Sistema Socio Sanitario

Carlo Poma

Regione Lombardia

ASST Mantova

Regolamento e principali misure di sicurezza in materia di utilizzo delle risorse informatiche, internet, posta elettronica

Rev. 06/10/2025

Sommario

1. OBIETTIVI E FINALITÀ 4

2. ACRONIMI E ABBREVIAZIONI 4

3. DEFINIZIONI 4

4. AGGIORNAMENTO E REVISIONE 5

5. CAMPO DI APPLICAZIONE 5

6. PREMESSA 5

1.1 ANALISI DEL RISCHIO 6

7. CONTATTI SISTEMI INFORMATIVI AZIENDALI 8

8. VERIFICHE 8

9. SANZIONI 8

10. POSTAZIONI DI LAVORO 10

10.1 UTILIZZO DELLE POSTAZIONI DI LAVORO 10
10.2 ASSISTENZA REMOTA 10
10.3 DISPOSITIVI PERSONALI E BYOD 11

11. STAMPANTI 11

11.1 STAMPA PROTETTA 11

12. WEBCAM 12

13. DISPOSITIVI DI TELEFONIA FISSA 12

14. TELEFONI CELLULARI (SMARTPHONE) 12

15. DISTRUZIONE-CANCELLAZIONE DEI DISPOSITIVI 12

16. GESTIONE DEI DISPOSITIVI SMARRITI O RUBATI 13

17. SISTEMI IN CLOUD 13

17.1 CLOUD COMPUTING 13
17.2 VANTAGGI DEL CLOUD 13
17.3 COME FUNZIONA 14
17.4 UTILIZZO DI SISTEMI CLOUD 14

18. MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI 15

18.1 GESTIONE DEI DATI TRATTATI MEDIANTE STRUMENTI ELETTRONICI 15

19. GESTIONE DEI DATI SULLE STAZIONI DI LAVORO 17

19.1 RISORSE CONDIVISE 18
19.2 UTILIZZO DI SUPPORTI MAGNETICI E DI MEMORIZZAZIONE (DRIVE USB, CD/DVD, DISCHI FISSI ESTERNI) 18

19.3 BACK-UP (SALVATAGGIO DEI DATI) 19
20. MISURE DI PROTEZIONE DAI VIRUS INFORMATICI, TROJAN-HORSE, SPYWARE, MALWARE 20
20.1 LE PRINCIPALI REGOLE PER LIMITARE L'INTRODUZIONE DI VIRUS SUL PC 20
21. POLICY AZIENDALE PER L'USO DEI SERVIZI/APPARATI IN RETE 22
21.1 USER ID E PASSWORD 22
21.2 PASSWORD DI PRIMA ATTIVAZIONE E PASSWORD PERSONALE 22
21.1.1 SUGGERIMENTI PER LA SCELTA PER UNA PASSWORD ROBUSTA ED EFFICACE 22
21.1.2 CONSIGLI PER LA CURA E LA GESTIONE DELLE PASSWORD 22
21.1.3 RIATTIVAZIONE DELLA PASSWORD 23
21.1.4 CASI PARTICOLARI: DISMISSIONI DEGLI ACCESSI 23
22 INTERNET 24
23 POSTA ELETTRONICA 25
23.1 Disclaimer Automatico 27
23.2 TRATTAMENTO DEI METADATI DI POSTA ELETTRONICA 27
23.3 CONTROLLI 28
24 APPLICAZIONI 29
25 INSTALLAZIONE DI NUOVE APPLICAZIONI 29
26 PROGETTAZIONE E SVILUPPO DI NUOVE SOLUZIONI INFORMATIZZATE 31
26.1 CONSULENZA 31
27. FORNITURE DI HARDWARE E SOFTWARE 32
27.1 ACQUISTI 32
27.2 RICHIESTE DI FORNITURA HARDWARE 32
28. RESPONSABILITÀ 33
RIFERIMENTI NORMATIVI 34

1. Obiettivi e finalità

L'obiettivo del presente documento è divulgare le politiche che ASST di Mantova ha messo in atto per una corretta gestione dei Sistemi informativi, mediante la formalizzazione di una serie di direttive per tutto il personale coinvolto nel trattamento dei dati. Il presente documento individua quindi, in generale, le misure che devono essere osservate dal personale che, nello svolgimento delle proprie mansioni, gestisce quotidianamente dati personali e sensibili. Le presenti disposizioni, in attuazione delle linee guida del Garante per la posta elettronica e internet [11] , hanno lo scopo principale di adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici messi a disposizione dall'ente per lo svolgimento delle mansioni attribuite, delle reti e della posta elettronica e per definire con altrettanta chiarezza il diritto di ASST a verificare l'uso corretto dei suddetti strumenti ed individuare le modalità con cui ASST esercita tale diritto. Le scelte di base delle presenti disposizioni sono orientate a prevenire usi arbitrari degli strumenti informatici o comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza dei dati, senza ledere, allo stesso tempo, il diritto alla riservatezza degli utenti, a proteggere le libertà fondamentali e la dignità delle persone. L'Amministrazione, quale datore di lavoro, nella persona del Direttore Generale adotta ogni misura volta ad eliminare la possibilità di controllo informatico, nel rispetto dell'art. 4 secondo comma dello Statuto dei lavoratori [1] e della vigente disciplina in materia di privacy [6][7].

2. Acronimi e abbreviazioni

ASST:	Azienda Socio-Sanitaria Territoriale
AdS:	Amministratore di Sistema
SIA:	servizio informativo Aziendale
PDL:	Postazioni di Lavoro
PIN:	Personal Identification Number
SISS:	Servizio Informativo Socio-Sanitario
HD	Help Desk
IT	Information Technology

3. Definizioni

Trattamento: (art. 4 Regolamento (UE) 2016/679):
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;

Azienda: La ragione sociale indicata in testata al presente documento.

Dipendente: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Disciplinare: Disciplinare per l'utilizzo degli strumenti informatici, di internet e della posta elettronica. È il presente documento.

Device: Qualsiasi computer (workstation o laptop), smartphone, tablet o altro tipo di dispositivo elettronico (comprese chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati)

GDPR: Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati.

Incaricato: ogni dipendente, come sopra identificato, ed ogni altra persona fisica che sotto il controllo dell'Azienda, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) gestiti dall'Azienda stessa.

NDA: non disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

PHISING: https://www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/index.html

4. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione al SIA (sia@asst-mantova.it).

La versione aggiornata del presente Regolamento, che avviene con cadenza almeno annuale da parte del SIA, è scaricabile dalla intranet aziendale (https://intranet.asst-mantova.it) nella sezione "Documenti e Moduli" →Sistemi Informativi Aziendali.

5. CAMPO DI APPLICAZIONE

Le presenti direttive si applicano a tutti i lavoratori dipendenti di ASST di Mantova, nonché a tutto il personale che, a qualsiasi titolo presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso le sedi dell'ente e che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato ed abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche di ASST.

Tale documento si intende applicabile a tutto il materiale di proprietà o noleggiato dall'ente ed all'utilizzo di eventuali dispositivi privati utilizzati nelle proprie strutture.

Il documento fa riferimento ad usi impropri dell'accesso ad internet e all'uso della posta elettronica solo in relazione a comportamenti che l'Amministrazione ritiene non conformi all'ambito lavorativo.

Per i reati commessi mediante l'uso delle tecnologie informatiche si fa riferimento alla legislazione vigente.
L'ente, tuttavia, è tenuto ad adottare ogni possibile misura di sicurezza volta a limitare utilizzi indebiti che possano essere fonte di responsabilità per l'utente.

6. Premessa

La corretta osservanza del presente disciplinare consente non solo di adempiere gli obblighi di legge, ma anche di migliorare l'organizzazione aziendale ottimizzando i processi di lavoro attraverso l'uso di strumenti informatici.
Premesso che l'utilizzo delle risorse informatiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne di comportamento comune, dirette ad evitare comportamenti inconsapevoli e/o scorretti.
Il disciplinare di cui in oggetto contiene un insieme di linee guida (comportamenti) da seguire al fine di ridurre a livelli accettabili i rischi derivanti da uso improprio o poco consapevole delle risorse informatiche aziendali.
I problemi di sicurezza possono provocare la perdita di profitti, spese aggiuntive, risvolti penali, la perdita della fiducia degli utenti e l'incapacità di gestire continuativamente le risorse e i processi collegati anche alla erogazione di prestazioni sanitarie.
Gli strumenti per il monitoraggio delle reti utilizzati per identificare le vulnerabilità tecniche sono utili solo per risolvere i problemi di natura tecnica; tuttavia, occorre ricordare che questi controlli possono essere accidentalmente o volontariamente messi fuori uso da utenti e processi, con una conseguente esposizione delle informazioni e delle reti ai rischi di natura diversa. Un approccio completo per la gestione dei rischi e la salvaguardia delle informazioni deve necessariamente prevedere l'identificazione delle vulnerabilità e delle minacce più probabili, una quantificazione del possibile impatto sulle risorse aziendali e lo sviluppo di strategie correttive capaci di ridurre il rischio a un livello accettabile.
La continua evoluzione di requisiti e sistemi impone ai professionisti della sicurezza la necessità di individuare un livello di rischio accettabile che non comprometta la disponibilità, la riservatezza e l'integrità dei dati.
Nella Tabella 1 sottostante raffiguriamo alcuni esempi di minacce, metodi, obiettivi e criteri di sicurezza, ai quali il presente documento analizza e tiene conto al fine di garantire non solo l'applicazione della normativa vigente in materia di protezione di dati, ma anche di tutela del patrimonio aziendale.

Minacce	Ragioni/Obiettivi	Metodi	Criteri di sicurezza
Dipendenti Malintenzionati Inesperti **Non dipendenti** Aggressori esterni Calamità naturali	Negare i servizi Sottrarre informazioni Alterare le informazioni Danneggiare le informazioni Eliminare le informazioni Fare uno scherzo Cercare visibilità	Social engineering Virus, trojan-horse, worm Modifica dei pacchetti Saturazione con posta Strumenti di *hacking* Identificazione password	Vulnerabilità Risorse Informazioni e dati Produttività Hardware Personale

Tabella 1

1.1 ANALISI DEL RISCHIO

L'analisi del rischio costituisce una fase fondamentale di ogni percorso di sicurezza.
Questo documento in larga misura tratta dell'adozione di misure minime di sicurezza, obbligatorie per legge [34], e quindi non graduabili. La valutazione del rischio sarà comunque utilizzata per tutte quelle situazioni in cui l'adozione di misure minime sia non sufficiente e pertanto si debba valutare una gradazione delle misure adottabili.

In tali contesti, cioè qualora sia necessaria una graduazione delle misure adottabili, si dovrà adottare una valutazione del rischio basata sui seguenti criteri:
si considerano gravi le minacce che possono limitare e/o rendere difficoltosa l'erogazione della attività assistenziale e/o rese al pubblico;
si considerano gravi le minacce che portano alla divulgazione/modifica/produzione illegittima di dati sensibili o che comportino un danno patrimoniale per l'azienda;
si considerano gravi le minacce che portano alla perdita o sottrazione illecita dei dati

In particolare:

- si considerano **gravi** le minacce che possono limitare la disponibilità di servizi informatici a supporto delle attività assistenziali o delle attività rese al pubblico;
- si considerano **gravi** le minacce che portano alla modifica illecita di messaggi – e quindi di informazioni gestite dall'azienda - qualora tali messaggi abbiano un valore medico-legale o la loro modifica comporti un danno patrimoniale per l'azienda;
- si considerano **gravi** le minacce di fraudolenta impersonificazione (masquerade) qualora ciò porti alla produzione di falsi atti con valore medico-legale o che comportino un danno patrimoniale per l'azienda;
- si considerano **gravi** le minacce di fraudolenta impersonificazione (masquerade) qualora ciò porti alla modifica fraudolenta di atti con valore medico-legale originariamente legittimi, o qualora ciò porti ad un danno patrimoniale per l'azienda;
- si considerano **gravi** le minacce di intercettazione qualora i dati intercettabili riguardino dati personali di natura sensibile ai sensi della legge sulla tutela dei dati personali.

Si considerano in genere **trascurabili** le minacce di analisi del traffico e di ripetizione, a patto che esse non portino a conseguenze elencate nei punti sopra elencati.

A tal fine, con l'obiettivo di garantire la continuità operativa nel rispetto della riservatezza dei dati sensibili e personali trattati dall'Azienda si sono definite nel presente documento una serie di comportamenti per l'utilizzo delle risorse informatiche, della posta elettronica e dell'accesso ad internet.

7. CONTATTI SISTEMI INFORMATIVI AZIENDALI

- Sede Operativa: Str. Lago Paiolo, 10 Palazzina 30
- Help Desk telefonico **H24**: 0376 464 420 (dall'interno interno 3420)
- Portale Self-Service per segnalazione problemi e richiesta forniture:

https://ariawdprod.service-now.com/fleet_portal

8. VERIFICHE

Salvo l'obbligo per ciascun utente di seguire il presente Regolamento e di segnalarne eventuali violazioni al Responsabile dei Sistemi Informativi Aziendali (sia@asst-mantova.it), le funzioni di verifica del suo rispetto sono assegnate alla SC SIA che potrà compiere anche verifiche sul corretto utilizzo dei supporti di memorizzazione e delle istallazioni di software e Hardware locali. Tutti gli utenti sono tenuti a segnalare prontamente qualsiasi violazione al presente Regolamento.
Non sono ammesse segnalazioni di violazioni in forma anonima; viene comunque tutelato dall'Azienda il diritto alla Privacy degli utenti che comunicassero dette violazioni, nei limiti previsti dalla normativa italiana in vigore.
In applicazione del GDPR, l'Azienda promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Azienda informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. Al contrario possono esserci verifiche programmate ai sensi del principio di Accountability ex art. 5.2 del GDPR.
Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files autore pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

9. SANZIONI

Poiché, in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità dei propri Sistemi Informativi/Informatici (vedi cap. 24).

In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali. Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle Autorità competenti.

10. POSTAZIONI DI LAVORO

10.1 UTILIZZO DELLE POSTAZIONI DI LAVORO

Le PDL, sia di tipo desktop che di tipo laptop (portatili), sono predisposte con tutta la necessaria dotazione di dispositivi (hardware) e programmi (software) tali da consentirne il corretto funzionamento in conformità a standard aziendali e nel rispetto della disponibilità delle necessarie licenze d'uso.
L'installazione e l'aggiornamento dei dispositivi e dei programmi è di esclusiva competenza del personale espressamente incaricato del SIA.
Non è consentito:

- Installare software non autorizzato e non coperto da adeguate licenze d'uso aziendali;
- Modificare in parte o del tutto il sw o le sue configurazioni di funzionamento;
- Asportare o copiare in parte o del tutto il sw;
- Modificare, aggiungere o rimuovere dispositivi hw;
- Utilizzare strumenti software e/o hardware atti a interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- Utilizzare dispositivi di comunicazione diversi da quelli di cui è dotata la PDL (es.: modem, switch, hub, router, telefoni cellulari e palmari, apparati di rete non autorizzati);
- Disattivare o disinstallare, anche temporaneamente, il sistema di protezione aziendale (antivirus, edr/xdr);
- Aprire sessioni di lavoro remote tramite PDL connesse alla rete aziendale;
- Compromettere il funzionamento dei servizi di rete e degli apparecchi che li costituiscono con virus o programmi diretti a danneggiare od interrompere la continuità operativa;
- Connettere alla rete aziendale computer e/o apparati, anche elettromedicali, non preventivamente comunicati al SIA;
- Distruggere, deteriorare o rendere in tutto od in parte inutilizzabili programmi, informazioni o dati altrui;
- Lasciare incustodita la stazione di lavoro se non in una condizione di spegnimento o blocco all'accesso (CTRL+ALT+CANC);

Si sottolinea che il cosiddetto software "shareware" o "freeware", scaricabile da Internet, è generalmente esente da licenza SOLO per uso amatoriale. L'utilizzo su stazioni di lavoro di un'azienda deve essere subordinato alla formalizzazione della relativa licenza d'uso (ricadono in questa categoria software molto comuni quali: screensavers, compressori, "criptatori"(winzip), ecc.), a tal proposito si richiama quanto già indicato nei punti precedenti.
Ogni PDL alla quale il dipendente può accedere deve essere considerata come strumento di produttività, e come tale deve essere utilizzato, inoltre, nei casi in cui la stazione di lavoro venga sottoposta a qualsiasi intervento di manutenzione, sia straordinario che dietro richiesta dall'utente (ad esempio in Assistenza Remota 11.2), e vengano individuati software applicativi non riconducibili ad installazioni aziendali o non coperte da regolari licenze d'uso, gli operatori del SIA sono autorizzati alla rimozione dalla PDL ripristinandone le configurazioni iniziali.

10.2 ASSISTENZA REMOTA

Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni al fine di garantire l'assistenza tecnica e la normale attività operativa nonché garantire la massima sicurezza contro *virus*, *spyware*, *malware* o qualsiasi criticità dei sistemi operativi secondo le ultime segnalazioni in fatto di vulnerabilità.

L'intervento viene effettuato esclusivamente su chiamata dell'utente (tramite contatti riassunti al cap.8) o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico/informativo[1] e, quindi, senza alcun avviso preventivo al fine di non compromettere o degradare la disponibilità dei servizi digitali erogati. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione in forma orale dell'intervento ex-post; l'operatore contattato dovrà fornire adeguato supporto al personale del SIA al fine di garantire tempestivamente l'intervento ed il ripristino delle normali condizioni di funzionamento.
L'attivazione dell'assistenza remota da parte dell'utente o l'accesso da parte del personale del SIA dietro evidenza di oggettiva necessità (come sopra descritto) comporta la liberatoria al personale incaricato delle operazioni alla visibilità di tutto il contenuto completo della propria PDL comprese le *share di rete*.

10.3 DISPOSITIVI PERSONALI E BYOD

Ai dipendenti non è permesso svolgere le attività istituzionali su PC (fissi o portatili) e tablet personali: i dati, di proprietà dell'azienda devono essere trattati unicamente con gli strumenti messi a disposizione dell'ente che sono configurati secondo requisiti di sicurezza, tra cui password/pin di attivazione, blocco automatico per tempo di inattività, cifratura del disco, XDR, …
Resta vietato l'utilizzo di memorie di massa esterne personali (pen-drive USB, memory card, archivi esterni-dischi fissi, DVD, macchine fotografiche, videocamere, tablet, …): lo scambio delle informazioni deve avvenire unicamente con i canali messi a disposizione dall'ente, tutto il materiale scambiato rimane di proprietà dell'ente e non può essere esfiltrato dai sistemi.

I dispositivi personali (es. smartphone, tablet, …) possono invece utilizzare la rete Wi-Fi dell'azienda per avere l'acceso ad internet usando la rete propagata con il nome "Ospiti" che prevede molteplici meccanismi di autenticazione (es. Google, Facebook, X, sms, email, …) liberamente usabili sia dal personale che dai cittadini che frequentano le sedi dove è presente la copertura Wifi stessa.

11. STAMPANTI

L'incaricato al trattamento dei dati deve effettuare la stampa dei soli dati necessari all'attività lavorativa e provvedere ad un rapido ritiro dei documenti dai vassoi delle stampanti, siano esse ad uso personale che ad uso comune, al fine di evitare un improprio accesso ai dati da parte di personale terzo non autorizzato.
Al momento del ritiro dei fogli stampati, l'utente deve porre massima attenzione a prelevare unicamente la documentazione di propria pertinenza.

11.1 Stampa protetta

Per rinforzare i meccanismi di protezione della documentazione mandata in stampa, si consiglia di contattare l'help-desk del SIA [8] per richiedere l'attivazione, laddove possibile, della funzionalità di "Stampa Protetta" ovvero il meccanismo che consente di mantenere nella memoria del dispositivo il documento fino a quando l'utente, dopo aver inserito un codice PIN personale, può provvedere al suo rilascio (stampa).

Qualora l'utente disponga di più dispositivi di stampa, si consiglia sempre di convogliare la stampa verso il dispositivo, che per sua configurazione garantisce un maggior controllo sul documento soprattutto quando esso contiene dati personali e/o sensibili.

[1] ad esempio per problemi correlati alla sicurezza informatica o per esigenze di business-continuity

12. Webcam

Per lo svolgimento delle attività lavorative le postazioni dei dipendenti possono essere dotate di webcam.
L'utilizzo della webcam, non prevede da parte dell'Amministrazione alcun controllo, né alcuna registrazione dei contenuti delle comunicazioni, ferma restando la responsabilità penale, civile ed amministrativa del dipendente nell'ipotesi di compimento di atti illeciti. È vietato l'utilizzo di webcam per comunicazioni di caratteri privato e non collegato con l'attività istituzionale. La richiesta di dispositivi segue le indicazioni del par. 27.2

13. Dispositivi di telefonia fissa

La postazione di lavoro è di norma corredata da un dispositivo di telefonia fissa. Le assegnazioni di linee telefoniche, utenze, apparati e abilitazioni, vengono attribuite dai Sistemi informativi, sulla base di motivate esigenze espresse dagli utenti, previa approvazione del Dirigente/Responsabile del servizio.

14. Telefoni cellulari (smartphone)

L'Amministrazione, compatibilmente con le esigenze organizzative, può mettere a disposizione dei propri dipendenti dei telefoni cellulari di servizio, secondo le indicazioni presenti nel regolamento aziendale [10].
Tali dispositivi devono essere utilizzati per scopi istituzionali.
Nell'ipotesi in cui occorra di riconsegnare il dispositivo, l'assegnatario provvederà in autonomia alla cancellazione di eventuali dati personali in esso presenti.

L'accesso a tali dispositivi deve essere sempre subordinato all'attivazione di alcune opzioni di sicurezza fondamentali come, ad esempio, il blocco schermo con una password, uno schema o un'impronta digitale.
Nonostante tali cautele, ove siano inevitabilmente presenti sul dispositivo mobile dati ed informazioni considerate critiche dal dipendente, questi dovrà richiedere l'attivazione - se tecnicamente possibile - della possibilità di blocco del dispositivo e la cancellazione dati da remoto in caso di furto.

Le cautele di cui al presente paragrafo trovano applicazione anche nel caso di utilizzo dei servizi di posta elettronica aziendale sullo smartphone di proprietà del dipendente, ad esclusione del caso in cui si acceda mediante web mail.

15. DISTRUZIONE-CANCELLAZIONE DEI DISPOSITIVI

Ogni dispositivo (computer, notebook, tablet, smartphone) affidato agli incaricati e restituito per termine di utilizzo, sarà sottoposto ad opportuna procedura di ricondizionamento secondo le norme vigenti per essere riassegnato, per quanto possibile, a nuovo utente.
Le modalità utilizzate (in funzione del tipo di dispositivo) potranno essere una delle seguenti:

- Distruzione fisica del supporto (hard disk magnetici/cd/dvd)
- Cancellazione Logica (Wiping) con passaggi multipli

16. Gestione dei dispositivi smarriti o rubati

Nel caso di smarrimento o furto di dispositivi informatici aziendali (PC portatili, smartphone, tablet, chiavette USB, smartcard, badge di autenticazione, ecc.), l'utente assegnatario è tenuto a segnalare tempestivamente l'accaduto al Servizio Informativo Aziendale (SIA) tramite i canali di contatto ufficiali (help desk o email a sia@asst-mantova.it) e, in caso di furto, a presentare denuncia presso le autorità competenti, trasmettendone copia al SIA non appena disponibile.

Il SIA provvederà, ove tecnicamente possibile, al blocco dell'accesso remoto al dispositivo e alla revoca o sospensione delle credenziali di autenticazione associate all'utente. Se il dispositivo è stato configurato con funzionalità di localizzazione o cancellazione da remoto, ne sarà avviata l'attivazione per tutelare la riservatezza dei dati contenuti.

È responsabilità dell'utente collaborare con il SIA per limitare i rischi di accesso non autorizzato alle informazioni aziendali e garantire la continuità operativa. L'eventuale accesso ai dati contenuti nel dispositivo da parte di soggetti non autorizzati potrà costituire violazione della normativa in materia di protezione dei dati personali (Regolamento UE 2016/679) e comportare conseguenze disciplinari secondo quanto previsto dal presente regolamento e dal contratto di lavoro.

17. SISTEMI IN CLOUD

17.1 CLOUD COMPUTING

I sistemi cloud sono una tecnologia che permette di utilizzare risorse informatiche come spazio di archiviazione, applicazioni e potenza di calcolo attraverso internet, senza la necessità di possedere fisicamente l'hardware o il software. In pratica, invece di conservare dati e applicazioni sul proprio computer o su server aziendali, questi vengono memorizzati su server remoti gestiti da fornitori di servizi cloud.

17.2 Vantaggi del Cloud

1. Accessibilità: Puoi accedere ai tuoi dati e applicazioni da qualsiasi luogo e con qualsiasi dispositivo connesso a internet.
2. Scalabilità: È facile aumentare o diminuire le risorse (come spazio di archiviazione o potenza di calcolo) a seconda delle necessità.
3. Affidabilità: I fornitori di servizi cloud offrono backup automatici e sistemi di sicurezza avanzati per proteggere i dati.
4. Risparmio sui Costi: Non c'è bisogno di investire in hardware costoso o di occuparsi della manutenzione, poiché tutto è gestito dal fornitore del servizio.

Esempi di Utilizzo del Cloud

- Archiviazione di File: Servizi come OneDrive, Google Drive o Dropbox permettono di salvare documenti, foto e video online, accessibili da qualsiasi dispositivo.
-Software su Abbonamento: Applicazioni come Microsoft Office 365 o Adobe Creative Cloud possono essere usate direttamente dal cloud, senza bisogno di installazioni locali.
- Piattaforme di Collaborazione: Strumenti come Microsoft Teams facilitano la comunicazione e la collaborazione tra i membri di un team, indipendentemente dalla loro posizione geografica.

17.3 Come Funziona

Quando utilizzi un servizio cloud, invii i tuoi dati a un server remoto attraverso internet. Questo server, gestito dal fornitore del servizio, archivia i tuoi dati e ti permette di accedervi quando ne hai bisogno. Il fornitore si occupa di tutte le operazioni tecniche, inclusi aggiornamenti, sicurezza e manutenzione.
In sintesi, i sistemi cloud rappresentano una soluzione versatile e conveniente per gestire dati e applicazioni, offrendo flessibilità e sicurezza senza le complicazioni della gestione fisica delle infrastrutture informatiche. In informatica, con il termine inglese cloud computing (in italiano nuvola informatica), si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la condivisione di dati, caratterizzata dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

17.4 UTILIZZO DI SISTEMI CLOUD

È vietato l'utilizzo di sistemi Cloud non espressamente approvati dall'Azienda o analoghi sistemi di condivisione dei documenti che non siano coperti da adeguate licenze d'uso aziendale (e non personale) quali, a solo titolo di esempio esempio Google Drive, We Transefer, DropBox, …
Per poter essere approvati ad abilitati, i sistemi cloud, devono rispondere ad i seguenti requisiti minimi:

- Essere certificati da ACN (Autorità per la Cybersicurezza nazionale) e quindi presenti nel catalogo https://catalogocloud.acn.gov.it/
- L'azienda che fornisce il sistema in Cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'ente;

Nel caso in cui, durante le normali attività di controllo del traffico da/verso l'azienda al fine di garantire gli standard di sicurezza e continuità operativa, si dovessero riscontrare accessi a piattaforme non preventivamente comunicate ed autorizzate dal SIA, i tecnici del servizio informativo, agendo sulla configurazione dei sistemi perimetrali di controllo del traffico (firewall) sono autorizzati senza alcun avviso preventivo ad operare al fine di bloccarne l'uso e l'accesso alle piattaforme.

18. MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

18.1 GESTIONE DEI DATI TRATTATI MEDIANTE STRUMENTI ELETTRONICI

ASST di Mantova adotta nell'ambito delle regole generali, un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza volte ad assicurare un livello minimo di protezione di dati personali e sensibili.
L'accesso dei dati trattati con l'ausilio di strumenti elettronici è disciplinato dalle seguenti misure e relative modalità di trattamento:

- Autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione;
- Aggiornamento periodico dell'individuazione dell'ambito di trattamento conseguito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, accessi non consentiti e a determinati programmi informatici;
- Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da organismi sanitari;
- Il trattamento di dati personali e/o sensibili con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura (di autenticazione) relativa a uno specifico trattamento o a un insieme di trattamenti;
- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (username) associato a una parola chiave (password) riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (es. smart-card), eventualmente associato a un codice identificativo (pin) o a una parola chiave;
- Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione: le credenziali di autenticazioni sono strettamente personali e per questo non devono essere in alcun modo comunicate ad altri operatori;
- Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;
- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la parola chiave è modificata almeno ogni tre mesi;
- Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;

- Sono state impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Alla fine della sessione di lavoro eseguire le procedure di uscita (logout) dall'applicativo accertandosi della chiusura di tutte le finestre nelle quali sono evidenti dati personali e/o sensibili;
- Nel caso l'autenticazione sia stata eseguita con smart-card, l'operatore si ricordi di rimuoverla dall'apposito lettore e trattenerla con sé al fine di evitarne smarrimenti ed utilizzi non consentiti;
- Abilitare sulle postazioni screen-saver automatici che intervengono dopo alcuni minuti di inattività: tali screen-savers devono richiedere all'utente la ri-immissione dello username e della password;
- quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema;

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione;

- gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale;
- Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno giornaliera/settimanale;
- accesso limitato per i locali relativi ai Servizi SIA, nello specifico Sala Server e uffici SIA.

19. GESTIONE DEI DATI SULLE STAZIONI DI LAVORO

Ad ogni dipendente è resa disponibile una risorsa di rete: questa risorsa, identificata come disco di rete, è assegnata dall'AdS per effettuare i salvataggi dei documenti, altri salvataggi su cartelle diverse da quella indicata non sono garantiti ai fini dell'applicazione delle misure di sicurezza. In caso di indisponibilità della risorsa, l'utente ha il dovere di informare lo staff tecnico preposto secondo i contatti di cui in. 8

a) Protezione dei dati

L'integrità e la disponibilità delle informazioni e dei dati sono garantite solo quando gli stessi sono memorizzati nei file server messi a disposizione dall'ente, oggetto di sistemi di protezione, monitoraggio e backup. Non è possibile utilizzare i file server come raccoglitore di dati personali. Al fine di garantire la sicurezza e la riservatezza dei dati è fatto obbligo agli utenti di mantenere la riservatezza delle proprie credenziali d'accesso, al sistema informativo nel suo complesso e ai singoli applicativi nel caso in cui questi fossero dotati di credenziali separate da quelle del resto dell'ecosistema digitale.
È altresì obbligatorio presidiare l'intero processo di stampa, copia, scansione di documenti, al fine di impedire l'involontaria o accidentale diffusione di dati personali o la perdita di riservatezza sulle informazioni contenute nei documenti stessi. Allo stesso scopo, è dovere degli utenti prelevare immediatamente i fogli riprodotti da stampanti, fotocopiatrici come suggerito in par. 12

b) Archivi informatici contenenti dati particolari (dati sensibili)

In relazione a specifiche funzioni è possibile che vengano acquisiti e detenuti archivi (cartelle) contenenti dati sensibili e/o dati giudiziari. Queste cartelle/sottocartelle non devono mai essere liberamente accessibili ma protette secondo livelli di autenticazione limitati ai soli soggetti autorizzati.
Per evitare che eventuali accessi abusivi dall'esterno possano compromettere la riservatezza di tale documentazione, è necessario, se tecnicamente possibile, che tali archivi siano cifrati (ad es., zippati con password o analoga misura).

c) Sistema di salvataggio dei dati

A tutto il personale che presta, a qualsiasi titolo, la propria attività lavorativa presso ASST, vengono assegnati, ove previsto e previa richiesta, spazi di lavoro (cartelle):

- personali e dedicati, della rete aziendale (file server) mediante cartelle ad accesso esclusivo;
- condivisi tra tutti gli autorizzati all'accesso (c.d. cartelle condivise/shared)

Operare sugli spazi di lavoro sopra descritti e non in locale costituisce una fondamentale regola di cautela, poiché sulle risorse di rete vengono applicate e gestite, centralmente ed automaticamente, specifiche politiche di back-up secondo la disciplina tecnica vigente; data la limitatezza dello spazio a disposizione sul file server e l'erosione delle risorse di rete che il riversamento di file comporta, è vietato salvare nelle cartelle documenti (intesi anche come immagini, filmati, audio) non direttamente attinenti l'attività lavorativa.
Altri salvataggi su cartelle diverse da quella indicata non sono garantiti ai fini dell'applicazione delle misure di sicurezza. Costituisce buona regola la pulizia periodica (almeno una volta l'anno) degli archivi, con cancellazione dei file obsoleti o ritenuti inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante delle informazioni al fine di salvaguardare spazio e permettere alla risorsa un'operatività costante ed efficiente nonché ridurre gli intervalli di manutenzione.
Le gestioni locali dei dati dovranno essere ridotte al minimo per essere sostituite da gestioni centralizzate su server come indicato dalla normativa vigente [2] e [3].
In linea generale le banche dati presenti sulle PDL non gestite centralmente devono essere prive d'anagrafica dei pazienti e riportare unicamente un numero identificativo in loro sostituzione (es. numero della cartella clinica).

Qualunque creazione di banche dati contenente dati personali deve essere comunicata al SIA ed autorizzata singolarmente previa verifica, il SIA non risponde di banche dati e archivi creati e trattati in difformità da quando stabilito in questo documento.
Nell'effettuare il trattamento dei dati personali devono essere soddisfatti i principali contenuti nella normativa in materia di privacy[2][3] e di sicurezza dei dati trattati. I dati personali devono esser esatti e, se necessario aggiornati nonché pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati [3][4]. Il trattamento deve avvenire in modo lecito, e secondo correttezza; la raccolta e registrazione dei dati stessi deve avvenire per finalità non incompatibili con tali scopi. La conservazione deve avvenire per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
In particolare, si deve osservare che le informazioni archiviate elettronicamente devono essere ridotte al minimo e riguardare esclusivamente quelle previste dalla legge, necessarie all'attività lavorativa secondo finalità determinate, esplicite e legittime, osservando il principio della pertinenza e non eccedenza.
Gli operatori incaricati dall'azienda per la manutenzione ordinaria e straordinaria del sistema informatico possono procedere alla rimozione di ogni file o applicazione sia sulle PDL che sulle unità di rete che riterranno essere pericolosi per la Sicurezza o non conformi a quanto esplicitato nei punti precedenti, previo avvertimento dell'utente.

19.1 RISORSE CONDIVISE

L'utilizzo di risorse condivise (cartelle/share di rete) deve essere ridotto al minimo al fine di diminuire i rischi per la sicurezza informatica e la salvaguardia degli aspetti collegati ad una corretta gestione dei dati personali.
In linea generale valgono le seguenti regole sull'utilizzo delle risorse condivise:

- Le cartelle condivise sono gestite a livello centrale e sono preventivamente concordate, configurate (definizione degli spazi e delle credenziali d'accesso) e mantenute dal SIA, solo di queste si garantisce il back-up/restore dei dati;
- Le cartelle condivise devono essere richieste dal responsabile della struttura dichiarando l'elenco degli utenti che devono potervi accedere e, per ognuno di loro, sono indicati anche i permessi di lettura/scrittura/visualizzazione dei contenuti;
- L'accesso alle cartelle condivise è sempre protetto da meccanismi di accesso costituiti da username personale, nella forma nome.cognome, e password ovvero tramite le c.d. credenziali di dominio;
- Poiché lo spazio assegnato è contingentato sarà cura dell'operatore la manutenzione del contenuto con rimozione dei files ritenuti obsoleti e non utilizzati;
- Le risorse condivise non vanno usate per operazioni di archiviazione e scambio di files il cui contenuto non sia riferibile all'attività lavorativa; pertanto, se nel caso di manutenzione da parte del personale del SIA si dovessero manifestare usi non corretti della risorsa il personale è autorizzato in prima istanza al blocco dell'accesso e alla successiva rimozione dei contenuti.

Il SIA non risponde di interventi di manutenzione di risorse condivise non preventivamente concordate e configurate sugli apparati centrali dei Servizi Informativi.

19.2 UTILIZZO DI SUPPORTI MAGNETICI E DI MEMORIZZAZIONE (Drive USB, CD/DVD, DISCHI FISSI ESTERNI)

Relativamente all'utilizzo dei supporti rimovibili valgono le seguenti linee guide:

- Non è consentito scaricare sulla propria PDL file contenuti in supporti magnetici/ottici/usb non aventi alcuna attinenza con la propria prestazione lavorativa;
- I supporti rimovibili contenenti dati sensibili e/o personali devono essere custoditi con cura in modo da evitarne l'utilizzo da parte di soggetti non autorizzati; la responsabilità dei dati contenuti su questi supporti è completamente attribuibile all'utente che li ha creati e gestiti;

- I supporti rimovibili, contenenti dati sensibili, se non più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (dopo aver formattato il dispositivo o cancellato il contenuto dal dispositivo stesso).

19.3 BACK-UP (SALVATAGGIO DEI DATI)

Il SIA non garantisce il ripristino dei dati dell'utente gestiti in difformità alle regole riassunte nel presente documento come, ad esempio ma a titolo non esaustivo, ripristino di dati di PDL non connesse al dominio aziendale o il cui accesso avviene con credenziali locali.

20. MISURE DI PROTEZIONE DAI VIRUS INFORMATICI, trojan-horse, SPYWARE, MALWARE

Al fine di prevenire le infezioni virali che potrebbero mettere a rischio la continuità operativa aziendale si adottano le seguenti misure:

- Le PDL sono dotate di un adeguato software (EDR/XDR) che monitora e riporta lo stato di accesso ai file con segnalazione automatica al SIA di eventi sospetti o dannosi: il SIA al ricevimento di opportune segnalazioni potrà procedere senza alcuna preventiva comunicazione alla rimozione di tali file che potrebbero compromettere il funzionamento dei sistemi;
- I file server sono dotati di software per la scansione dei documenti gestiti;
- Ogni stazione di lavoro personale dotata di memorie di massa removibili che abbia strumenti di produttività personale e che mantenga documenti in locale è dotata di software antivirale.
- Per quanto organizzativamente possibile ed appropriato, sono disabilitate sui server le funzionalità di *editor* e di *file transfer* a utenti non in possesso di credenziali di amministratore di sistema.

Qualora la PDL fosse sprovvista del software antivirale o fosse dubbio il suo funzionamento, si invitano gli utenti a contattare l'HELP-DESK del SIA (cap. 8) per le verifiche tecniche del caso, lo stesso dicasi nel caso in cui il software antivirale rilevi la presenza di virus che non è riuscito a ripulire.
Si invitano inoltre gli utenti, come specificato all'interno delle lettere di incarico, a seguire i seguenti comportamenti:

a) massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione anche removibile (es. USB) - sia stato utilizzato su un computer diverso dal proprio - supponendo che il proprio PC sia immune da infezioni - occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato si invitano gli utenti a contattare il SIA per la verifica del caso;
b) in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
c) è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri.

20.1 LE PRINCIPALI REGOLE PER LIMITARE L'INTRODUZIONE DI VIRUS SUL PC

Ecco alcune utili regole di comportamento necessarie per ridurre il rischio d'introduzione dei *virus-worm-malware* all'interno della propria PDL e nella rete aziendale:

- Verificare la presenza del software antivirus aziendale accertandosi del suo corretto funzionamento;
- Effettuare le scansioni complete dei supporti rimovibili (es: pen USB, ecc..) tutte le volte che questi vengono connessi al sistema;
- Evitare l'installazione di programmi che non servono per la produttività e la cui provenienza non è ben nota;
- Prestare estrema attenzione agli allegati alle e-mail evitandone l'apertura qualora non siano preventivamente noti o comunque concordati i contenuti con il mittente del messaggio;

- Disabilitare le macro nei documenti o almeno trattarle con lo stesso sospetto dei programmi esterni;
- Prestare attenzione all'uso dei *files* crittografati o la cui estensione non è definita o conosciuta;
- Trattare con sospetto anche i file con estensioni mai viste o classificate come potenzialmente pericolose;
- Segnalare qualunque anomalia o comportamento sospetto all'indirizzo fornito al pag.8 par. 8

21. POLICY AZIENDALE PER L'USO DEI SERVIZI/APPARATI IN RETE

21.1 USER ID E PASSWORD

L'accesso ai servizi in rete è subordinato al possesso di un identificativo (Username) da utilizzare associato ad una parola chiave riservata, personale, non cedibile ovvero la Password.
L'utilizzo combinato di Username e Password è quindi condizione necessaria per l'accesso ai servizi e per l'attivazione di una "sessione di lavoro".
L'attivazione dei servizi in rete è concessa su base personale ed esclusivamente per ragioni e finalità connesse ai compiti del dipendente titolare della Username: pertanto non è consentito cedere a terzi, neppure temporaneamente la "sessione di lavoro" o le informazioni necessarie ad attivarne una.

L'uso di username e password è strettamente personale per cui ogni attività non regolare verrà imputata, nei limiti di legge, al titolare delle stesse.
Gli utenti sono pertanto tenuti a non rivelare le proprie credenziali d'accesso avendo altresì cura che esse non vengano utilizzate in modo improprio. Gli utenti dovranno prontamente avvisare il SIA nell'ipotesi di smarrimento o anche solo di probabile diffusione presso terzi dei dati d'accesso.

E' vietato inoltre:

- Accedere abusivamente ai Servizi in Rete;
- Diffondere o detenere abusivamente password;
- Violare la sicurezza di archivi e computers;
- Connettere in rete apparati, pc fissi, pc portatili senza preventiva notifica al SIA che provvederà a verificare i requisiti e a stabilire le policy d'accesso ai servizi.

21.2 PASSWORD DI PRIMA ATTIVAZIONE E PASSWORD PERSONALE

La password di prima attivazione è comunicata dall'ente esclusivamente all'interessato, il quale sarà obbligato a cambiarla con una password personale già al primo collegamento. La Password personale è nota esclusivamente al titolare della Username collegata, deve essere custodita con diligenza ed attenzione e non deve essere comunicata a terzi, neppure temporaneamente.

21.1.1 SUGGERIMENTI PER LA SCELTA PER UNA PASSWORD ROBUSTA ED EFFICACE

Utilizzare una combinazione di almeno 8-10 caratteri che includa lettere Maiuscole e minuscole, numeri e caratteri speciali come ad esempio: !",£$.#^+
La nuova password non deve contenere lo username, le precedenti password (che potrebbero essere state compromesse in passato) o parti di esse;
Evitare l'uso di informazioni personali e familiari come nomi propri, date di nascita, luoghi comuni;
Evitare l'uso di parole semplici di uso comune presenti in un dizionario di qualsiasi lingua;
Non inserire sequenze di caratteri identici o gruppi di caratteri ripetuti (12345, abcdef, 11111, qwerty…);
Utilizzare una *passphrase* ovvero una frase segreta senza spazi con simboli e punteggiatura: lunga, complessa e più facile da ricordare. Occorre ovviamente che le frasi non facciano parte di testi noti.

21.1.2 CONSIGLI PER LA CURA E LA GESTIONE DELLE PASSWORD

La password è strettamente personale e non deve essere comunicata o condivisa con altri;
Si consiglia quindi di:

- Utilizzare password differenti e complesse per diversi servizi;
- Non rispondere MAI ad e-mail sospette che richiedono l'inserimento delle proprie credenziali e/o cliccare sui link durante la navigazione web (o nell'email) per evitare di incorrere in possibili frodi informatiche (come il *phishing* , lo *spear phishing*, il furto d'identità);
- Modificare subito la propria password in caso di sospetta violazione dell'account;
- Evitare di annotare le password in modo insicuro su fogli di carta, documenti cartacei e file conservati all'interno della propria postazione di lavoro.

21.1.3 RIATTIVAZIONE DELLA PASSWORD

Nel caso il sistema non riconosca la Password personale, è necessario contattare l'HELPDESK (così come in caso di dimenticanza della Password), che provvederà al ripristino di una password di prima attivazione, la modifica della password secondo necessità dell'utente deve essere eseguita in piena autonomia.

21.1.4 CASI PARTICOLARI: DISMISSIONI DEGLI ACCESSI

Relativamente alla gestione delle credenziali d'autenticazione:

- Le credenziali di autenticazione non utilizzate da almeno **sei mesi** sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali (esempio cambio di assegnazione di reparto/servizio);

L'accesso agli applicativi aziendali e alla posta elettronica vengono disabilitati quando i dipendenti, gli specialisti convenzionati, i collaboratori, i borsisti, gli incaricati a tempo determinato e tutto il personale che per qualsiasi motivo utilizza le piattaforme aziendali con credenziali personali cessa il rapporto di collaborazione con l'azienda per differenti motivi: collocamento a riposo, dimissioni, mobilità, termine incarico, ecc..

La **disabilitazione** dell'utenza avverrà dal **giorno successivo** del termine della collaborazione con l'ente.

La **rimozione** di tutti i contenuti associati all'utente (posta, file server, ..) avverrà trascorsi **30gg**. dal termine della collaborazione con l'ente.

22 INTERNET

L'accesso ad Internet, attraverso la rete aziendale, è consentito per ragioni e finalità connesse ai compiti istituzionali del colaboratore utilizzatore.

Quindi:

- è vietato l'utilizzo della rete internet per fini personali estranei all'attività lavorativa;
- È fatto divieto assoluto di scaricare programmi, o contenuti multimediali senza la previa autorizzazione del SIA;
- È vietato porre in essere attività di violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- Non è consentita ogni genere di transazione finanziaria (acquisti/vendite on-line) e simili salvo casi direttamente autorizzati dalla Direzione Generale e con il rispetto delle normali procedure di acquisto;
- Gli utenti sono invitati a limitare al massimo il rilascio d'informazioni personali durante la navigazione via Web. L'utente è tenuto, nel corso della navigazione, a leggere con attenzione qualsiasi finestra, *pop-up* o avvertenza prima di proseguire nella navigazione stessa e in particolare prima di accettare qualsivoglia condizione contrattuale o di aderire ad iniziative online;
- Non è permesso l'uso della rete internet per attività ludiche;
- Non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in *guest book* anche utilizzando pseudonimi (o *nickname*);
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza politica;
- Il SIA, su autorizzazione della Direzione Generale, ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi aziendali.
- E' tuttavia consentito (vedi [8]) l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro, ad esempio per effettuare adempimenti on-line nei confronti dei pubbliche amministrazioni e di concessionari di servizi pubblici ovvero per tenere rapporti con istituti bancari (*home-banking, remote-banking*) ed assicurativi, purché contenuto nei tempi strettamente necessari allo svolgimento delle transazioni;
- E' vietato utilizzare sistemi Peer to Peer (P2P), di file sharing (condivisione di file all'interno di una rete comune), podcasting (sistema che permette di scaricare in modo automatico documenti, generalmente audio o video) o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via Web).

Nel caso si verificasse la necessità di scaricare programmi o loro aggiornamenti dalla rete (download), è necessario rivolgersi al SIA ed in ogni caso:

- verificare il possesso dei necessari diritti d'uso;
- verificare la presenza sulla PDL dell'adeguato software antivirus aziendale;
- non violare regole di copyright od assimilabili.

Non potrà essere comunque fornito alcun supporto o consulenza sulle installazioni effettuate in violazione dei principi sopra enunciati.
Il "download" di documenti di dimensione considerevole può degradare significativamente la prestazione della Rete: si raccomanda di effettuare tali attività ad orari opportuni (all'inizio od al termine dell'orario di lavoro).
Esiste la possibilità tecnica di verificare l'utilizzo di Internet e, per assicurarne la funzionalità, l'Azienda si riserva il diritto di verificare, nei modi e nei fini consentiti dalla legge, le modalità di utilizzo di tale servizio.

23 Posta Elettronica

La casella di posta elettronica, assegnata dall'Azienda all'utente, è uno strumento di lavoro, gli assegnatari della casella sono pertanto responsabili del corretto utilizzo delle stesse.
La comunicazione in forma elettronica, per scopi istituzionali, deve avvenire esclusivamente con l'utilizzo del sistema di posta elettronica dell'ente (@asst-mantova.it) ovvero non sono consentiti l'utilizzo di comunicazioni effettuate da account differenti da quello aziendale riferito all'utente e o al servizio (esempio @libero.it, @virgilio.it,@gmail.com…).

L'indirizzo di posta elettronica personale dell'utente **dipendente** è così strutturato:

nome.cognome@asst-mantova.it

L'indirizzo di posta elettronica personale **non dipendente** (borsisti, stagisti, ecc..) è così strutturato:

nome.cognome@ext.asst-mantova.it

Ciascuna casella *email* viene fornita di una password di prima attivazione che l'utente sarà obbligato a modificare già dal suo primo accesso, la casella sarà ulteriormente protetta con i moderni sistemi di autenticazione noti come autenticazione a più fattori (MFA), ovvero un metodo di autenticazione che richiede all'utente di fornire almeno due fattori di verifica per poter accedere alla risorsa.
Tale metodo è sempre più utilizzato, anche in altri campi come quelli bancari e finanziari, perché garantisce che eventuali malintenzionati in possesso di utenza e password carpite agli utenti attraverso modi illeciti (phishing, spear phising, social engineering,…), non riescano ad accedere ai dati del titolare, in mancanza del secondo fattore di autenticazione. Al fine di garantire la sicurezza di tutti gli utilizzatori, questa modalità di autenticazione sarà lo standard operativo per tutti gli utenti del dominio @asst-mantova.it e @ext.asst-mantova.it. La procedura di autenticazione sfrutta, come in altri casi, un'applicazione installabile sul dispositivo mobile dell'utente e richiede solo qualche secondo in più per effettuare l'accesso alla casella.
Gli utenti che non aderiranno a questa modalità saranno invitati a firmare una Lettera di Assunzione di Responsabilità (LAR) con la quale si:

> *"..Assumono la piena responsabilità per qualsiasi conseguenza derivante da questa decisione, inclusi, ma non limitati a, accessi non autorizzati, violazioni di dati, perdite di informazioni e eventuali danni finanziari o reputazionali per l'azienda."*

La casella di posta elettronica aziendale è consultabile laddove vi è una connessione internet unicamente in modalità web raggiungendo uno degli indirizzi:

https://outlook.office.com

a riguardo il SIA non fornisce alcun supporto tecnico nel caso si effettuassero accessi con Client di posta installati in autonomia e non coperti da opportuna licenza d'uso.

Esistono tuttavia account condivisi associati a reparti, servizi, funzioni che vengono strutturati previo accordo con gli addetti del SIA, tali caselle definite *shared* prevedono la puntuale identificazione degli utenti che possono avere accesso alla medesima direttamente partendo dalla casella personale.
Il servizio di posta elettronica è messo a disposizione degli utenti esclusivamente per attività connesse a fini istituzionali, pertanto, è vietato l'utilizzo della posta elettronica per scopi non associabili alle attività lavorative.

E' vietato:

- utilizzare altri sistemi di posta, anche se offerti gratuitamente, diversi rispetto agli strumenti standard aziendali (Webmail);

- utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;
- inviare a terzi, esterni all'Azienda, materiale di proprietà di ASST di Mantova senza preventiva autorizzazione del responsabile della struttura;
- inviare messaggi o documenti con contenuti illeciti;
- aderire o innescare "catene di Sant'Antonio";
- rispondere allo spam o a e-mail il cui mittente sia di dubbia natura;
- installare e/o configurare autonomamente account di posta elettronica alternativi e non direttamente riferibili all'azienda: nel caso ciò accadesse gli operatori del SIA non presteranno alcuna attività di supporto nella gestione di tali account e saranno abilitati alla loro rimozione previo avvertimento dell'utente;
- inviare messaggi non pertinenti alle attività aziendali o comunicazioni non richieste (spamming);
- è vietato l'invio per posta elettronica di password o codici di accesso, credenziali e/o client VPN;
- utilizzare il sistema di posta e l'indirizzo di posta elettronica forniti da ASST a fini personali;
- Su richiesta scritta e motivata sarà concesso un *forward* verso altro account (non gestito da ASST) per un periodo di mesi tre, al termine dei quali l'account verrà definitivamente rimosso;
- Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione e/o iscrizione a dibattiti, mailing-list, forum, bacheche elettroniche non attinenti all'attività istituzionale fatto salvo la preventiva autorizzazione da parte della Direzione.

Poiché la posta elettronica diretta all'esterno della rete aziendale è suscettibile di intercettazione da parte di estranei e talvolta malintenzionati non deve essere utilizzata per inviare documenti di lavoro riservati contenenti dati personali e/o sensibili, se tale necessità si manifestasse si consiglia di attivare meccanismi di crittografia dei dati o di spedizione multiple al fine di ridurre i rischi derivanti dall'attività.
L'utilizzatore è responsabile della manutenzione della propria casella di posta elettronica ed avrà cura di:

- controllate la posta regolarmente;
- cancellare i messaggi non più utili;
- non inviare messaggi contenenti dati personali e/o sensibili

Si ricorda inoltre:

- la documentazione ricevuta o inviata resta di proprietà aziendale;
- l'Azienda si riserva di verificare, nei modi ed ai fini consentiti dalla legge, il rispetto delle modalità di utilizzo del servizio di posta, specificate in queste norme.

Va altresì ricordato che come espresso all'interno del documento [6]:

Il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati; in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla già menzionata *policy* datoriale.

Alla luce di quanto sopra esposto, qualora l'utente abbia le necessità di abilitare autorisponditori (ad esempio in caso di assenze prolungate per ferie o in seguito ad attività di lavoro fuori sede) esiste la possibilità di abilitare tali strumenti, per le operazioni del caso ci si riferisca all'HD del SIA al fine di essere guidati alla loro corretta e completa configurazione.

23.1 Disclaimer Automatico

Si ricorda inoltre che ogni messaggio di posta elettronica che esce dal dominio di ASST è corredato da un messaggio, in calce all'e-mail, che riporta la seguente avvertenza sulla Privacy (discalimer)e sulla confidenzialità dei messaggi inviati:

> *Ai sensi del Regolamento (UE) 2016/679, Le informazioni contenute in questo messaggio e ogni documento o file ad esso allegato sono riservati e confidenziali. Il loro utilizzo è consentito esclusivamente al destinatario del messaggio o a diversa persona da questo autorizzata, per le finalità indicate nel messaggio medesimo. Qualora Lei non fosse la persona cui il presente messaggio è destinato, La invitiamo a eliminarlo dal Suo Sistema e a distruggere le varie copie o stampe, dandocene gentilmente comunicazione. Ogni utilizzo improprio è contrario ai principi del Regolamento (UE) 2016/679. ASST di Mantova opera in conformità al Regolamento (UE) 2016/679 citato. Per qualsiasi informazione a riguardo si prega di consultare i riferimenti disponibili nella sezione "Data Protection Officer (DPO)" del nostro sito aziendale.*

Si chiede pertanto di disabilitare qualsiasi altro ulteriore messaggio che l'utente vuole accodare al corpo dell'e-mail.

23.2 Trattamento dei Metadati di Posta Elettronica

Nel contesto dell'utilizzo della piattaforma Microsoft 365 per la gestione della posta elettronica aziendale, si evidenzia che, oltre al contenuto dei messaggi, vengono generati e conservati metadati relativi all'attività degli utenti. Tali metadati includono, a titolo esemplificativo, informazioni su mittente, destinatario, oggetto, orario di invio/ricezione, indirizzi IP, dispositivi utilizzati e log di accesso.
Secondo quanto previsto dal provvedimento del Garante per la Protezione dei Dati Personali del 6 giugno 2024, la raccolta sistematica e preventiva di metadati da parte di fornitori cloud (come Microsoft) deve essere limitata nel tempo, proporzionata e trasparente.
Il datore di lavoro è tenuto a:

- Informare i dipendenti circa la natura e le finalità del trattamento dei metadati;
- Limitare la conservazione dei dati al tempo strettamente necessario (es. 90 giorni per i log di Exchange Online, 7-30 giorni per i log di accesso Entra ID, salvo estensioni per motivi di sicurezza);
- Evitare trattamenti eccedenti o non pertinenti rispetto alle finalità dichiarate.

In conformità al Regolamento (UE) 2016/679 (GDPR), tali trattamenti devono rispettare i principi di liceità, trasparenza, minimizzazione e limitazione della conservazione (artt. 5 e 6), e devono essere oggetto di valutazione d'impatto se comportano rischi elevati per i diritti e le libertà degli interessati.
Inoltre, la Direttiva NIS2, recepita in Italia con il D.lgs. 82/2024, impone agli enti pubblici e sanitari obblighi stringenti in materia di cybersecurity e logging degli accessi, rendendo necessaria la conservazione dei metadati per finalità di sicurezza informatica e risposta agli incidenti.

L'Azienda, pertanto, adotta misure tecniche e organizzative per garantire che l'accesso ai metadati sia limitato al personale autorizzato, per finalità di sicurezza, audit o indagini disciplinari, nel rispetto del principio di accountability e delle Linee guida del Garante.

23.3 CONTROLLI

Premesso che l'azienda potrebbe effettuare controlli generici sull'effettivo adempimento dell'attività lavorativa e il corretto utilizzo degli strumenti di lavoro si precisa quanto segue:

L'ente per esigenze organizzative, di sicurezza, di disponibilità dei servizi, può avvalersi legittimamente e nel rispetto dello statuto dei lavoratori (art. 4), di sistemi che consentono in maniera indiretta un controllo sulle attività di rete che potrebbero determinare un trattamento di dati nei confronti dei lavoratori.

Fermo restando che l'Azienda già adotta misure organizzativa e tecniche al fine di prevenire eventuali utilizzi impropri e distorti degli strumenti informatici (es. black-list, sistemi antivirus e antispyware, sistemi *intrusion prevention* ecc.) gli accessi ad internet vengono comunque e per una questione di sicurezza dei sistemi centrali, registrati all'interno del sistema firewall. L'accesso ai dati è consentito unicamente agli AdS in prima battuta in forma aggregata, ovvero non è possibile individuare direttamente l'utente interessato. Nel caso in cui vengano ravvisate anomalie nel traffico dati o rischi alla sicurezza, il Responsabile per la Cybersecurity invierà al responsabile dell'area coinvolta un avviso generalizzato richiamando gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite all'interno del presente documento. Solo in fasi successive e nei casi di reiterata violazione delle procedure, l'azienda restringerà il campo di intervento ed effettuerà controlli prolungati e costanti fino ad arrivare all'analisi dei singoli file di log.
Gli stessi dati vengono conservati per un periodo di circa sei mesi e successivamente cancellati salvo esigenze tecniche o di sicurezza; se tali informazioni saranno conservate, verranno giustificate tramite apposito verbale indicando le motivazioni e comunque i limiti di tempo di conservazione.
I casi in cui si possono conservare i dati sono:

- Esigenze tecniche o di sicurezza particolari;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- Obblighi su specifiche richieste dell'autorità giudiziaria.

Il Responsabile per la cybersecurity, in collaborazione con il Direttore del SIA, conformandosi ai principi di necessità, correttezza, pertinenza e non eccedenza di cui al Regolamento (UE) 2016/679, potrà provvedere al controllo delle informazioni relative ai dati sopra descritti.

Per la verifica del corretto utilizzo della posta elettronica ed internet:
l'Ads ed il Responsabile per la Cybesecurity:

- si riserva la facoltà di effettuare controlli periodici nei log file, in conformità della legge e al solo fine di garantire la funzionalità e sicurezza del sistema. I dati da elaborare verranno estratti in forma anonimizzata, privi di qualsiasi riferimento che possa essere ricondotto all'utente (matricola, cognome nome, indirizzo IP, MAC Address);
- elabora informazioni di tipo statistico quali accessi a banche dati e visite a siti di interesse, riservandosi la facoltà di raggruppare dati per struttura per verifiche di fruibilità;
- non effettua monitoraggi sistematici delle pagine Web visualizzate dal singolo lavoratore.
- Saltuariamente può estrarre pagine visitate dai dipendenti, prive di riferimenti che possano essere ricondotti al singolo utente, per l'individuazione di siti non correlati all'attività lavorativa, da inserire nel web filtering.

L'attività di monitoraggio viene svolta dal Responsabile per la Cybersecurity in collaborazione con gli uffici preposti a questi servizi, nel rispetto del principio di riservatezza di cui all'art. 5, par. 1, lett f) del GDPR.

24 Applicazioni

L'accesso alle applicazioni specifiche attraverso la rete aziendale, come ad esempio CCE, Portale Sanitario, Sale Operatorie, …, è subordinato all'attribuzione dei corretti diritti di accesso (userID/password/profilo) rilasciati dal gruppo identità digitale (identita.digitale@asst-mantova.it) in base alle richieste di abilitazione provenienti dai responsabili dei servizi sanitari/amministrativi.

L'accesso alle applicazioni è concesso su base personale ed esclusivamente per ragioni e finalità connesse ai compiti del dipendente titolare: pertanto non è consentito cedere a terzi, neppure temporaneamente la "sessione di lavoro" e/o le credenziali d'accesso.
E' vietato:

- *accedere abusivamente alle Applicazioni;*
- *diffondere o detenere abusivamente password;*
- *violare la sicurezza delle Applicazioni;*
- *esportare dati dalle Applicazioni senza permesso;*

Le richieste di nuove abilitazioni, revoche e modifiche dei permessi di accesso alle applicazioni, devono provenire ad identita.digitale@asst-mantova.it a cura dei responsabili dei rispettivi servizi. attraverso la compilazione dell'apposito modulo completo in tutti i campi previsti, ed opportunamente firmato digitalmente.

25 Installazione di nuove applicazioni

La messa a disposizione all'utenza di nuove applicazioni, coperte da opportune licenze d'uso aziendale, o concesse come add-on a forniture di dispositivi, deve essere preventivamente concordate con il SIA in modo che possano essere verificati i presenti requisiti:

1) sia verificato l'aspetto contrattuale relativo alla possibile installazione dell'applicazione in ambiente aziendale;
2) sia verificata la compatibilità con l'hardware e software aziendale: Il nuovo software deve essere compatibile con l'infrastruttura hardware e software esistente governata dal SIA;
3) deve poter integrarsi con altri sistemi già in uso (ad esempio, sistemi di autenticazione MS AD, sistemi di gestione dei pazienti, sistemi di laboratorio, ecc.).
4) sia conforme con le normative di settore: Il software, nel caso in cui tratta dei dati personali e sensibili, deve essere conforme alle normative e requisiti di sicurezza come, ad esempio, il GDPR per la protezione dei dati e le funzionalità di crittografia e controllo degli accessi.
5) Il software permetta l'audit e il logging: deve essere possibile tracciare e registrare tutte le attività all'interno del sistema per eventuali audit di sicurezza.
6) Il software deve essere coperto da contratti di supporto e manutenzione: deve essere definito e garantito un adeguato supporto tecnico e manutenzione continua del software, dei back-up, del patching.

Una volta verificata la conformità del software a quanto indicato, l'installazione, pianificata assieme ai tecnici del SIA sarà effettuata e controllata assieme al fornitore della soluzione applicativa ed installata unicamente sulle pdl individuate.

Al SIA dovranno essere rilasciate copia delle credenziali di amministrazione della stessa in modo che siano possibili interventi di disinstallazione quando uno dei criteri di sicurezza viene a non essere soddisfatto.

Qualunque richiesta di installazione da parte dei fornitori che non sia stata preventivamente comunicata e concordata con il SIA non troverà seguito.

26 PROGETTAZIONE E SVILUPPO DI NUOVE SOLUZIONI INFORMATIZZATE

26.1 Consulenza

Al fine di implementare sistemi aziendali interdipartimentali la cui conformità ai requisiti logici e fisici stabiliti ed individuati dal SIA siano rispettati e nell'ottica di garantire una continuità operativa necessaria per gli applicativi sanitari è vincolante ottenere la liberatoria all'implementazione delle soluzioni da parte del SIA già a partire dalle fasi progettuali; la progettazione e lo sviluppo di soluzioni che necessitino l'introduzione in azienda di apparati HW e soluzioni SW comporta la negoziazione delle specifiche in fase preliminare con gli esperti individuati dal responsabile dei Sistemi Informativi Aziendali.
Le specifiche da negoziare devono comunque riguardare i seguenti ambiti operativi:

1. Definizione delle competenze ed individuazione degli amministratori di sistema con nomina formale dei responsabili;
2. Individuazione delle responsabilità relativamente alla gestione della manutenzione;
3. Definizione delle caratteristiche connettività fisica e logica: protocollo, indirizzamento, definizione degli utenti;
4. Definizione degli standard (sistemi operativi, ecc..);
5. Definizione ed integrazione con gli eventuali sistemi aziendali;
6. Sicurezza informatica: patching ed antivirus aziendali

Relativamente al 3 si deve comunque sottolineare che qualunque PDL inserita sulla rete aziendale deve essere provvista di almeno un account con profilazione d'Amministratore ad uso eclusivo degli operatori del SIA, in caso contrario, tali operatori saranno comunque autorizzati al distacco della stessa dalla rete aziendale al fine di tutelare il corretto funzionamento e la sicurezza dell'infrastruttura informatica.

27. FORNITURE DI HARDWARE E SOFTWARE

27.1 Acquisti

Qualunque acquisto di apparecchiatura hardware e software deve essere preventivamente concordata con il SIA al fine di poter dare parere tecnico sulla conformità rispetto alle attuali configurazioni ed integrazioni tra i sistemi.
Per ogni acquisto è comunque valida la normativa attualmente in vigore per le pubbliche Amministrazioni e le procedure in essere alla base del sistema gestionale amministrativo.
Ogni apparecchiatura hardware deve essere acquistata con una copertura di garanzia di almeno tre anni, on-site, next-day.
Per qualsiasi informazione siete pregati di inviare una comunicazione preventiva agli indirizzi forniti al par. 8

27.2 Richieste di fornitura hardware

Saranno accettate unicamente richieste di fornitura di materiale hardware, non previste dalla gestione globale dei sistemi informativi aziendali, solo se accompagnate da motivazione e/o progetto nell'ambito del quale si rende necessario acquisire quanto indicato una volta che la copertura economica per l'acquisto sia garantita.
Le apparecchiature hardware, di qualunque genere nell'ambito informatico, non devono essere in contrasto con il regolamento SIA e della Sicurezza dei Sistemi Informativi.

28. Responsabilità

I responsabili delle Unità Operative e/o Servizi Aziendali dovranno adottare misure idonee per un corretto utilizzo delle risorse informatiche messe a disposizione della loro struttura, esercitando una funzione di istruzione, indirizzo e controllo sugli utenti incaricati ed individuando con precisione le responsabilità per la gestione dei dati, dei salvataggi e delle risorse stesse.

In caso di cessazione del rapporto di lavoro, trasferimento ad altro servizio, o comunque di non necessità di utilizzo da parte di utenti già autorizzati, sarà data tempestiva comunicazione scritta, per gli applicativi da esso gestiti, al SIA che provvederà alla disattivazione delle credenziali di autenticazione ovvero alla loro modifica per ogni diversa esigenza.

Gli utenti che utilizzano le risorse informatiche si impegnano a rispettare il presente regolamento, ed in particolare:

- mantenere una adeguata riservatezza dei dati;
- mantenere una adeguata riservatezza sulle misure di sicurezza adottate e sulle modalità di accesso;
- utilizzare esclusivamente le risorse al cui utilizzo essi sono abilitati;
- segnalare tempestivamente al SIA ogni malfunzionamento ed ogni accertata violazione delle norme che regolano l'utilizzo delle risorse informatiche;

Il SIA è responsabile della sicurezza, della funzionalità, della continuità operativa e del corretto impiego delle risorse informatiche centralizzate e della intera infrastruttura informativa dell'ente.

Non rientrano nelle proprie competenze la gestione e l'assistenza tecnica:

- delle apparecchiature elettromedicali (di competenza Ingegneria Clinica);
- dei sistemi informatici di quelle unità operative (Laboratorio Analisi, Radiologia, Centro Trasfusionale, Anatomia Patologica, etc.) che ospitano nelle loro sedi i server dedicati, sui quali però rimane obbligatoria l'installazione di soluzione EDR/XDR che può essere effettuata contattando l'HELP-DESK del SIA.

La gestione e responsabilità di questi ultimi è demandata ai singoli Direttori che provvedono ad assegnare agli utenti, da loro incaricati, le credenziali di autenticazione ed autorizzazione, verificano la corretta applicazione delle misure minime di sicurezza e che hanno rapporti diretti con le società fornitrici, con le quali l'Azienda ha provveduto a stipulare contratti di manutenzione ed assistenza tecnica anche con collegamenti da remoto. Per le postazioni personal computer "stand alone", ossia non collegate in rete, la responsabilità nell'applicazione delle misure minime di sicurezza è demandata all'utente finale ed al direttore dell'Unità Operativa/Sevizio che le ha in dotazione.

Va inoltre ricordato che poiché l'accesso agli applicativi aziendali è fornito tramite account personale nominativo protetto da password personale le eventuali controversie anche di natura legale che si potranno manifestare come conseguenza ad un utilizzo non congruo dello strumento saranno imputate direttamente all'utente possessore delle credenziali con le quali sono state compiute operazioni illecite.

RIFERIMENTI NORMATIVI

[1] “Norme sulla tutela delle libertà e dignità dei lavoratori, della libertà sindacala e nell’attività sindacale nei luoghi di lavoro e norme sul collocamento” (Statuto dei lavoratori) Legge 20 maggio 1979, n. 300

[2] “Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni” Direttiva 16 gennaio 2002; DPCM 16 gennaio 2002, Dipartimento per l'innovazione e le tecnologie;

[3] Linee guida AgID sulla sicurezza ICT (2022);

[4] Regolamento ACN su servizi cloud per PA (2023);

[5] Norme tecniche del Ministero Salute su FSE 2.0 e interoperabilità applicativa.

[6] "Codice in materia di protezione dei dati personali”, Decreto Legislativo 30 giugno 2003, n. 196

[7] Decreto legislativo 10 agosto 2018, n. 101: 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)(GU Serie Generale n.205 del 04-09-2018)

[8] “Codice dell’Amministrazione Digitale” Decreto Legislativo 7 marzo 2005, n.82;

[9] Decreto Legislativo 18 maggio 2018, n. 65 Attuazione della 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. (18G00092) (GU Serie Generale n.132 del 09-06-2018)

[1 0] “Linee Guida per la Pubblica Amministrazione Digitale”, Direttiva 18 novembre 2005;

[1 1] “Linee guida del Garante per posta elettronica e internet”, Gazzetta Ufficiale n. 58 del 10 marzo 2007;

[1 2] “Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro”, Direttiva 02/09, Dipartimento della Funzione Pubblica

[1 3] “Regolamento aziendale per l’assegnazione e l’uso delle apparecchiatura di telefonia mobile e delle ralative utenze”, Delibera n. 423 del 02/04/2020 ASST di Mantova