SOMMARIO

il presente regolamento e' adottato con deliberazione n. 720 del 25/06/2021

PREMESSA

Le tecnologie dell'informazione e della comunicazione assumono un ruolo sempre più importante all'interno della pubblica amministrazione, rappresentando uno strumento a supporto al cambiamento innovativo della Pubblica Amministrazione (PA) per una miglior efficienza.

Nel contempo la sicurezza informatica è necessaria per garantire disponibilità, integrità e riservatezza delle informazioni del Sistema informativo della Pubblica Amministrazione. L'individuazione di regole precise e chiare per l'utilizzo delle risorse interne dell'Azienda, da parte dei dipendenti e dei collaboratori, è un passaggio necessario nel percorso che porta dell'ottimizzazione del funzionamento dell'organizzazione.

ARTICOLO 1. SCOPO E FINALITA'

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda Ospedaliero Universitaria Sant'Andrea (di seguito AOUSA) adotta il presente Regolamento per i seguenti scopi e finalità:

- Tutela del lavoratore. Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.
- Diritti di protezione dei dati personali. Nell'impartire le seguenti prescrizioni l'AOUSA tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (art. 1 Regolamento UE 2016/679- artt. 1 e 2, D.Lgs. 196/03 - Codice in materia di protezione dei dati personali e s.m.i).
  Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica. I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza dei principi di necessità, correttezza, per finalità determinate, esplicite e legittime osservando il principio di pertinenza e non eccedenza e nella misura meno invasiva possibile.
- Principio di trasparenza. In base al richiamato principio di correttezza, l'AOUSA ispira il presente regolamento ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4 Statuto dei lavoratori).
- Regole di utilizzo. Assicurare la funzionalità e il corretto impiego degli strumenti aziendali da parte dei lavoratori, definendo le modalità d'uso nell'organizzazione dell'attività lavorativa.
- Misure tecniche ed organizzative adeguate. Mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

ARTICOLO 2. AMBITO DI APPLICAZIONE

Il regolamento si applica a tutti i dipendenti e collaboratori interni ed esterni dell'azienda a prescindere dal rapporto contrattuale intrattenuto con la stessa (tra questi rientrano anche i lavoratori somministrati, i collaboratori a progetto, in stage, specializzandi, ecc.) che utilizzano i sistemi e gli apparati messi a disposizione dall'Azienda stessa.

Il presente Regolamento disciplina l'utilizzo di tutti i servizi/strumenti messi a disposizione dall'AOUSA per consentire lo svolgimento delle attività lavorative degli utenti quali ad esempio: personal computer e relativo accesso alle applicazioni aziendali, smartphone, cellulari, tablet, sistemi di autenticazione informatica, Internet, cartelle di rete, posta elettronica, Posta Elettronica Certificata, Sistema di firma digitale e qualsiasi altra tecnologia destinata a trattare, memorizzare o a trasmettere dati e informazioni.

ARTICOLO 3. ACRONIMI E DEFINIZIONI

AOUSA	Azienda Ospedaliero-Universitaria Sant'Andrea
PA	Pubblica Amministrazione
UO	Unità Operativa
UOC SIeTC	UOC Sistema Informativo e Tecnologie della Comunicazione
UOC RM,Q&A	UOC Risk Managent, qualitá e accreditamento
Amministratore di sistema	La figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi compresi gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
Banca dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
Credenziali di autenticazione	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Categorie particolari di dati	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Interessato	La persona fisica cui si riferiscono i dati personali.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
Strumenti elettronici	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Violazione di dati personali	Violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione.

ARTICOLO 4. RIFERIMENTI NORMATIVI

- Codice civile artt. 2104 e 2105
- Legge n. 300/1970 Statuto dei lavoratori
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio- GDPR - Regolamento generale sulla protezione dei dati
- Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003 e successive modifiche ed integrazioni)
- D.lgs. n. 242/1996 Modifiche ed integrazioni al decreto legislativo 19 settembre 1994, n. 626, recante attuazione di direttive comunitarie riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro (in tema di controlli operati mediante il sistema informatico aziendale)
- D.lgs. n. 101/2018 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- D. lgs 82/2005 Codice dell'Amministrazione Digitale – CAD aggiornato con il D.lgs 179/2016 e s.m.i.
- 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 (G.U: 28 Marzo 2005 n. 97)
- Linee guida del Garante della Privacy per posta elettronica e internet emanate con Delibera
- n. 13 del 1° marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007
- Linee guida del Garante in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico – Deliberazione n. 23 del 14 giugno 2007 Gazzetta Ufficiale 13 luglio 2007, n. 161
- Linee guida del Garante della Privacy in tema di referti on-line del delibera n. 21 del 25 giungo 2009
- Provvedimento del Garante della Privacy - Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015
- Guidelines on personal data breach notification under Regulation 2016/679 – Article 29 Data Protection Working Party
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019
- Articolo 615 ter codice penale (accesso abusivo ad un sistema informatico e telematico)
- Articolo 640 ter codice penale (frode informatica)

ARTICOLO 5. UTILIZZO DEI DISPOSITIVI INFORMATICI

Ogni collegamento alla rete aziendale di un dispositivo deve essere autorizzato dalla UOC Sistemi Informativi e Tecnologie della Comunicazione.
I dispositivi informatici (Personal Computer fissi e portatili, tablet, Palmari, lettori di vario genere, stampanti, altri strumenti messi a disposizione) sono affidati al personale dietro esplicita e preventiva richiesta da parte del Direttore/Responsabile della Unità Operativa di appartenenza.
E' compito della UOC SIeTC valutare lo stato di obsolescenza del materiale affidato e prevedere dei piani di sostituzione dello stesso.
Tali apparati devono essere considerati come strumenti di lavoro e pertanto:

- devono essere custoditi in modo appropriato (per i personal computer portatili si deve evitare l'abbandono, anche provvisorio, in luoghi quali uffici aperti, sale riunioni, nell'automezzo in aree di parcheggio e in caso di utilizzo interno devono essere riposti in armadi con serratura al termine dell'attività lavorativa o assicurati con il cavetto/lucchetto di sicurezza);
- devono essere utilizzati per fini professionali;
- l'eventuale furto/danneggiamento o smarrimento deve essere prontamente denunciato all'autorità di pubblica sicurezza e all'AOUSA;

- nel caso di utilizzo di personal computer portatili all'esterno dell'azienda, conservare sul disco solo i file strettamente necessari;
- in caso di furto o smarrimento, conseguenza del non rispetto delle regole di conservazione degli strumenti assegnati, possono essere attivati dall'azienda meccanismi di rimborso del danno subito (bene e attività correlate) e possono essere applicate sanzioni disciplinari;
- è obbligatoria la rimozione di qualsiasi dato dai dispositivi aziendali utilizzati prima della loro riconsegna;
- al termine del rapporto di lavoro con l'AOUSA l'utente dovrà inviare i dati attinenti alla propria attività lavorativa all'ufficio di competenza, dovranno essere riconsegnati i dispositivi privi di qualsiasi dato e non sarà consentito alcun accesso ai dati ad altro utente.
- è assolutamente vietato l'utilizzo di contenuti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

La UOC SIeTC ha il compito di installare correttamente, per quanto di competenza, le postazioni di lavoro e informare/formare i lavoratori sull'utilizzo dei software installati o resi disponibili sui server aziendali.

ARTICOLO 6. UTILIZZO PERSONAL COMPUTER

- All'utente non è consentito modificare le caratteristiche hardware e software del PC, compresa la configurazione di rete.
- Alla conclusione del proprio turno/giornata di lavoro è necessario spegnere il PC se l'utilizzo è esclusivo altrimenti è necessario disconnettersi (logout).
- Non è consentito lo spostamento dei PC e delle relative periferiche.
- Qualora l'utente debba allontanarsi dalla propria postazione di lavoro è tenuto ad eseguire una delle seguenti operazioni: spegnimento, blocco o disconnessione dalla sessione di lavoro.
- Non è consentita l'archiviazione di dati (in particolare personali e/o sensibili) all'interno dei PC aziendali se non per esigenze estemporanee; la UOC SIeTC non è responsabile dell'integrità dei dati archiviati localmente.
- Nel caso di PC portatili, l'utente è tenuto a collegarsi periodicamente alla rete aziendale per consentire l'aggiornamento del software di sistema.
- Non è consentito scaricare file contenuti in supporti di memorizzazione esterni non aventi alcuna attinenza con la prestazione lavorativa.

ARTICOLO 7. UTILIZZO SUPPORTI RIMOVIBILI

- È vietato memorizzare su qualsiasi tipo di supporto rimovibile (CD e DVD, chiavette USB, ecc.) dati personali e dati appartenenti a categorie particolari nonché know-how aziendale.

ARTICOLO 8. UTLIZZO DI STAMPANTI, FOTOCOPIATRICI E FAX

- È vietato l'utilizzo delle fotocopiatrici e stampanti aziendali per fini personali.
- Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato. Il materiale cartaceo non più necessario dovrà essere distrutto.
- La stampa di documenti informatici deve essere limitata all'attività lavorativa e in ogni caso per documenti per cui esiste l'assoluta necessità di disporre della copia cartacea.
- È esclusa la trasmissione di documenti tra pubbliche amministrazioni a mezzo fax.

ARTICOLO 9. UTILIZZO CREDENZIALI DI AUTENTICAZIONE

È responsabilità delle singole persone autorizzate al trattamento applicare le seguenti modalità operative:

- Le credeziali sono rilasciate dalla UOC SIeTC a seguito di approvazione dalla UOC RM,Q&A per la dirigenza medica, dalla UOC Professioni sanitarie per il personale del comparto sanitario e da altra Direzione o UOC di appartenenza per tutte le altre strutture. A tal fine, l'utente appartenente a

qualsiasi struttura fa richiesta di credenziali di autenticazione su apposito modulo disponibile nell'archivio documentale aziendale (M/919/37), che deve essere debitamente compilato, autorizzato dal Direttore/Responsabile della Unità Operativa di afferenza ed inviato mediante protocollo unitamente alla fotocopia di un documento d'identitá alla struttura competente per l'approvazione (UOC RM,Q&A, UOC Professioni sanitarie, altre Direzioni, UOC di appartenenza per le altre strutture).

- Le credenziali di autenticazione devono essere custodite con la massima diligenza e segretezza da parte dell'incaricato;
- Nel caso le credenziali siano costituite da una coppia username/password, devono essere adottate le seguenti politiche di gestione delle password:
    - La password deve essere formata da almeno otto caratteri, con lettere maiuscole e/o minuscole, numeri e/o caratteri speciali, in combinazione fra loro, senza riferimenti agevolmente riconducibili all'incaricato;
    - È obbligatorio modificare la password al primo utilizzo e, successivamente, almeno ogni 90 giorni oppure ogni qualvolta vi sia dubbio sulla sua segretezza; inoltre le password impiegate devono essere diverse dalle ultime 10 utilizzate;
- L'utente è responsabile, sia nei confronti di terzi che dell'Azienda, dell'attività svolta a seguito dell'autenticazione effettuata;
- È vietato accedere alle postazioni di lavoro con credenziali altrui;
- Per le abilitazioni assegnate ai dirigenti medici è obbligo del Direttore/Responsabile della Unità Operativa comunicare alla UOC RM,Q&A eventuali variazioni necessarie (modifica o revoca) afferenti alla propria UO (es. modifica incarico, dimissione ecc); la UOC RM,Q&A, comunicherá alla UOC SIeTC le modifiche da apportare;
- Per le abilitazioni assegnate a tutte le altre strutture è obbligo del Direttore Responsabile della Unità Operativa complessa comunicare, eventuali variazioni necessarie (modifica o revoca) afferenti alla propria UO (es. modifica incarico, dimissione ecc), alla UOC SIeTC le modifiche da apportare;
- La UOC SIeTC manterrá gli elenchi aggiornati di tutto il personale abilitato alle varie utenze;
- La UOC SIeTC si riserva la facoltà di introdurre nuove tecniche di accesso ai sistemi che garantiscano una maggiore sicurezza per la tutela dei dati;
- Le credenziali di amministratore di sistema assegnate devono essere utilizzate esclusivamente per effettuare operazioni che ne richiedano i privilegi e non per la normale prassi lavorativa;
- Le credenziali degli amministratori di sistema devono avere requisiti di robustezza elevati, utilizzando password di lunghezza minima di 8 caratteri alfanumerici, maiuscole, minuscole e caratteri speciali, non deve essere agilmente riconducibile all'amministratore e deve essere cambiata ogni 90 giorni oppure ogni qualvolta vi sia dubbio sulla sua segretezza; inoltre le password impiegate devono essere diverse dalle ultime 10 utilizzate;
- La lista degli amministratori di sistema viene pubblicata nella sezione privacy presente sull'intranet aziendale.

ARTICOLO 10. UTILIZZO DELLA RETE INTERNET

Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale destinato, in via prioritaria, allo svolgimento dell'attività lavorativa. La navigazione al fine di ricerca di informazioni deve limitare quanto più possibile l'utilizzo della banda di connessione.
Sono vietate in modo tassativo le seguenti attività:

- utilizzo di modem per i PC collegati alla rete;
- download/upload di software e/o contenuti non autorizzati o comunque non legati all'attività lavorativa;
- utilizzo dei servizi di messaggistica istantanea (esclusi quelli espressamente autorizzati dall'azienda); programmi di condivisione file (file sharing); di programmi P2P;
- partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati),

di bacheche elettroniche anche utilizzando pseudonimi (o nicknames);
- l'utilizzo di qualsiasi software che consenta l'accesso alla postazione di lavoro o ai dati istituzionali al di fuori della rete aziendale (condivisione dati online);
- la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

È responsabilità personale dell'utente qualsiasi danno arrecato all'Azienda nell'utilizzo della connessione ad Intenet in termini di sicurezza o di illecito commesso durante l'utilizzo di internet.

ARTICOLO 11. UTILIZZO SOCIAL NETWORK

All'utente è fatto divieto di utilizzare anche in forma privata i social network durante l'orario di lavoro.

L'utente nell'utilizzo in forma privata, fuori dall'ambiente di lavoro, dei propri profili social è tenuto, anche in quanto pubblico dipendente, a non effettuare commenti denigratori o lesivi in genere della dignità di terzi e/o dell'Azienda. È altresì fatto assoluto divieto pubblicare qualsiasi contributo in forma di immagine, di documento o qualsiasi altro formato realizzato all'interno dell'Azienda.

Quale conseguenza di utilizzo improprio dei propri profili social che possano essere considerati lesivi della dignità, reputazione di terzi e/o dell'Azienda potranno essere attivati dall'Azienda stessa meccanismi di rimborso del danno subito e potranno essere applicate sanzioni disciplinari.

L'Azienda si riserva di attivare profili ufficiali aziendali strettamente correlati all'attività lavorativa.

ARTICOLO 12. UTILIZZO DI CLOUD O SISTEMI ANALOGHI

Non è consentito l'utilizzo di cloud extraziendale che consenta il carico di qualsiasi dato, documento o l'utilizzo di applicativi disponibili sulla rete on line, se non espressamente autorizzati dal Direttore Generale, in qualità di Titolare del Trattamento, e dal Responsabile della UOC SIeTC.

Pertanto è severamente vietato archiviare o inserire sui sistemi cloud o sulle applicazioni on line qualsiasi tipologia di dati attinente all'attività lavorativa svolta presso l'AOUSA.

L'utente dovrà rimuovere qualsiasi contenuto archiviato in cloud rientrante nella fattispecie precedente.

ARTICOLO 13. SISTEMI DI VIDEOCONFERENZA

Non è consentito l'utilizzo di sistemi di videoconferenza/audioconferenza se non preventivamente autorizzati dalla UOC SIeTC.

L'Azienda ha introdotto sistemi istituzionali di videoconferenza/audioconferenza allo scopo di ridurre le distanze e permettere senza spostamenti l'interazione diretta tra le persone. La richiesta di utilizzo dovrà pervenire alla SIETC inviando una mail a sietc@ospedalesantandrea.it allegando l'autorizzazione da parte del Responsabile della UOC di appartenenza, la motivazione della sessione ed i relativi partecipanti.

ARTICOLO 14. UTILIZZO POSTA ELETTRONICA

L'Azienda come strumento di lavoro mette a disposizione una casella di posta aziendale per tutte le comunicazioni inerenti all'attività lavorativa ai soli dipendenti aziendali come individuati nel regolamento per l'acceso agli applicativi aziendali.

- Non è consentito l'utilizzo di caselle di posta elettronica personali, al di fuori di quella aziendale, per le comunicazioni istituzionali.
- I messaggi contengono in calce un avvertimento standardizzato aziendale, secondo le indicazioni aziendali, nel quale sia dichiarata la natura non personale degli stessi nonché i vincoli in materia di riservatezza, con precisazione che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.
- In calce l'utente deve riportare altresì i recapiti aziendali personali e dell'ufficio secondo il formato e la grafica predisposta a livello aziendale. Sono tassativamente vietate grafiche e modelli diversi da quelli indicati dall'Azienda, al fine di assicurare la comunicazione aziendale integrata verso l'esterno e l'interno.

- All'atto della cessazione del rapporto di dipendenza/collaborazione con l'Azienda la casella di posta elettronica è bloccata e/o cancellata su comunicazione della UOC Gestione del Personale.
- Gli utilizzatori delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- È fatto divieto utilizzare le caselle di posta elettronica per motivi diversi da quelli legati all'attività lavorativa con l'eccezione dell'esercizio dei diritti normativamente tutelati per l'invio e la ricezione di informazioni di natura sindacale.
- È obbligatorio prestare la dovuta attenzione all'apertura di messaggi o allegati di dubbia provenienza; in ogni caso l'utente deve informare la UOC SIeTC della ricezione di tali messaggi.
- Gli utenti sono obbligati a consultare la posta elettronica aziendale.
- Gli utenti sono tenuti a cancellare periodicamente le e-mail inutili.

ARTICOLO 15. INDIRIZZI DI POSTA ELETTRONICA ASSEGNATI ALLE UO AZIENDALI

Si fa presente che l'utilizzo di indirizzi di posta elettronica assegnati alle Unità Operative Aziendali permette l'accesso ai messaggi da parte di tutti gli autorizzati all'accesso a quell'indirizzo di posta elettronica.

Per tale motivo, sugli account sopra indicati non può essere garantita la riservatezza delle comunicazioni.

La richiesta di attivazione di questi gruppi deve contenere l'elenco dei nominativi da includere, deve essere motivata, protocollata e inoltrata dal Responsabile/Direttore della unità richiedente al Responsabile della UOC Sistemi Informativi Tecnologie della Comunicazione.

ARTICOLO 16. UTILIZZO POSTA ELETTRONICA CERTIFICATA (PEC)

La casella di posta elettronica istituzionale certificata (PEC) è lo strumento attraverso il quale l'azienda trasmette e riceve documenti informatici soggetti alla registrazione di protocollo.
È obbligatorio, al fine di garantire la dovuta conservazione di legge, allegare esclusivamente la seguente tipologia di file ai messaggi PEC: PDF, PDF/A, TIFF, JPG, office open XML (OOXML), ODF, XML, TXT.
Le caselle di Posta Elettronica Certificata sono assegnate alle UOC amministrative, alle Direzioni Generale, Amministrativa e Sanitaria e non sono nominative.
La Direzione Aziendale può autorizzare l'eventuale attivazione di ulteriori caselle di posta certificata.
Ciascun Direttore di UOC dell'ambito amministrativo deve indicare, attraverso apposita comunicazione trasmessa al SIETC mediante protocollo, i nominativi dei collaboratori che possono gestire e visualizzare la casella di Posta Elettronica Certificata di propria competenza. La corrispondenza mediante la Posta Elettronica Certificata ricevuta dalle singole strutture viene automaticamente inoltrata, utilizzando le funzioni della PEC stessa, al Protocollo Generale che provvede alla protocollazione ed eventualmente provvede ad assegnarla a varie strutture. Per quanto riguarda la posta PEC in uscita le singole strutture dovranno obbligatoriamente utilizzare la procedura di protocollo per effettuare l'invio verso l'esterno, scegliendo la PEC da utilizzare, quella aziendale o quella assegnata al singolo ufficio. Per quest'ultimo punto risulta esentato esclusivamente l'ufficio proposto all'invio degli stipendi del personale. La responsabilità della verifica e gestione della posta certificata arrivata ed inviata è attribuita al Responsabile/Direttore della UO a cui è assegnata.
Le PEC precedentemente assegnate *ad personam* verranno disabilitate trascorsi tre mesi dall'entrata in vigore del presente regolamento, pertanto ciascun utente deve provvedere al salvataggio della documentazione in esse contenuta, poiché non sarà più disponibile oltre il termine predetto.

Per il salvataggio delle mail di posta certificata è possibile usufruire del supporto tecnico dell'HelpDesk inviando un'email al seguente indirizzo helpdeskrti@ospedalesantandrea.it o utilizzando il pulsante "Invio segnalazioni" presente all'interno della Intranet aziendale.

ARTICOLO 17. UTILIZZO SOFTWARE AZIENDALI

Qualunque software utilizzato all'interno della struttura aziendale deve essere accompagnato da regolare licenza d'uso. La violazione di questo principio comporta l'applicazione di sanzioni penali secondo quanto disposto dalla Legge 633 del 1941 sul Diritto d'Autore e s.m.i..
È pertanto fatto tassativo divieto a chiunque utilizzi computer aziendali di scaricare dalla rete Internet qualsiasi software non autorizzato o installare sulle macchine stesse software privi di licenza d'uso provenienti dall'esterno. Qualunque nuova installazione deve essere espressamente autorizzata dalla UOC SIeTC. Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge n. 128 del 21.05.2004 e s.m.i.

ARTICOLO 18. STRUMENTI DI GESTIONE REMOTA PER MANUTENZIONI IT

La UOC SIeTC adotta soluzioni di gestione remota configurandone e aggiornandone le Impostazioni nel rispetto dei criteri di sicurezza e conformità.

Gli accessi e le disconnessioni da remoto sono notificati all'utente, che deve accettare la connessione, sempre che questo non pregiudichi la necessaria tempestività dell'intervento.

Gli strumenti adottati sono: System Center Configuration Manager (SCCM) e altri strumenti che garantiscano le stesse misure di sicurezza.

Per le attività di manutenzione da remoto da parte di società esterne previste da contratti sottoscritti con l'AOUSA, il RUP e il DEC dei rispettivi contratti devono richiedere l'abilitazione di accesso tramite VPN attraverso l'apposita modulistica disponibile sulla intranet aziendale, protocollata e inviata al Responsabile della UOC SIeTC, indicando i nominativi, i perimetri di accesso e allegando i documenti di riconoscimento degli utenti da abilitare.

ARTICOLO 19. UTILIZZO DEVICE PERSONALI CON SISTEMA OPERATIVO MICROSOFT

Non è consentito l'utilizzo di device personali per finalità lavorative all'interno dell'Azienda.

I Device personali (dispositivi di proprietà dell'utente) non sono autorizzati alla connessione alla rete aziendale.

Il loro utilizzo per finalità lavorative e la connessione alla rete aziendale è consentita solo in caso di smartworking o su richiesta protocollata del Direttore/Responsabile della UO, in cui è necessario evidenziare la motivazione e la proprietà delle licenze software installate sul dispostivo. In tali casi la UOC SIeTC valuta la possibilità della configurazione in rete.

Una volta autorizzati, i Device Personali sono conseguentemente messi in dominio aziendale.

I Device Personali al momento della richiesta di connessione in rete aziendale devono avere il sistema operativo aggiornato all'ultima release emessa dal produttore con installate le patch di sicurezza rilasciate dallo stesso.

I Device con sistemi operativi dichiarati a fine supporto (end of support) non possono essere autorizzati alla connessione in rete.

Dal momento in cui i Device personali sono autorizzati ad essere connessi alla rete aziendale, l'unico amministratore di sistema dei dispositivi diverrà l'AOUSA ed è obbligatoria l'installazione dell'antivirus aziendale.

ARTICOLO 20. UTILIZZO DEVICE PERSONALI CON SISTEMA OPERATIVO DIVERSO DA MICROSOFT

Non è consentito l'utilizzo di device personali per finalità lavorative all'interno dell'Azienda.

I Device Personali (dispositivi di proprietà dell'utente) non sono autorizzati alla connessione alla rete aziendale.

Il loro utilizzo per finalità lavorative e la connessione alla rete aziendale è consentita solo in caso di smartworking o su richiesta protocollata del Direttore/Responsabile della UO, in cui è necessario evidenziare la motivazione e la proprietà delle licenze sw installate sul dispostivo, la UOC SIeTC valuta la possibilità della configurazione in rete.

I Device Personali devono avere il sistema operativo aggiornato all'ultima release emessa dal produttore con installate le patch di sicurezza rilasciate dallo stesso e sw antivirus aggiornati.

I Device con sistemi operativi dichiarati a fine supporto (end of support) non possono essere autorizzati alla connessione in rete.

Tuttavia l'utilizzo di questi ultimi dispositivi è limitato a specifiche VLAN che garantiscono la sicurezza informatica aziendale.

ARTICOLO 21. UTILIZZO CARTELLE DI RETE

Le cartelle di rete possono essere utilizzate esclusivamente per archiviare file inerenti l'attività lavorativa e possono essere accedute da più utenti contemporaneamente.

Non è responsabilità della UOC SIeTc la perdita dei dati dovuti ad accessi simultanei di utenti diversi alla stessa cartella di rete.

- Non è consentita l'archiviazione di file video con le seguenti estensioni:
  .3gp; .asf; .avi; .divx; .flv; .swf; .mp4; .mpeg / .mpg; .ogm; .wmv; .mov; .mkv; .nbr; .rm; .vob; .sfd; .webm; .xvid; ecc…. I file con tali estensioni presenti nelle cartelle di rete saranno automaticamente rimosse dalla UOC SIeTC a partire dalla approvazione del presente Regolamento.
- Nelle cartelle condivise è severamente vietato archiviare qualsiasi file video ed in particolare quelli riconducibili ad atti operatori o che vedano coinvolti pazienti.
- E' severamente vietato archiviare sulle cartelle di rete file video utilizzando sistemi di zip.
- I privilegi di accesso alle cartelle di rete vengono definiti dal Direttore/Responsabile della struttura titolare delle cartelle stesse valutando il bilanciamento delle esigenze della produttività e della necessaria riservatezza.
- La UOC SIeTC si riserva la facoltà di procedere alla verifica ed eventuale rimozione di qualsiasi file memorizzato nelle cartelle di rete qualora ritenuto pericoloso per la sicurezza o non attinente all'attività lavorativa (vedi file zip che contengano file exe ecc).
- Per il ripristino dei dati accidentalmente persi o modificati sulle cartelle di rete è fatto obbligo avvisare tempestivamente la UOC SIeTC.

ARTICOLO 22. UTILIZZO DEI FILE CONTENENTI CATEGORIE PARTICOLARI DI DATI

E' vietato salvare file conteneti categorie particolari di dati nelle cartelle di rete poiché non è detto che chi acceda a tali cartelle abbia la facoltà di poter visionare dati sensibili riferibili a pazienti/utenti/fornitori

Qualora per motivi di lavoro si debbano utilizzare dati sensibili su una stazione di lavoro, questa deve sempre essere protetta da accessi da parte di altro personale (es. mediante password). Ogni qualvolta che l'utente lasci la stazione di lavoro questa deve essere spenta o posta in modalità protetta ovverosia con accesso successivo tramite password. Ogni file contenente dati sensibili deve essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni da parte di soggetti diversi da quelli autorizzati (es. mediante password).

I dati possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti istituzionali.

Nell'invio di dati sensibili tramite posta elettronica agli interessati finali che dispongano della facoltà di trattare i dati sensibili stessi, si devono utilizzare file in forma di allegato e non come testo del messaggio stesso. Il file allegato deve essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione da parte di soggetti diversi dal destinatario che può consistere in una password forte (utilizzando un generatore di password) per l'apertura del file o in una chiave crittografica rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione del file.

L'AOUSA mette a disposizione degli utenti abilitati uno spazio cloud, "AOUSA Cloud" (https://cloud.ospedalesantandrea.it), che permette la condivisione dei documenti in modalità sicura attraverso uno strumento di cifratura. È severamente vietato trasferire all'interno del cloud e all'interno della postazione di lavoro dati appartenenti a categorie particolari e nello specifico dati relativi alla salute dei pazienti.

ARTICOLO 23. UTILIZZO DEI SISTEMI DI FIRMA DIGITALE

La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

La firma digitale è l'equivalente informatico di una firma autografa apposta su carta ed ha il suo stesso valore legale. La sua funzione è quella di garantire autenticità, integrità e validità di un documento: tramite l'apposizione della firma digitale, infatti, è possibile sottoscriverne il contenuto, assicurarne la provenienza e garantire l'inalterabilità delle informazioni in esso contenute.

I sistemi di firma digitale vengono assegnati per quanto riguarda l'area sanitaria secondo quanto previsto dall'articolo 3 del regolamento per l'accesso agli applicativi aziendali per consentire l'esecuzione di quanto previsto nelle stesse applicazioni. In ogni caso, sia area sanitaria che amministrativa, dovrà essere compilata la Modulistica (M919/607) di Richiesta di firma digitale, disponibile sulla rete intranet, inserendo gli estremi del richiedente, la UO di assegnazione, la motivazione, gli applicativi che si intende utilizzare con il predetto sistema, l'autorizzazione del Direttore/Responsabile della UO a cui afferiscono, allegando copia di un documento di riconoscimento. La documentazione deve essere protocollata e inviata alla Direzione Amministrativa o Sanitaria a cui afferisce la UO.

A seguito di autorizzazione da parte delle Direzioni, la modulistica è inoltrata alla UOC SIeTC per l'attivazione e consegna della firma digitale.

Al momento della consegna l'assegnatario deve sottoscrivere la modulistica di consegna della firma digitale.

L'utente a cui è assegnata la firma digitale è obbligato alla riconsegna e disattivazione della stessa dal momento in cui a qualsiasi titolo non presta servizio, anche temporaneamente, presso la AOUSA, nel caso della compromissione del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare di firma elettronica qualificata, di sospetti abusi o falsificazioni. Il titolare si deve recare presso la UOC SIeTC e sottoscrivere la modulistica di disattivazione e riconsegnare contestualmente la card.

In caso di perdita del possesso è altresì obbligato a darne immediata comunicazione alla UOC SIETC che provvederà alla disattivazione.

ARTICOLO 24. CONTROLLI E CORRETTEZZA NEL TRATTAMENTO

L'AOUSA utilizzando sistemi informativi per esigenze di natura organizzative, produttive oppure di tutela del patrimonio aziendale, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori, di sistemi che possono comportare un controllo indiretto a distanza e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori.

L'AOUSA rispetta le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica dei predetti.

24.1 RETE INTERNET

Garanzie per i lavoratori

Vista la delicatezza ed il carattere personale dei dati contenuti sui log sono adottate tutte le cautele necessarie per evitare di pregiudicare il diritto alla riservatezza del lavoratore. L' AOUSA non utilizza sistemi hardware e software preordinati al controllo a distanza attraverso i quali sia possibile:

- effettuare controlli prolungati, costanti o indiscriminati;

- riprodurre e memorizzare sistematicamente le pagine Web visualizzate dal lavoratore;
- utilizzare strumenti di lettura e di registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
- effettuare analisi occulta di computer portatili affidati in uso.

Forme di controllo

La AOUSA riduce il rischio di usi impropri della "navigazione" in Internet, quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità non autorizzate, adottando opportune misure che possono prevenire controlli successivi sul lavoratore.

In particolare, la AOUSA adotta le seguenti misure:

- individuazione dei permessi di navigazione in Internet (accesso libero ad esclusione delle categorie di cui al punto successivo);
- individuazione di categorie di siti considerati non pertinenti e pertanto bloccati
- configurazione di sistemi e utilizzo di filtri che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche;
- conservazione nel tempo dei dati (log) strettamente limitata al perseguimento di finalità organizzative e di sicurezza. Sono autorizzati all'accesso, delle informazioni esclusivamente gli Amministratori di sistema opportunamente nominati;
- l'eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere luogo solo in relazione a:
    - esigenze tecniche o di sicurezza del tutto particolari;
    - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
    - obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

24.2 POSTA ELETTRONICA

Garanzie per i lavoratori

Secondo un ormai unanime orientamento di dottrina e giurisprudenza il contenuto dei messaggi di posta elettronica - come pure i dati esteriori delle comunicazioni e i file allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'Amministrazione Digitale).

Forme di controllo

Con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

L'Azienda Ospedaliero Universitaria Sant'Andrea nel rispetto della riservatezza dei dati contenuti nella posta elettronica dei lavoratori assicura la completa non accessibilità a terzi dei dati. Qualora si verificassero casi di un non corretto funzionamento del sistema in uso da parte dell'utente finale, solo su autorizzazione di quest'ultimo, l'azienda può intervenire per la manutenzione. L'esplicita autorizzazione può avvenire utilizzando il pulsante "Invio segnalazioni" presente all'interno della Intranet aziendale. La ricezione di tale richiesta rappresenta consenso esplicito al personale di poter effettuare le attività tecniche inerenti la manutenzione con possibile accesso ai dati. Le stesse regole si applicano agli interventi tecnici sulle singole stazioni di lavoro effettuate in locale o in remoto. La richiesta di intervento corrisponde ad un'autorizzazione al personale all'effettuazione dell'attività ed al possibile accesso ai dati.

Conseguenze per il non corretto utilizzo di sistemi di posta elettronica e navigazione internet:

- Qualora si verificassero dei casi di un non corretto uso dei sistemi sopra citati e si dovesse quindi averne una segnalazione, si procede con la segnalzione al Direttore/Responsabile della unità di appartenenza per l'applicazione del "*Regolamento per i Procedimenti Disciplinari relativi al personale dipendente dell'AOUSA*" pubblicato sull'intranet aziendale.

24.3 SOFTWARE AZIENDALE

Forme di controllo

Periodicamente sono effettuati controlli sulle macchine aziendali al fine di prevenire violazioni della legge a tutela del diritto d'autore sul software o rischi relativi alla sicurezza. Nel caso in cui vengano rinvenuti software non autorizzati installati su macchine aziendali, verranno immediatamente eliminati e conseguentemenete avviate le azioni di natura disciplinare.

L'azienda procede anche periodicamente ad una verifica del numero di licenze software presenti e, in caso di mancanza di alcune di esse, provvede, se ritenuto necessario, alla loro integrazione, in caso contrario procede alla rimozione del software non dotato di licenza.

24.4 AMMINISTRATORE DI SISTEMA

Forme di controllo

Al fine di garantire le misure adeguate per la sicurezza delle tecnologie dell'informazione e della comunicazione (ICT) previste dalla normativa vigente sono previste delle forme di controllo affinché:

- gli amministratori di sistema utilizzino correttamente le utenze privilegiate, accedendo ai sistemi in uso con credenziali diverse da quelle non privilegiate;
- tutte le utenze debbono essere nominative e riconducibili ad una sola persona;
- tutte le utenze siano state debitamente e formalmente autorizzate.

Inoltre la registrazione degli accessi effettuati dagli amministratori di sistema è svolta da parte del fornitore dello specifico servizio.

Si specifica che gli amministratori di sistema nell'esecuzione delle loro attività di controllo, manutenzione ed interventi di rispristino dei sistemi utlizzando dall'esterno esclusivamente collegamenti in modalità VPN che sono autorizzati dal SIETC.

24.5 DEVICE PERSONALI

Forme di controllo

Nel caso di utilizzo di un device personale (dispositivi di proprietà dell'utente), alle condizioni sopra specificate, per l'utilizzo della casella di posta aziendale è obbligatorio, qualora venissero rilevate comprovate violazioni in termini di sicurezza (es. furto del dispositivo), che l'utente comunichi tempestivamente alla UOC SIeTC l'accaduto e cambi immediatamente le password di accesso ai sistemi aziendali.

ARTICOLO 25. SANZIONI

La AOUSA si riserva di adottare adeguati provvedimenti, anche di tipo disciplinare, qualora si constati un utilizzo dei dispositivi informatici contrario a quanto previsto dal seguente regolamento, secondo le modalità previste all'art. 7 dello Statuto dei Lavoratori, dal Contratto Collettivo Nazionale di Lavoro (art. 32), dal Codice Civile (artt. 2104 - 2105) e dal Regolamento Per I Procedimenti Disciplinari relativi al personale dipendente dell'AOUSA.

Le sanzioni disciplinari sono graduate a seconda della gravità del comportamento punito, partendo dalla più lieve, al rimprovero verbale, fino alla possibilità di licenziamento per giusta causa.

Qualora si constati un utilizzo dei dispositivi informatici contrario a quanto previsto dal seguente regolamento da parte di utenti appartenenti a ditte esterne, il RUP del contratto coinvolto, una volta ricevuta

la segnalazione dovrà applicare, a seconda della gravità rilevata, le penali o gli atti che potranno portare anche alla risoluzione del contratto e la richiesta dei danni subiti e subendi ivi compresi quelli di immagine.

ARTICOLO 26. NORME FINALI E TRANSITORIE

Il presente regolamento abroga e sostituisce tutte le disposizioni adottate in materia in precedenza, comunicate in qualsiasi forma.

Copia della disposizione, oltre ad essere pubblicata sul portale aziendale, è consegnata al momento dell'assunzione a ciascun dipendente.

È dovere di ogni utente applicare il complesso di regole stabilite da questo regolamento al fine di contribuire personalmente alla tutela del patrimonio delle informazioni aziendali e alla sicurezza dei suoi sistemi informatici.

Il presente regolamento ha effetto dalla data riportata nel decreto di adozione e contestualmente vengono disapplicati i precedenti regolamenti in materia.

ALLEGATI

Allegato 1: "Modalità operative per il collegamento di dispositivi alla rete aziendale"

Allegato 2: "Modalità operative per l'installazione di software sulle postazioni di lavoro aziendali"

Allegato 3: "Comportamenti da adottare durante l'attività di smart working (lavoro agile) ambito Sistemi Informativi e Tecnologie della Comunicazione"