aziendale o in cloud. Per ragioni di manutenzione ed assistenza tecnica gli amministratori di sistema possono accedere a qualunque casella di posta elettronica. Gli accessi verranno fatti esclusivamente

per: configurarle, dismetterle, manutenerle, o nei casi previsti dalle vigenti normative. L'accesso al contenuto delle caselle di posta è consentito al titolare del trattamento, per il tramite dell'amministratore di sistema, nel caso in cui la casella di posta elettronica sia stata utilizzata dal dipendente per la commissione di reati o illeciti di qualsiasi natura, nonché nel caso in cui vi sia il fondato sospetto che il dipendente abbia utilizzato la casella di posta elettronica impropriamente e/o per far fuoriuscire dalla rete aziendale informazioni aziendali e documentazione riservata di qualsiasi genere.

13.12. E' possibile per l'utente recuperare i messaggi di posta eliminati entro 30 gg dalla cancellazione del messaggio stesso.

13.13. La conservazione dei metadati - ossia delle informazioni relative ad operazioni di invio, ricezione e smistamento dei messaggi che possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati, l'oggetto del messaggio spedito o ricevuto - ha durata 90 giorni, tempo minimo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

13.14. Tutto il contenuto della casella di posta elettronica personale viene cancellato in caso di cessazione del rapporto di lavoro.

14. NAVIGAZIONE IN INTERNET

14.1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È severamente vietato al dipendente navigare su siti web caratterizzati da contenuti indecorosi, offensivi, non sicuri né leciti. A titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- caricare o scaricare software commerciale in violazione del "copyright";
- upload/download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (ivi compresi filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
- ogni genere di transazione finanziaria privata ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente connessi allo svolgimento dell'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line, bacheche elettroniche e registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- l'uso di servizi di rete con finalità ludiche;
- la conduzione di attività illegali;
- la predisposizione o l'invio di comunicazioni offensive, inclusi commenti o scherzi basati sulla razza, la nazionalità di origine, il sesso, l'handicap, la religione o le opinioni politiche;
- scommesse e giochi; sollecitazione di guadagni o benefici personali; rilevare o diffondere informazioni aziendali, o informazioni confidenziali, o private;

- simulare l'identità di qualcuno attraverso l'uso di pseudonimi o rinvio di messaggi;
- fare commenti o esprimere giudizi che potrebbero essere considerati diffamatori o pregiudizievoli;
- copiare qualsiasi software o file senza verificare la presenza di virus;
- permettere ad altre organizzazioni l'accesso non autorizzato ai sistemi dell'ASST Ovest Milanese;
- effettuare intenzionalmente qualsiasi azione che possa interferire con le misure di sicurezza;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- accedere al servizio Internet mediante sistemi di connessione personali (modem o "internet-Key" personali) se non per motivate necessità di urgenza del servizio.

14.2. Al fine di evitare la navigazione in siti pericolosi e non consentiti è attivo uno specifico sistema di filtraggio automatico dei siti che registra ogni tentativo di accesso e le postazioni da cui esso viene effettuato. Gli eventuali controlli compiuti dal personale SIA a garanzia della sicurezza e della continuità operativa aziendale potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante analisi dei "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda. L'azienda si riserva di monitorare, all'occorrenza, l'uso di Internet effettuato dai dipendenti, bloccando l'accesso a siti ritenuti non appropriati, nel rispetto dei principi di pertinenza e non eccedenza, con modalità graduale, nel rispetto della normativa vigente sulla privacy.

15. GESTIONE SICURA DELLE VIDEO CONFERENCE, COLLOQUI E LEZIONI ONLINE

15.1. Gli utenti che conducono incontri, riunioni di lavoro o colloqui in videoconferenza, sono tenuti ad osservare le seguenti cautele:

- esplicitare le identità e i ruoli di ogni partecipante;
- evitare la presenza di terze persone estranee agli scopi durante i colloqui a distanza;
- non registrare né fotografare (anche mediante screenshot) i soggetti coinvolti nel colloquio, incluso il personale dell'Azienda se non dietro acquisizione del consenso;
- assicurarsi, di volta in volta che i contatti forniti siano corretti e che nessun soggetto esterno possa avere accesso al colloquio e alle informazioni scambiate;

16. ACCESSO AI DATI TRATTATI DALL'UTENTE

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'azienda, tramite il personale SIA o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti e dati ivi contenuti.

17. MODALITA' DI ASSISTNZA TECNICA DA REMOTO

I sistemi informativi e/o i tecnici delle aziende che forniscono assistenza tecnica potranno collegarsi da remoto sul pc dell'utente per risolvere malfunzionamenti, effettuare installazioni di programmi, fare delle verifiche tecniche, assicurarsi del corretto funzionamento delle postazioni e degli applicativi ivi installati.

La connessione avviene dal pc del tecnico al pc dell'utente collegato alla rete aziendale e consente al tecnico di visualizzare l'intero desktop del pc su cui presta assistenza.

18. SISTEMI DI CONTROLLI GRADUALI

Il personale dei Sistemi Informativi della ASST Ovest Milanese è autorizzato – per motivi tecnici - a compiere interventi nel sistema informatico aziendale atti a garantire la sicurezza, la salvaguardia, la continuità operativa del sistema stesso, nonché assicurarne la manutenzione (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, rimozione file infetti, modifiche di configurazioni, disabilitazioni di funzionalità, dismissione di strumenti e programmi obsoleti, etc.).

18.1. Il personale incaricato del SIA ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità ed emergenza, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico a prescindere dal consenso dell'utente.

18.2. In caso di anomalie o rilevazione di un utilizzo irregolare degli strumenti informatici, il personale del SIA effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, e si inviteranno gli interessati ad attenersi scrupolosamente alle disposizioni del presente regolamento. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

18.3. A garanzia della sicurezza e della continuità operativa vengono tracciati gli accessi ai sistemi e agli applicativi attraverso la generazione automatica di file di log. L'Azienda, per tramite del personale del SIA o dei fornitori incaricati, si riserva la possibilità di effettuare controlli sul registro degli accessi (log) in conformità alla legge, per:

- individuare fattori di rischio in materia di privacy,
- effettuare verifiche sulla funzionalità e sicurezza del sistema;
- istruire incidenti e segnalazioni di data breach;
- ottemperare alla normativa che impone il controllo degli accessi sugli amministratori di sistema interni o esterni alla struttura;
- fornire alle Autorità competenti fonti certe relative ad accessi illeciti o operazioni non consentite da parte degli utenti.

Si precisa che nel caso, durante i controlli, si rilevassero abusi singoli o reiterati, questi saranno oggetto di istruttoria, anche mediante il coinvolgimento stesso del lavoratore, al fine di constatare i presupposti di un data breach.

19. CONNESSIONI REMOTE (VPN) PER ESPLETAMENTO ATTIVITA' LAVORATIVE

AMBITO DI APPLICAZIONE

Le disposizioni di cui al presente capitolo si applicano alle attività da svolgere in remoto tramite un collegamento alla rete aziendale dall'esterno. Sono escluse dalle funzioni applicative remotizzabli quelle per le quali è necessario l'utilizzo di macchine o strumentazioni presenti in azienda e qualunque altro servizio le cui caratteristiche tecniche, a giudizio dei sistemi informativi, non rendono possibile la remotizzazione o non la rendono possibile in modo sicuro.

MALFUNZIONAMENTO

In caso di problematiche di natura tecnica e/o informatica, e comunque in caso di cattivo funzionamento dei sistemi informatici, qualora lo svolgimento dell'attività lavorativa a distanza sia impedito o sensibilmente rallentato, il dipendente è tenuto a darne tempestiva informazione al proprio Responsabile. Questi, qualora le suddette problematiche dovessero rendere temporaneamente impossibile o non sicura la prestazione lavorativa, può richiamare il dipendente a lavorare in presenza.

In caso di rischi di sicurezza, si precisa che i sistemi informativi hanno l'obbligo di intervenire tempestivamente all'interruzione della connessione dandone successivamente comunicazione al responsabile e all'utente.

LAVORO AGILE

Per l'utilizzo di connessioni remote a supporto dello svolgimento di lavoro agile, si rimanda alla Delibera n. 489 del 19.09.2024 e ss.mm.ii, nonché ai provvedimenti aziendali specifici.

20. MANCATA OSSERVANZA DELLE DISPOSIZIONI DEL REGOLAMENTO

Le disposizioni del presente regolamento rivestono carattere di obbligatorietà e la loro mancata osservanza costituisce illecito disciplinare. Inoltre, ricorrendone gli estremi, i fatti posti in violazione delle presenti disposizioni potranno essere segnalati alle autorità competenti. In particolare, si richiama l'art. 615-quinquies Codice Penale che recita testualmente: «Diffusione di programmi diretti a danneggiare od interrompere un sistema informativo: Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro.»

21. RIFERIMENTI NORMATIVI

- Decreto legislativo 30 giugno 2003, n. 196, intitolato “Codice in materia di protezione dei dati personali “, noto anche come Testo unico sulla Privacy o Codice sulla Privacy entrato in vigore dal 1º gennaio 2004 e Aggiornato al D.ls 101/2018;
- Reg. UE 2016/679
- Delibera n. 13 del 1° marzo 2007 “Lavoro: le linee guida del Garante per posta elettronica e Internet”;
- CIRCOLARE 18 aprile 2017 , n. 2/2017 dell’Agenzia per l’Italia digitale ‘Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».’
- Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS)
- Framework della Cybersecurity rilasciato da US National Institute of Standards and Technology (NIST)
- Decreto Legislativo 7 marzo 2005, n. 82 – Codice dell’amministrazione digitale e ss.mm.ii.
- DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 giugno 2023, n. 81 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165».
- Garante per la protezione dei dati personali - Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati
- Garante per la protezione dei dati personali - Provvedimento del 17 luglio 2024 sull’accesso alla posta elettronica da parte del datore di lavoro
- Decreto Legislativo 4 settembre 2024, n. 138 - Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148
- LEGGE 28 giugno 2024, n. 90 Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.
- DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 giugno 2023, n. 81 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165». (23G00092) (GU n.150 del 29-6-2023)

22. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione a seguito di modifiche organizzative o normative.