Sistema Socio Sanitario
Regione Lombardia
ASST Cremona

DECRETO N. 983 **DEL 28/10/2026**

OGGETTO: APPROVAZIONE DEL REGOLAMENTO AZIENDALE DISCIPLINANTE L'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI E PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

Struttura proponente: S.C. AFFARI GENERALI E LEGALI

Responsabile del procedimento: MARIANNA BONFANTI

IL DIRETTORE GENERALE	DOTT. EZIO BELLERI
Acquisito il parere favorevole del DIRETTORE AMMINISTRATIVO	DOTT. GIANLUCA LEGGIO
Acquisito il parere favorevole del DIRETTORE SANITARIO	DR. FRANCESCO REITANO
Acquisito il parere favorevole del DIRETTORE SOCIOSANITARIO	DR. GIORGIO SCIVOLETTO

PREMESSO che:
- gli strumenti informatici aziendali costituiscono uno dei principali strumenti di lavoro messi a disposizione del personale che, a qualunque titolo, presta attività lavorativa presso l'Azienda;
- l' Azienda, è tenuta a garantire un uso corretto e funzionale allo svolgimento dell'attività lavorativa dei sistemi informativi aziendali da parte del personale utilizzatore;

VISTI E RICHIAMATI:
- la normativa nazionale e sovranazionale in materia di sicurezza informatica di cui al decreto legislativo 4 settembre 2024, n. 138, che recepisce la direttiva (UE) 2022/2555 (NIS2);
- le Linee Guida del Garante della Protezione dei Dati Personali per l'utilizzo della posta elettronica e internet del 10 marzo 2017;
- l'art. 4 della legge 20 maggio 1970, n. 300, che, nel quadro normativo sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento, disciplina l'impiego di impianti audiovisivi e altri strumenti di controllo per esigenze organizzative e produttive;
- il Regolamento (UE) 2016/679, recante il Regolamento generale sulla protezione dei dati (GDPR);
- il codice di comportamento e il codice etico di quest'Azienda;

RITENUTO di dover definire, mediante adozione di una policy interna:
- le modalità tecniche ed operative di impiego delle risorse informatiche messe a disposizione del personale utilizzatore nell'ambito organizzazione dell'attività lavorativa;
- i limiti entro i quali il personale utilizzatore può legittimamente fare uso dei sistemi informativi aziendali nello svolgimento della propria attività;
- le misure necessarie a garantire disponibilità, sicurezza e integrità delle attrezzature informatiche, dei dispositivi digitali, dei servizi applicativi e informativi aziendali;

CONSIDERATO che, alla luce della normativa sopra richiamata, la policy aziendale in tema di utilizzo degli strumenti informatici aziendali, deve essere orientata al perseguimento e alla conciliazione dei seguenti obiettivi generali:
- disponibilità delle informazioni a supporto dei processi sanitari, sociosanitari e amministrativi, delle risorse tecnologiche e delle capacità elaborative necessarie al loro trattamento;
- integrità delle informazioni, attraverso processi che ne assicurino consistenza, completezza e validità ai fini dei processi aziendali;
- riservatezza dei dati aziendali gestiti, prevenendone la divulgazione e l'uso improprio;

con la piena osservanza dei principi in materia di protezione dei dati personali;

RITENUTO, pertanto, opportuno procedere all'adozione del Regolamento aziendale disciplinante l'utilizzo degli strumenti informatici aziendali e per la sicurezza del trattamento dei dati, allegato e costituente parte integrante e sostanziale del presente provvedimento, proposto dal Direttore della SC Sistemi Informativi aziendali e dal Direttore S.C. Affari Generali e Legali, come da nota protocollo n. 59584/26 in atti;

ATTESO che, a fronte dei ritmi dell'innovazione tecnologica e della progressiva integrazione, anche nel contesto della Pubblica Amministrazione, di strumenti basati su algoritmi e modelli di Intelligenza Artificiale, questa Azienda si riserva di procedere, in una fase successiva, a completare la sopra richiamata policy aziendale in tema di sistemi informativi attraverso l'adozione di un apposito documento disciplinante principi e modalità di implementazione e impiego di detta tecnologia, al fine di garantire la piena osservanza della normativa nazionale e sovranazionale vigente in materia, nonché il massimo livello di conciliazione delle esigenze di progressiva innovazione, con quelle di riservatezza, protezione dei dati personali e di sicurezza aziendale;

PRESO ATTO dell'attestazione resa dal Responsabile del procedimento in ordine alla regolarità tecnica del presente provvedimento;

ACQUISITI i pareri favorevoli del Direttore Amministrativo, del Direttore Sanitario e del Direttore Sociosanitario;

DECRETA

1. per tutte le motivazioni espresse in narrativa, di approvare il Regolamento aziendale disciplinante l'utilizzo degli strumenti informatici aziendali e per la sicurezza del trattamento dei dati, allegato e costituente parte integrante e sostanziale del presente provvedimento;
2. di dare atto che dal presente provvedimento non derivano oneri a carico del bilancio aziendale;
3. di provvedere alla pubblicazione del Regolamento aziendale oggetto del presente provvedimento sul sito web istituzionale nella sezione "Amministrazione Trasparente", come da normativa vigente;
4. di dare atto che il presente provvedimento è immediatamente esecutivo ai sensi dell'articolo 17, comma 6, della legge regionale della Regione Lombardia 30 dicembre 2009, n. 33.

IL DIRETTORE GENERALE
DOTT. EZIO BELLERI

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge

Direzione Generale

REGOLAMENTO AZIENDALE DISCIPLINANTE L'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI E PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

Sommario

GLOSSARIO 4
ART. 1 PREMESSA 5
1.1. Scopo 5
1.2. Campo di applicazione 6
ART. 2 PRINCIPI GENERALI 6
2.1. Responsabilità e principio di non-ricusazione 6
2.2. Protezione dei dati dalla progettazione e per impostazione predefinita 7
ART. 3 REGOLE PER L'UTILIZZO DELLE RISORSE INFORMATICHE 7
3.1. Titolarità delle attrezzature informatiche e dei dati trattati 7
3.2. Finalità dell'utilizzo delle attrezzature informatiche e dei dispositivi 7
3.3. Abilitazione all'utilizzo delle attrezzature informatiche aziendali e modalità di accesso 8
3.3.1. Regole per la configurazione delle credenziali personali 8
3.3.2. Regole per la gestione delle credenziali personali 9
3.3.3. Utenze generiche 10
3.3.4. Autenticazione a due fattori (2FA) e autenticazione multifattore (MFA) 10
3.4. Protezione delle postazioni di lavoro 11
3.4.1. Operazioni di Login e Logout 11
3.4.2. Salvaschermo 12
3.4.3. Obblighi dell'utente 12
3.4.4. Utilizzo e gestione del Personal Computer aziendale 12
3.4.5. Divieti espressi riguardanti l'utilizzo del Personal Computer aziendale 13
3.5. File Server per file sharing e cartelle condivise all'interno dell'Ente 13
3.6. Utilizzo della rete Internet e dell'account di posta elettronica 14
3.6.1. Internet 14
3.6.2. Posta Elettronica 15
3.6. Videoconferenze 18
3.7. Utilizzo di altri dispositivi 18
3.7.1. Utilizzo del notebook, tablet o smartphone 18
3.7.2. Memorie esterne (pendrive usb, hard disk, memory card, cd-rom, dvd, ecc.) 19
3.7.3. Restituzione dei *device* 19
3.7.4. Device personali 19
ART. 4 SISTEMI IN CLOUD 19
4.1. Cloud computing 19

4.2. Utilizzo di sistemi Cloud 20
ART. 5 PRINCIPALI MINACCE E MISURE DI SICUREZZA 20
5.1. Classificazione delle principali minacce 20
5.2. Le principali misure di sicurezza aziendali 22
ART. 6 SEGNALAZIONE ANOMALIE E MALFUNZIONAMENTI 23
ART. 7 CESSAZIONE DELL'UTILIZZO DEGLI STRUMENTI INFORMATICI DELL'ASST 23
ART. 8 CONTROLLI E SANZIONI 24
ART. 9 NOTE FINALI 24
ART. 10 ENTRATA IN VIGORE, PUBBLICITÀ E VALIDITÀ 24

GLOSSARIO

- **Autenticazione a due fattori (2FA) e autenticazione multi-fattore (MFA):** metodi di sicurezza che aggiungono ulteriori livelli di protezione nella procedura di accesso ad account, applicazioni e servizi, richiedendo la conferma dell'identità dell'utente mediante uno o più fattori aggiuntivi rispetto a quello base, normalmente costituito dalla password, riducendo il rischio di accesso non autorizzato. I metodi di autenticazione a due o più fattori sono anche definiti metodi di "autenticazione forte".
- **Credenziali di dominio:** credenziali, connesse al dominio aziendale, che consentono di accedere alla postazione di lavoro, alla posta elettronica, ai software applicativi aziendali ed alla rete aziendale.
- **Credenziali SISS:** l'insieme degli strumenti di autenticazione attribuiti agli utenti autorizzati del Sistema Informativo Socio-Sanitario della Regione Lombardia, utilizzati per accedere ai servizi e alle informazioni del sistema, assicurando l'identificazione dell'utente, la tracciabilità delle operazioni effettuate e il rispetto dei requisiti di sicurezza previsti dal SISS.
- **Sistema Informativo Socio-Sanitario (SISS):** sistema federato regionale che integra applicazioni e infrastrutture informatiche di farmacie, medici, ospedali, Regione Lombardia e altri attori sanitari, permettendo la cooperazione e lo scambio di informazioni tra i diversi sistemi autonomi per supportare l'organizzazione e l'erogazione dei servizi socio-sanitari.
- **Dati personali**: informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc…
- **Firma remota**: sistema di firma digitale che consente al titolare di sottoscrivere documenti informatici mediante un certificato qualificato le cui chiavi di firma sono custodite presso infrastrutture remote sicure gestite da un prestatore di servizi fiduciari. L'utilizzo della firma è subordinato all'autenticazione forte del titolare e garantisce l'identificazione certa del sottoscrittore, l'integrità del documento e la validità legale della sottoscrizione.
- **Log**: termine utilizzato per indicare la registrazione sequenziale e cronologica delle operazioni effettuate, da un utente, un amministratore o automatizzate, man mano che vengono eseguite dal sistema o applicazione. Il file, o insieme di file, su cui tali registrazioni sono memorizzate ed eventualmente accedute in fase di analisi dei dati, detto anche registro eventi.
- **Malware:** software che, una volta eseguito, danneggia il funzionamento e la sicurezza del sistema operativo
- **Metadati**: termine utilizzato nel linguaggio informatico per definire un insieme di informazioni sui dati. I metadati relativi alla posta elettronica sono delle "stringhe descrittive", generate automaticamente dai sistemi server di gestione e smistamento della posta elettronica. I metadati rappresentano le caratteristiche o le proprietà della e-mail, tipicamente data, ora di invio, destinatario, mittente e indirizzo IP, ma non il contenuto o gli allegati - ossia il c.d. envelope (ovvero, l'insieme delle intestazioni tecniche organizzate che registrano il percorso del messaggio, la sua origine e altri dettagli tecnici).
- **Phishing**: tipo di frode ideato allo scopo di rubare l'identità di un utente della Rete. Quando viene attuato, una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti. Il phishing viene generalmente attuato tramite posta indesiderata o finestre a comparsa.
- **Spear phishing**: tipo di frode con la quale, una mail viene indirizzata a una persona, un'organizzazione o un'azienda specifica con l'obiettivo di sottrarre dati per scopi dannosi (es. installazione malware sul computer dell'utente preso di mira).
- **Pharming**: tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato ed indirizzato direttamente verso un server web clone che lo porterà a rivelare inconsapevolmente a sconosciuti i propri dati sensibili, come numero di conto corrente, nome utente, password, numero di carta di credito.

- **Smishing**: forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti (ad esempio, per poi sottrarre denaro da conti e carte di credito). I messaggi di smishing invitano i destinatari a compiere azioni (cliccare link, ecc.) o fornire informazioni con urgenza, per non rischiare danni (es: blocco di utenze, blocco della carta di credito o del conto) o sanzioni.
- **Trattamento di categorie particolari di dati personali (ex sensibili)**: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.
- **Trattamento dei dati personali relativi a condanne penali e reati**: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (es. i provvedimenti penali di condanna definitivi) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- **Utente**: il soggetto fisico che, in quanto autorizzato, usufruisce delle dotazioni informatiche messe a disposizione dell'ASST.

ART. 1 PREMESSA

L'Azienda Socio-Sanitaria Territoriale di Cremona (di seguito nel presente Regolamento indicata come "ASST") dispone di una architettura informatica complessa ed articolata, attraverso la quale vengono resi disponibili sistemi, tecnologie e servizi che supportano il corretto ed efficace svolgimento delle attività di ambito sanitario, sociosanitario ed amministrativo.

Il personale che opera a diverso titolo presso l'ASST usufruisce di strumenti e servizi informatici messi a disposizione dall'Azienda stessa per lo svolgimento delle rispettive attività professionali.

Il corretto utilizzo delle attrezzature informatiche, postazioni di lavoro, dispositivi, servizi applicativi ed informativi da parte degli utenti aziendali è un requisito fondamentale per assicurare il corretto funzionamento dell'intera architettura informatica, la valorizzazione del patrimonio informativo e la protezione dei dati che vengono trattati per lo svolgimento delle attività istituzionali.

1.1. Scopo

Il presente "Regolamento aziendale disciplinante l'utilizzo degli strumenti informatici aziendali e per la sicurezza del trattamento dei dati " descrive le modalità tecniche ed operative con le quali devono essere utilizzate le attrezzature informatiche, i dispositivi digitali, i servizi applicativi e informativi da parte degli utilizzatori autorizzati, in conformità all'art. 4 comma 2 della legge 20 maggio 1970 n. 300, come modificata dal decreto legislativo n. 151/2015, al Regolamento Europeo n. 679/2016 "General Data Protection Regulation" (GDPR) ed alle Linee Guida del Garante per l'utilizzo della posta elettronica e internet del 10 marzo 2017 ed alla normativa nazionale in materia di sicurezza informatica di cui al decreto legislativo n. 138/2024 (NIS2).

Scopo del Regolamento è quello di indicare i limiti entro i quali i fruitori possono legittimamente usare gli strumenti elettronici messi a disposizione dall'ASST nello svolgimento delle proprie attività, al fine di assicurare il più alto livello possibile di protezione dei dati gestiti, contribuendo in modo significativo al raggiungimento dei seguenti obiettivi generali:

- riservatezza delle informazioni, attraverso la prevenzione di divulgazione ed uso improprio dei dati;
- disponibilità delle informazioni a supporto dei processi socio - sanitari e disponibilità delle risorse

tecnologiche e delle capacità elaborative necessarie al loro trattamento;
- integrità delle informazioni, attraverso processi che assicurino la consistenza, completezza e validità delle informazioni ai fini dei processi socio - sanitari.

Il documento intende rappresentare un riferimento generale rivolto a tutto il personale che opera presso l'ASST, sin dal momento dell'assunzione o dell'instaurazione della collaborazione, e descrive in modo chiaro e comprensibile le modalità tecniche, operative e comportamentali a cui gli utilizzatori si devono attenere, costituendo, in tal senso, anche uno strumento di formazione e di sensibilizzazione nell'ambito degli obiettivi e delle politiche di sicurezza delle informazioni adottati dall'ASST.

1.2. Campo di applicazione

Il Regolamento disciplina le modalità di utilizzo di qualsiasi dotazione informatica (attrezzature e servizi informatici di utilizzo generale) resi disponibili dall'ASST al personale che opera a diverso titolo nei reparti, servizi ed uffici dell'Azienda.

Il Regolamento si applica a qualsiasi dotazione ICT intesa come risorsa informatica e/o telematica (a titolo esemplificativo e non esaustivo: computer, notebook, server, software, rete, utenza, file, cartella di rete, internet key, telefono, tablet, smartphone, modem, pendrive, router ecc..), messa a disposizione dall'ASST all'utente per rendere la prestazione lavorativa.

Ai fini della sicurezza, si identificano come "risorse informatiche":

- *gli apparati fisici e i dispositivi*, direttamente coinvolti nel processo di elaborazione, archiviazione e trasmissione delle informazioni: essi sono definiti sensibili quando il loro danneggiamento, alienazione o distruzione può provocare l'interruzione di funzionamento e la conseguente sospensione di servizio, ovvero la diffusione di informazioni;
- *i Sistemi operativi*: essi sono definiti sensibili quando la loro modifica, cancellazione o indisponibilità può comportare l'interruzione di funzionamento e la conseguente sospensione del servizio, ovvero la possibilità di accesso o alterazione di dati da parte di personale non autorizzato;
- *il Software applicativo*: esso è definito sensibile quando la sua manomissione, cancellazione o indisponibilità può produrre la sospensione di alcune funzioni, l'alterazione delle corrette caratteristiche di funzionamento del sistema informativo ovvero la possibilità di accesso o alterazione di dati da parte di personale non autorizzato;
- *le Informazioni (dati): e*ssi sono definiti sensibili quando la loro indisponibilità, manomissione o divulgazione può provocare la sospensione di funzioni del sistema informativo o compromettere il suo corretto funzionamento o procurare danno diretto o indiretto all'Azienda.

Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello e a tutti i collaboratori dell'ASST, a prescindere dal rapporto contrattuale con la stessa intrattenuto e a chiunque abbia in dotazione, anche temporaneamente, risorse informatiche e telematiche di proprietà dell'ASST o ad essa affidate. Tali soggetti, nell'ambito del Regolamento, sono indicati anche come "utente", "utilizzatore" "autorizzato".

ART. 2 PRINCIPI GENERALI

2.1. Responsabilità e principio di non-ricusazione

Chiunque usi risorse informatiche della ASST deve operare nei limiti delle proprie competenze e secondo le norme definite.

L'operato dell'utente su risorse classificate sensibili in quanto a riservatezza, disponibilità ed integrità, deve essere riconducibile ad una non negabile responsabilità personale, attraverso opportuni meccanismi di autenticazione (non-ricusazione).

Chiunque operi in violazione delle norme aziendali o al di fuori delle proprie competenze è sottoposto ai provvedimenti indicati nel paragrafo "Controlli e sanzioni", in relazione alla gravità dell'operato.

2.2. Protezione dei dati dalla progettazione e per impostazione predefinita

L'attività dell'ASST inerente alla gestione ed utilizzo di un sistema o di un servizio informatico è ispirata ai seguenti principi:

- *Privacy by design*: ossia la considerazione dei principi di riservatezza e protezione dei dati personali a partire dalla progettazione di un trattamento dei dati e delle relative applicazioni informatiche di supporto (in particolare la necessità di minimizzare l'uso del dato e la necessità di tutelare i diritti dell'interessato);
- *Privacy by default*: l'adozione di misure tecniche ed organizzative che garantiscano, per impostazione predefinita, che siano trattati solo i dati necessari per ogni specifica finalità del trattamento.

ART. 3 REGOLE PER L'UTILIZZO DELLE RISORSE INFORMATICHE

3.1. Titolarità delle attrezzature informatiche e dei dati trattati

L'ASST è esclusiva titolare e proprietaria delle attrezzature informatiche, delle periferiche associate e dei dispositivi mobili messi a disposizione degli utilizzatori ai soli fini dell'attività lavorativa.

L'ASST è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante le proprie attrezzature informatiche e dispositivi.

Il personale non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nelle attrezzature informatiche aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi sia internamente che esternamente senza l'autorizzazione dell'ASST.

3.2. Finalità dell'utilizzo delle attrezzature informatiche e dei dispositivi

Le attrezzature ed i dispositivi informatici assegnati sono uno strumento lavorativo nelle disponibilità degli utilizzatori esclusivamente per un fine di carattere lavorativo / professionale (in relazione alle mansioni assegnate). I dispositivi informatici, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza aziendale. Ai dipendenti e ai collaboratori è consentito l'utilizzo di strumenti informatici forniti dall'ASST per poter assolvere ad incombenze personali senza doversi allontanare dalla sede di servizio purché l'attività sia contenuta in tempi ristretti, senza alcun pregiudizio per i compiti istituzionali e a condizione che non venga in alcun modo messa a rischio l'infrastruttura informativa aziendale.

Qualsiasi eventuale tolleranza da parte dell'ASST, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Regolamento.

3.3. Abilitazione all'utilizzo delle attrezzature informatiche aziendali e modalità di accesso

3.3.1. Regole per la configurazione delle credenziali personali

All'inizio del rapporto lavorativo o di consulenza, la S.C. Gestione e Sviluppo delle Risorse Umane con il supporto della S.C. Sistemi Informativi Aziendali, avvia il processo di abilitazione del personale all'uso delle attrezzature informatiche aziendali di base.

La dotazione standard per i dipendenti e collaboratori a vario titolo è costituita dalle seguenti attrezzature e servizi di comunicazione di base:

- Personal Computer e periferiche associate;
- servizio di posta elettronica con casella personale;
- servizio di navigazione Internet/Intranet con accesso individuale;
- servizi di comunicazione (telefonia e messaggistica, se previsto).

L'accesso alla dotazione aziendale di base è possibile principalmente mediante le c.d. ***credenziali di dominio*** (nome utente e password). Si tratta di credenziali connesse al dominio aziendale – **asst-cremona.it** – che identifica l'Ente in modo univoco attraverso Internet ed i servizi ad esso connessi**.**
Le credenziali di dominio sono configurate, al momento dell'assunzione, su impulso della SC Gestione e Sviluppo delle Risorse Umane – per i dipendenti – o del Responsabile della Struttura che prenderà in carico del lavoratore all'interno dell'ASST – per i non dipendenti –, con il supporto dell'Help Desk informatico e dei Sistemi Informativi Aziendali, seguendo le indicazioni riportate nella procedura operativa pubblicata nella sezione Sistemi Informativi della Intranet aziendale.
La dotazione aziendale standard è completata dall'accesso agli **applicativi dipartimentali**, ossia i sistemi implementati dall'azienda a supporto all'attività clinica, assistenziale e amministrativa quotidiana.
L'accesso a tali applicativi è subordinato ad una richiesta ad hoc formulata, dal Responsabile della Struttura di appartenenza del dipendente o collaboratore, mediante compilazione, sottoscrizione e invio dell'apposito modulo all'Help Desk informatico. La procedura operativa per la richiesta delle credenziali in argomento e il relativo modulo, sono disponibili nella sezione Sistemi Informativi della Intranet aziendale.
In caso di cambiamenti organizzativi e/o di modifiche o di cessazione del rapporto che lega l'utente all'ASST, la S.C. Gestione e Sviluppo delle Risorse Umane provvede alla corretta e tempestiva informazione al Servizio Sistemi Informativi Aziendali affinché lo stesso proceda a creare, cancellare o modificare i profili di accesso (account) alle risorse informatiche aziendali, per garantirne il corretto e dovuto accesso ed evitare possibili abusi o illeciti. Le informazioni e le azioni da attuare sono così riassumibili:

EVENTO	ATTIVITA'	RICHIEDENTE
Assunzione/modifica rapporto di lavoro/mobilità interne/altri (es. interinali, specializzandi)	Creazione/modifica profilo utente	S.C. Gestione e Sviluppo delle Risorse Umane / Responsabile Struttura
Cessazione dipendente o collaboratore	Chiusura profilo utente	S.C. Gestione e Sviluppo delle Risorse Umane
Attivazione/Cessazione contratto fornitore	Creazione/chiusura profilo utente	RUP/DEC

L'accesso agli applicativi e alle infrastrutture del Sistema Informativo Socio-Sanitario (SISS) di Regione Lombardia, invece, avviene mediante le c.d. ***credenziali SISS***.
Le credenziali SISS vengono rilasciate, al momento dell'assunzione o in altro successivo momento,

direttamente dalla S.C. Gestione e Sviluppo delle Risorse Umane, previa apposita istanza formulata da parte del Responsabile di Struttura che prende in carico l'utente e indirizzata ai contatti dell'ufficio PDA/PDR.
Qualora il dipendente sia già in possesso delle credenziali SISS (ad esempio, in quanto configurate nell'ambito di precedente rapporto di lavoro intrattenuto con altra azienda del SSR oppure nell'ambito dell'attività svolta presso altra Struttura), previa apposita richiesta del Responsabile di Struttura all'ufficio PDA/PDR, quest'ultimo provvederà a modificare i profili di visibilità intestati all'utente per adeguarli al nuovo contesto aziendale o di unità operativa.
Nel SSR lombardo, il SISS incorpora il sistema di **firma remota**, il cui certificato è generato proprio con la configurazione delle credenziali SISS (per un approfondimento sulla firma remota si veda par. 3.3.4.).

3.3.2. Regole per la gestione delle credenziali personali

L'utilizzo di credenziali individuali con password riservate e adeguatamente protette rappresenta il principale metodo di autenticazione utilizzato dall'ASST per garantire l'accesso protetto ad un sistema informatico oppure ad un applicativo software.

Le credenziali sono connotate da riservatezza e segretezza. In altre parole, le credenziali, e in particolar modo la password, NON devono essere memorizzate su supporti facilmente intercettabili da altre persone e NON devono essere svelate ad altri soggetti. La divulgazione delle proprie credenziali o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'ASST nel suo complesso.

La sicurezza della password personale diminuisce nel tempo e, pertanto, è necessario che ciascun utente provveda periodicamente alla sua sostituzione (per ulteriori indicazioni sulla gestione delle password si veda il successivo sottoparagrafo). In particolare, l'ASST chiede obbligatoriamente a tutti gli utilizzatori non amministratori di sistema **la sostituzione periodica della password di dominio entro 90 giorni.**

Le credenziali non utilizzate da almeno ***6 mesi*** sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, che rimangono nella disponibilità esclusiva degli amministratori di sistema e di eventuali sistemi automatizzati che ne fanno uso per l'erogazione di servizi.
A discrezione dell'Ente, le credenziali possono essere disattivate a fronte di particolari condizioni (ad esempio un cambiamento del rapporto di lavoro).
In caso specifico di cessazione del rapporto di lavoro le credenziali vengono disattivate **dopo 30 giorni** solo per consentire l'accesso al portale del dipendente per il recupero dell'ultima busta paga.
I casi che richiedano l'immediata disattivazione delle utenze dovranno essere comunicati tempestivamente alla S.C. Sistemi Informativi Aziendali.

Su apposita segnalazione veicolata via ticket relativa al cambio di ruolo/struttura/S.C., la S.C. Sistemi Informativi Aziendali provvede alla riallocazione delle risorse informatiche associate al nuovo ruolo/struttura/S.C.

Regole per la corretta gestione delle Password

L'utente, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

1. le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. occorre cambiare immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura" o su segnalazione del SIA a fronte di sospette compromissioni;
3. le password devono avere le seguenti caratteristiche minime: lunghezza di 12 caratteri (per gli amministratori di sistema la lunghezza è maggiore) e devono contenere lettere maiuscole, minuscole, caratteri speciali e numeri;

4. le password non devono essere memorizzate su alcun tipo di supporto facilmente consultabile da terzi (ad esempio Post-It sul monitor o sotto la tastiera) o agende condivise (cartacee, posta elettronica, telefono cellulare);
5. è vietato affidare agli applicativi qualsiasi memorizzazione automatica delle credenziali di accesso (caching) e l'utente è tenuto a digitare la password ad ogni accesso;
6. è obbligatoria la sostituzione della password entro ***90 giorni*** di calendario;
7. evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ASST.

Password non ammesse

Al fine di una corretta gestione delle password, l'ASST stabilisce il divieto di utilizzare come propria password:

1. nome, cognome e loro parti;
2. lo username assegnato;
3. una password già impiegata in precedenza fino ad un pregresso di 12 volte.

La password ideale non deve contenere riferimenti a dati personali e/o terminologie inappropriate, e deve essere facile da ricordare.

3.3.3. Utenze generiche

L'adozione di un sistema di autenticazione basato principalmente sull'utilizzo di credenziali individuali, personali e non cedibili risponde al principio di accountability, garantendo l'identificazione univoca dell'utilizzatore e la tracciabilità degli accessi e delle operazioni effettuate.

Pertanto, **non è previsto il rilascio di utenze generiche o condivise**. Sono **fatte salve**, esclusivamente per specifiche esigenze organizzative, le **utenze generiche di dominio già in essere.**

Anche in tali casi, tuttavia, l'utilizzo di utenze generiche non costituisce una buona prassi, rendendo difficoltosa l'attribuzione univoca delle operazioni effettuate al singolo utilizzatore e, conseguentemente, l'individuazione delle relative responsabilità, con possibili implicazioni in materia di accountability.

Nelle more delle azioni necessarie alla progressiva dismissione e definitiva eliminazione delle utenze generiche di dominio, **il relativo utilizzo è, pertanto, fortemente sconsigliato e deve essere limitato ai soli casi di effettiva necessità organizzativa.**

3.3.4. Autenticazione a due fattori (2FA) e autenticazione multifattore (MFA)

L'autenticazione a due fattori (2FA) e l'autenticazione multifattore (MFA) sono metodi di sicurezza che aggiungono uno o più livelli di protezione nella procedura di accesso ad account, applicazioni e servizi telematici, richiedendo la conferma dell'identità dell'utente mediante due o più fattori di autenticazione.

Tra i fattori di autenticazione – elementi di prova dell'identità dell'utente – vi sono:

- Qualcosa che l'utente sa (es. password, PIN, passphrase).
- Qualcosa che l'utente ha (es. dispositivo fisico – es. smartphone –, token di sicurezza, passkey, smart card).
- Qualcosa che l'utente è (es. impronta digitale, riconoscimento facciale).

L'autenticazione a due o più fattori, richiedendo all'utente, oltre a "qualcosa che sa" – normalmente la password – anche "qualcosa che ha" e/o "qualcosa che è", costituisce un metodo di c.d. "autenticazione forte", riducendo il rischio di accesso non autorizzato, anche in caso di compromissione della password.

ASST Cremona si avvale di metodi di "autenticazione forte" principalmente nei casi in cui l'utente debba accedere alla rete aziendale da una rete esterna, ad esempio dalla propria abitazione o durante trasferte, mediante browser (es. casella posta elettronica e VPN aziendali); oppure, per l'accesso a sistemi di particolare rilevanza, in considerazione della natura particolare dei dati trattati e degli effetti delle operazioni sugli stessi effettuate (es. Menù SISS, sistema di firma remota).

Le modalità di autenticazione a due o più fattori e i sistemi che richiedono metodi di "autenticazione forte" sono indicate nelle procedure operative pubblicate sulla Intranet aziendale.

3.3.5. La firma remota e SISS

La firma remota è una particolare modalità di firma digitale nella quale il certificato qualificato di firma non risiede su una smart card o token USB posseduto fisicamente dall'utente, ma è custodito in modo sicuro presso un prestatore di servizi fiduciari qualificato.

Quando il titolare firma avvalendosi del sistema di firma remota:

- viene identificato in modo certo;
- viene verificata la sua volontà di sottoscrivere il documento;
- viene utilizzato il certificato qualificato associato alla sua identità;
- il documento acquisisce pieno valore legale.

Di conseguenza, considerata la necessità intrinseca di garantire l'autenticità del firmatario, nonché l'esigenza per il titolare della firma di mantenere il controllo esclusivo sulla stessa, la generazione della firma remota è condizionata, oltre al possesso di un certificato di firma qualificata, anche all'attivazione di procedure di "autenticazione forte", idonee ad accertare l'identità dell'utente, a manifestarne in modo inequivocabile la volontà di sottoscrizione e, conseguentemente ad ottenere l'autorizzazione da parte del sistema all'utilizzo del certificato.

Per un approfondimento sul metodo di autenticazione previsto per il sistema di firma remota attualmente in uso dall'ASST Cremona, si rinvia alla procedura operativa pubblicata nella sezione Sistemi Informativi dell'Intranet aziendale.

In Regione Lombardia il sistema di firma remota è integrato nel sistema SISS (Sistema Informativo Socio-Sanitario), le cui credenziali sono il principale strumento di identificazione forte degli operatori sanitari. Per questo motivo, il certificato di firma remota è generato proprio con la configurazione delle credenziali SISS, rilasciate direttamente dalla S.C. Gestione e Sviluppo delle Risorse Umane (ufficio PDA/PDR).
Le credenziali SISS consentono agli operatori sanitari del SSR Lombardo:

- l'identificazione;
- l'autenticazione ai servizi SISS;
- la firma elettronica delle operazioni autorizzate.

Nell'ambito del SISS, oltre ad essere uno strumento di firma digitale di documenti clinici, verbali, prescrizioni e atti amministrativi, il sistema di firma remota, permettendo l'identificazione certa del titolare, si sostanzia anche in un fattore di autenticazione per accedere a piattaforme e servizi telematici regionali che richiedono un elevato livello di sicurezza.

3.4. Protezione delle postazioni di lavoro

In questa sezione vengono trattate le operazioni a carico dell'utente e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.4.1. Operazioni di Login e Logout

Il "Login" è l'operazione con la quale l'utente si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password ed aprendo una sessione di lavoro. In alcuni casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

Ogni utente è autorizzato all'utilizzo unicamente del proprio specifico username e password per accedere a tutti i sistemi ai quali è stato autorizzato. L'ASST, solo in casi eccezionali e specifici, potrà

assegnare un univoco username e password per gruppi di autorizzati all'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa, salvo differenti indicazioni. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Per ragioni di sicurezza, alcune applicazioni prevedono il logout automatico come funzionalità intrinseca, come ad esempio la posta elettronica aziendale, la quale esegue automaticamente il logout dopo otto ore di attività.

Durante le pause di lavoro o in caso di abbandono temporaneo della postazione di lavoro, si raccomanda il "blocco del computer", operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.4.2. Salvaschermo

Per policy aziendale, ogni postazione di lavoro è configurata per attivare un salvaschermo (screen saver) **dopo 10 minuti** di inattività da parte dell'utente, a protezione della confidenzialità ed integrità dei dati trattati. Su specifica richiesta dei Responsabili dei servizi, giustificata da vincoli applicativi/funzionali (ad esempio periferiche di laboratorio), il time-out del salvaschermo può essere oggetto di variazione.

3.4.3. Obblighi dell'utente

L'utilizzo dei dispositivi fisici e la gestione dei dati in essi contenuti devono avvenire nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'utente deve quindi eseguire, anche in osservanza della politica di "schermo pulito", le seguenti operazioni:

- se si allontana dalla propria postazione dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti;
- bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
- salvo diverse indicazioni, chiudere la sessione (Logout) a fine giornata;
- controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo;
- a fine orario di servizio, gli assegnatari di pc portatili e smartphone aziendali sono tenuti a scollegarli dalla rete aziendale e custodirli in luoghi sicuri (armadi o cassettiere sottochiave);
- salvo esplicita autorizzazione dell'ASST, gli assegnatari di pc portatili aziendali possono utilizzarlo solo all'interno del perimetro aziendale (incluse le sedi territoriali), ad eccezione di quanto previsto dal vigente Regolamento Aziendale in tema di lavoro agile e da remoto;
- non lasciare la postazione di lavoro incustodita con file aperti sul desktop.

3.4.4. Utilizzo e gestione del Personal Computer aziendale

Il sistema informativo aziendale è composto da un insieme di sistemi informatici centrali e molteplici personal computer e dispositivi connessi alla rete aziendale che utilizzano diversi sistemi operativi e applicativi.

L'ASST non effettua il backup dei dati salvati in locale favorendone la memorizzazione su file server aziendale dotato di backup giornaliero e che ne consente la condivisione tra utenti. **Non sarà quindi possibile recuperare i files creati, elaborati o modificati sul computer assegnato e salvati localmente in caso di guasto o malfunzionamento del sistema**.

Il computer assegnato all'area di lavoro dove opera l'utente è uno strumento di lavoro e contiene tutti i software utili a svolgere le attività necessarie ed affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso a ciascun Personal Computer è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata.

A fronte di necessità improrogabili d'intervento e manutenzione sulla postazione di lavoro gli amministratori di sistema – sia autonomamente sia su richiesta dell'utente previa apertura ticket – potranno accedere alla stessa dandone contezza al dipendente o al collaboratore anche avvalendosi della sua contestuale collaborazione in fase di risoluzione della problematica.

In particolare, l'utente deve adottare le seguenti misure:
1. utilizzare solo ed esclusivamente spazi di memoria resi disponibili dall'ASST per creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di indebito utilizzo da parte di terzi senza possibilità di accertarne la responsabilità ed estendendo in tal modo l'intera superficie d'attacco della rete aziendale;
3. utilizzare sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), autorizzati dall'ASST;
4. non dare accesso al proprio computer ad altri utenti/terzi, a meno che non siano figure incaricate a seguito di apposita autorizzazione.

3.4.5. Divieti espressi riguardanti l'utilizzo del Personal Computer aziendale

È vietato:
1. gestire, memorizzare (anche temporaneamente) o il trattare di file, documenti e/o informazioni personali dell'utente o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere;
2. modificare le configurazioni già impostate sul personal computer;
3. utilizzare programmi e/o sistemi di criptazione non autorizzati dall'ASST;
4. installare software di cui l'ASST non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'ASST. Non è, peraltro, consentito fare copia del software installato al fine di farne un uso personale;
5. caricare sul disco fisso del computer o nel server documenti, giochi, files musicali o audiovisivi o immagini diversi da quelli necessari allo svolgimento delle mansioni affidate;
6. aggiungere o collegare dispositivi hardware o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB, hard disk, ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'ASST;
7. creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'ASST, quali per esempio virus, trojan horses, malware, spyware ecc.;
8. accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
9. effettuare in proprio attività manutentive e di cambio configurazione hardware;
10. permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'ASST.

3.5. File Server per file sharing e cartelle condivise all'interno dell'Ente

L'infrastruttura ASST dispone di un File Server aziendale sul quale è possibile depositare file in cartelle di rete condivise tra gli utenti che, ancorché operanti presso sedi fisiche diverse, hanno la necessità di condividere documenti e file di varia natura.

Ogni Responsabile stabilisce quali tipologie di documenti prodotti dalla propria struttura siano da salvare sulle cartelle condivise, definendo anche per ciascun utente i privilegi da assegnare allo stesso (sola lettura, scrittura, cancellazione) previa apertura di un ticket all'Help Desk informatico come specificato nella procedura operativa pubblicata nella sezione Sistemi Informativi della Intranet aziendale.

Si specifica che non è consentito l'utilizzo del File Server aziendale per memorizzare risorse/file non pertinenti all'attività lavorativa, ad esempio, a titolo indicativo e non esaustivo contenuti impropri, offensivi, dati sensibili o particolari non protetti da accesso debitamente autorizzato.

3.6. Utilizzo della rete Internet e dell'account di posta elettronica

La connessione alla rete Internet ed il sistema di posta elettronica sono strumenti di comunicazione, informazione e trasmissione; il loro uso è consentito esclusivamente per scopi attinenti allo svolgimento delle mansioni lavorative assegnate.

3.6.1. Internet

La finalità della navigazione internet (web browsing) deve ricondursi al reperimento di informazioni connesse con l'attività lavorativa. Un utilizzo improprio del servizio Internet può avere conseguenze rilevanti per l'etica professionale, danneggiare la reputazione dell'ASST e compromettere la sicurezza dei sistemi informativi aziendali.

Misure preventive per ridurre navigazioni illecite

L'ASST potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

Divieti espressi per la navigazione Internet

1. È bloccata la navigazione nei siti che possono rivelare le opinioni politiche, religiose, sindacali e di salute dell'utente poiché potenzialmente idonea a rivelare dati particolari ai sensi del GDPR.
2. È vietato accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'utente il download di software (anche gratuito) prelevato da siti Internet.
4. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'ASST, salvo specifica autorizzazione dell'Azienda stessa.
5. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
6. È vietato promuovere utile o guadagno personale attraverso l'uso della rete Internet aziendale o della posta elettronica aziendale.
7. È vietato creare siti web personali sui sistemi dell'ASST nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, quandanche effettuata secondo quanto descritto al paragrafo successivo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili, è da considerarsi sempre e comunque di completa personale responsabilità dell'utente inadempiente.

Navigazione Internet non filtrata

L'accesso a siti internet considerati per policy aziendali appartenenti a categorie non pertinenti

all'attività lavorativa - es. categorie improprie, offensive alla morale, di giochi d'azzardo, pericolose in termini di cybersicurezza, ecc… - è bloccato di default dai firewall perimetrali dell'Ente.

Tuttavia, ad alcuni siti bloccati di default è possibile accedere attraverso l'inserimento delle proprie credenziali di dominio, in modo da consentire la navigazione web libera, ma comunque completamente tracciata.

Per una guida sulla navigazione Internet non filtrata, si rinvia alla procedura operativa pubblicata nella sezione "Sistemi Informativi Aziendali – Posta Aziendale e Navigazione Internet" della Intranet aziendale.

3.6.2. Posta Elettronica

La casella di posta elettronica assegnata dall'Azienda è strettamente connessa allo svolgimento dell'attività lavorativa ed è vietato utilizzarla per fini diversi da quelli istituzionali, quali ad es. registrazione a siti e servizi non pertinenti all'attività lavorativa (social network, siti di e-commerce, e-trading etc.).
Si precisa che i dati ed i metadati di posta elettronica sono di proprietà dell'ASST.

La posta elettronica, anche nel caso in cui contenga riferimenti al nome e cognome dell'utente, è uno strumento di esclusiva proprietà di ASST, messo a disposizione di dipendenti e collaboratori a vario titolo al solo fine dello svolgimento delle proprie mansioni lavorative; pertanto, ogni utente assegnatario della casella di posta elettronica è responsabile del corretto utilizzo della stessa. Si chiarisce, pertanto, che non è possibile avanzare richieste di esportazione del proprio database di posta elettronica al momento della cessazione del rapporto di lavoro. (da leggersi con quanto previsto nell'ultimo capoverso del successivo ART. 7 CESSAZIONE DELL'UTILIZZO DEGLI STRUMENTI INFORMATICI DELL'ASST).

Per prassi, **NON è previsto il rilascio automatico di caselle di posta a collaboratori esterni a vario titolo**, quali es. liberi professionisti, consulenti a vario titolo, personale a qualsiasi titolo di imprese fornitrici ai beni o servizi a favore dell'ASST, frequentatori, tirocinanti o studenti presenti in azienda in virtù di convenzione attiva con l'università di appartenenza; ai lavoratori di pubblica utilità, ai volontari, etc.

Ogni Struttura/Servizio aziendale definito dal vigente POAS avrà almeno un indirizzo e-mail identificativo del servizio stesso. Sulla Intranet aziendale nella sezione "Sistemi Informativi Aziendali - Posta Aziendale e Navigazione Internet" è disponibile la documentazione aggiornata sull'utilizzo della piattaforma di posta elettronica in uso.

Gli indirizzi e-mail **condivisi** possono essere di due tipi:

a) ***account con delega***: si tratta di account di posta del formato nomestruttura@asst-cremona.it cui possono accedere in "*sola lettura, lettura/scrittura, invio, invio per conto di*" solo account individuali del medesimo dominio aziendale @asst-cremona.it configurati come ***delegati***.

b) ***lista di distribuzione***: si tratta di un indirizzo e-mail del formato nomestruttura@asst-cremona.it che riceve le mail e le inoltra in automatico ad un elenco di indirizzi e-mail del medesimo dominio aziendale @asst-cremona.it configurati come ***partecipanti***. I messaggi in uscita partono con l'indirizzo di posta nominale di chi prende in carico la richiesta. I membri della lista sono responsabili delle risposte inviate all'esterno secondo le mansioni loro assegnate.

E' il Responsabile della Struttura/Servizio che dovrà chiedere ali Servizi Informativi Aziendali la creazione e denominazione di un account con delega/lista di distribuzione, specificando i nominativi dei delegati/partecipanti (nome, cognome e matricola).

Modalità di utilizzo e buona prassi

L'utente assegnatario è responsabile della propria casella di posta elettronica, in particolare della segretezza delle password nonché del contenuto dei messaggi inviati e, pertanto, è proibito inviare messaggi sconvenienti ed offensivi, inclusi commenti inerenti alla sfera personale dell'individuo.

La posta elettronica aziendale è prefigurata in modo tale da consentire l'impostazione di un messaggio di risposta automatica, configurabile dall'utente. È consigliabile l'utilizzo di tale funzione, che invia in automatico una e-mail di risposta al mittente principalmente nel caso di assenze programmate (es. ferie, congedo, ecc…).

La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente documenti inutili, messaggi pubblicitari, mail non rilevanti e soprattutto allegati ingombranti, limitandone la sua dimensione complessiva.

Le e-mail sono uno dei principali vettori di vulnerabilità ed infezioni dei sistemi informatici (vd c.d. "phishing"); pertanto, un utilizzo attento e scrupoloso della casella di posta elettronica contribuisce in ampia misura alla sicurezza della postazione di lavoro e della rete.

Il servizio di posta elettronica è dotato di un sistema automatico di rilevazione e blocco di messaggi basato su algoritmi di apprendimento automatico che può classificare come sospetti e/o malevoli l'oggetto, il contenuto ed eventuali allegati. In questi casi al destinatario è recapitata una mail di alert a seguito della quale quest'ultimo – qualora ritenesse legittimo il messaggio ricevuto – può richiederne lo sblocco aprendo un ticket all'Help Desk informatico, che con la S.C. Sistemi Informativi Aziendali in ogni caso valuterà l'evasione della richiesta in funzione dell'effettiva potenziale minaccia in termini di cybersicurezza veicolata dal messaggio stesso.

La posta elettronica deve, in ogni caso, essere utilizzata applicando le seguenti accortezze di buona prassi:

- controllare attentamente il dominio di provenienza, (es. gooogle.com) diffidando da quelli sospetti;
- diffidare dalle e-mail inaspettate, anche da mittenti in apparenza conosciuti, e dei relativi allegati;
- diffidare dei collegamenti internet all'interno delle e-mail;
- diffidare di e-mail che invitano a comunicare le credenziali di accesso (nome utente e password) e/o altre informazioni relative a propri dati personali e/o particolari;
- non rispondere ai messaggi di posta elettronica indesiderata (spam);
- inserire nel messaggio la firma aziendale conformemente alle linee guida aggiornate pubblicate sulla Intranet aziendale nella sezione "Kit Brand Aziendale" - "Brand Book ASST Cremona".

In caso di dubbi è consigliabile contattare la S.C. Sistemi Informativi Aziendali per opportune verifiche.

In caso di violazione o inadempimento di quanto riportato al presente paragrafo in merito all'utilizzo della posta elettronica, l'ASST impedirà all'utente la possibilità di collegamento alla casella di posta elettronica assegnata ed accerterà eventuali responsabilità disciplinari, nel caso in caso in cui la violazione sia stata commessa da personale dipendente, o contrattuali se la violazione sia stata posta in essere da professionisti e/o collaboratori.

Per accedere alla posta tramite smartphone (sia proprio sia aziendale) l'unico strumento consentito e certificato è rappresentato dall'utilizzo dell'applicazione relativa al servizio di posta elettronica in uso presso l'ASST e scaricabile gratuitamente dai principali app store associati ai sistemi operativi maggiormente in uso. In questo modo potranno essere garantiti alti livelli di sicurezza dovuti ai continui aggiornamenti resi disponibili dal vendor.

Trasmissione di e-mail contenenti dati particolari

L'invio di referti, relazioni di tipo clinico o documenti contenenti dati particolari con posta elettronica è consentito solo in via residuale, qualora non siano praticabili soluzioni alternative.

In conformità alle indicazioni del Garante per la Protezione dei Dati Personali, qualora non sia possibile procedere all'anonimizzazione dei dati particolari oggetto di trasmissione, l'invio mediante posta elettronica è consentito esclusivamente a condizione che siano adottate cumulativamente tutte le seguenti misure di sicurezza:

a- utilizzo preferenziale della posta elettronica certificata (PEC) per la trasmissione della comunicazione;
b- trasmissione dei dati esclusivamente mediante allegato cifrato, protetto da password o da apposita chiave crittografica;
c- trasmissione della password o della chiave crittografica mediante un canale di comunicazione distinto rispetto a quello utilizzato per l'invio dell'allegato, quale, a titolo esemplificativo, SMS, applicazione di messaggistica o PEC indirizzata a un diverso recapito;
d- assenza di riferimenti a dati personali nell'oggetto e nel corpo della comunicazione, al fine di evitare la divulgazione di informazioni personali non necessarie.

Si evidenzia altresì l'importanza di limitare l'invio di tali dati ad un numero più ristretto possibile di destinatari.

Relativamente alla ricezione, in alcuni casi è possibile che il sistema antispam integrato nel server di posta blocchi messaggi legittimi con allegati protetti da password (es. referti di laboratorio provenienti da altri Enti/domini). Il destinatario dovrà segnalare la necessità di sblocco della consegna aprendo un ticket all'help desk informatico.

Per un approfondimento sulle modalità di cifratura dei documenti, si rinvia all'apposita guida operativa pubblicata nella sezione "Sistemi Informativi – Posta Aziendale e Navigazione Internet" della Intranet aziendale.

Divieti espressi ed utilizzi illeciti di posta elettronica

1. È vietato utilizzare l'indirizzo di posta elettronica aziendale con dominio @asst-cremona.it per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Azienda, nonché utilizzare il dominio dell'ASST per scopi personali.
2. È vietato creare, archiviare o spedire, sia internamente che esternamente al dominio @asst-cremona.it, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non attinenti allo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
3. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.
4. È vietato sollecitare donazioni di beneficenza, propaganda elettorale (al netto delle lecite comunicazioni sindacali) o altre voci non legate all'attività lavorativa.
5. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'ASST informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
6. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
7. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

Qualora l'utente riceva messaggi aventi contenuti vietati, è tenuto a cancellarli immediatamente e a darne comunicazione all'ASST tramite apertura di un ticket all'Help Desk informatico.

Disabilitazione e cancellazione della posta elettronica

La casella di posta elettronica, trascorsi 30 giorni dalla cessazione del rapporto di lavoro, verrà disabilitata. La casella di posta elettronica, trascorsi 4 mesi dalla cessazione definitiva del rapporto di lavoro, verrà cancellata senza possibilità di recupero.
Rimane comunque la possibilità di conservare la casella di posta elettronica per più di 4 mesi su esplicita richiesta della Direzione Strategica.

3.6. Videoconferenze

Le Strutture/Servizi dell'ASST possono fare ricorso a riunioni in modalità telematica intendendo per essa la possibilità che uno o più componenti partecipino alla riunione in luoghi diversi.

La partecipazione in modalità telematica alle riunioni presuppone la disponibilità di una postazione di lavoro o di un dispositivo mobile opportunamente configurato per garantire una buona qualità audio e video. La verifica della configurazione della postazione di lavoro aziendale dovrà essere richiesta con adeguato preavviso al S.C. Sistemi Informativi Aziendali.

I partecipanti alle videoconferenze devono adottare i dovuti accorgimenti affinché eventuali dati personali e/o particolari non siano visti o uditi da terze parti, ovvero evitando l'uso dei sistemi di videoconferenza in luoghi pubblici e/o utilizzando cuffie audio e/o evitando di esporre lo schermo alla visione di terze persone.

3.7. Utilizzo di altri dispositivi

3.7.1. Utilizzo del notebook, tablet o smartphone

Il computer portatile (qualora non già assegnato come postazione di lavoro), il tablet e il cellulare (di seguito generalizzati in "*device* mobile") possono venire concessi in uso dall'ASST agli utenti che, durante gli spostamenti, necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Azienda.

L'Incaricato è responsabile dei *device* mobili assegnatigli dall'ASST e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

La consegna dei device mobili è vincolata alla sottoscrizione da parte del destinatario di uno specifico modulo di assegnazione fornito dalla S.C. Sistemi Informativi Aziendali.
Ai *device* mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i files creati o modificati sui *device* mobili devono essere trasferiti sul file server aziendale al primo rientro in ufficio e cancellati in modo definitivo dai *device* mobili (wiping).

Sui *device* mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'ASST. I *device* mobili utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei *device* mobili deve far seguito la denuncia alle Autorità competenti. Allo scopo si deve avvisare immediatamente l'ASST che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche durante l'orario di lavoro, all'utente non è consentito lasciare incustoditi i *device* mobili.

Laddove il *device* mobile sia accompagnato da un'utenza, l'utente è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requisiti differenti, l'utente è tenuto ad informare tempestivamente e preventivamente l'ASST tramite il proprio responsabile.

In relazione alle utenze mobili, salvo autorizzazione dell'ASST, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'Azienda, gli utilizzi all'esterno devono essere preventivamente comunicati all'ASST per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

3.7.2. Memorie esterne (pendrive usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli utenti può essere assegnata una memoria esterna (quali chiavi USB, hard disk esterni, memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …) previa richiesta autorizzata.

Questi dispositivi devono essere gestiti con le stesse accortezze di cui al precedente paragrafo 3.7.1. e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

Tenuto conto del rischio insito di perdita/furto/distruzione dei dispositivi sopra descritti, l'uso degli stessi deve essere minimizzato e accuratamente valutato.

3.7.3. Restituzione dei *device*

Ogni *device* ed ogni memoria esterna affidati agli autorizzati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'ASST che provvederà a smaltirli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare, l'ASST provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

3.7.4. Device personali

Ai dipendenti e ai collaboratori non è permesso svolgere la loro attività lavorativa usando *device* personali (BYOD – Bring Your Own Device) - quali a titolo indicativo non esaustivo PC fissi, portatili, ecc - né utilizzarli per accedere alla rete aziendale (cablata o wi-fi).

È vietato altresì, salvo esplicita autorizzazione, l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).

Utilizzo di cellulare personale

Durante l'orario di lavoro, comprese le eventuali pause, agli utenti è concesso l'utilizzo del telefono cellulare personale, non eccedendo nella durata e comunque sempre per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

Gli autorizzati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell'ASST solo se espressamente autorizzati dall'Azienda e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

ART. 4 SISTEMI IN CLOUD

4.1. Cloud computing

Con il termine *cloud computing* si indica un insieme di risorse o servizi informatici, come l'archiviazione, l'elaborazione o la gestione di dati tramite sistemi esterni alla rete aziendale, solitamente erogati attraverso Internet.

La frequente esigenza di condividere file di dimensione anche consistente con utenti sia interni sia

esterni all'Azienda può comportare l'esigenza di servizi di *cloud computing* che, tuttavia, può esporre l'ASST a potenziali rischi in termini di sicurezza informatica e protezione dei dati personali, segnatamente, al rischio di esfiltrazione non autorizzata di dati sensibili con potenziale compromissione della loro integrità nonché perdita accidentale di parti di essi.

Al fine di salvaguardare l'Azienda e/o i pazienti presso di Essa in cura e nel pieno rispetto del codice di comportamento del collaboratore, si rende necessario osservare scupolosamente le indicazioni di utilizzo al seguente paragrafo.

4.2. Utilizzo di sistemi Cloud

1. È vietato agli utenti l'utilizzo di sistemi o servizi cloud non espressamente autorizzati dall'ASST. I sistemi cloud autorizzati, infatti, sono dotati dei seguenti requisiti minimi di garanzia:
    a- sono oggetto di apposita **contrattualizzazione da parte dell'Ente**;
    b- sono **certificati e qualificati secondo la normativa e i requisiti previsti da AgID**;
    c- **i fornitori sono nominati Responsabili del trattamento dei dati personali**, ai sensi della normativa vigente, da parte dell'ASST;
    d- **i fornitori comunicano all'ASST,** con cadenza almeno annuale, **i nominativi degli Amministratori di Sistema che operano nell'ambito del servizio cloud;**
    e- **i fornitori garantiscono e l'ASST verifica il rispetto delle indicazioni e delle prescrizioni emanate dal Garante per la Protezione dei Dati Personali** in materia di Amministratori di Sistema e di servizi cloud.
2. Non è ammessa la condivisione di file o dati di qualsiasi altra natura attraverso strumenti di file sharing basati su cloud associati ad account diversi da quello aziendale, ad esempio a mail private personali o create allo scopo.

Per l'elenco degli strumenti cloud autorizzati dall'ASST per la condivisone di file con utenti sia interni sia esterni e le relative modalità di utilizzo si rinvia alla procedura operativa pubblicata sulla sezione "Sistemi Informativi Aziendali – Posta Aziendale e Navigazione Internet" della Intranet aziendale.

ART. 5 PRINCIPALI MINACCE E MISURE DI SICUREZZA

5.1. Classificazione delle principali minacce

Al fine di promuovere un utilizzo consapevole e sicuro delle risorse informatiche aziendali, si richiamano le principali minacce che possono compromettere la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informativi.

Per malware si intendono programmi o codici informatici progettati per arrecare danni ai sistemi, alterarne il funzionamento, sottrarre informazioni o consentire accessi non autorizzati.

Considerata la continua evoluzione delle minacce informatiche, si evidenzia che l'elenco seguente ha carattere esemplificativo e non esaustivo.

- Virus: parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
- Worm: Malware che modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. L'esecuzione è tendenzialmente indotta mediante tecniche di ingegneria sociale o

sfruttando difetti (bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

- Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima.
- CryptoLocker: una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione. CryptoLocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da mittenti legittimi.
- Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un Worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.
- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
- Hijacker: programmi che si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.
- Rootkit: solitamente sono composti da un driver e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.
- Scareware: programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, definiti rogue antivirus, caratterizzati dal fatto di presentarsi come dei veri e propri antivirus, talvolta anche a pagamento.
- Rabbit: programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.
- Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.
- Batch: "virus amatoriali", non sempre pericolosi, ma che possono attivare comandi di formattazione o altri comandi dannosi alla loro esecuzione. Possono presentarsi come dei file exe e spesso gli antivirus non riconoscono la pericolosità dei Batch.
- Keylogger: programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del Keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i Keylogger vengono installati sul computer dai trojan o dai Worm, in altri casi invece il Keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente.
- Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.
- Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC prefissati.
- Zip Bomb: è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a occupare tutto lo spazio su disco rigido.

Oltre ai malware, costituiscono fonti di rischio per il sistema informativo:

- Intercettazioni delle comunicazioni: possono comportare l'accesso non autorizzato alle banche dati per consultazione e copia di dati personali da parte di persone non autorizzate.
- Attacchi alle password: questi attacchi effettuati in varia forma sono dei tentativi per venire a conoscenza e quindi rubare le password degli utenti, di programmi e di accesso a siti Internet.
- Crimini informatici con implicazioni di tipo civile e penale (spamming, tentativi di intrusione, trattamento di testi o immagini proibite, violazione della corrispondenza, scaricamento di software o file non autorizzato o coperti da diritto d'autore, etc.).
- Danni all'hardware: l'elemento più delicato dell'elaboratore, cui danneggiamento può comportare la perdita di tutti i dati.
- Usurpazione di identità: al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione e potrebbe scaricare un software maligno da un sito web che si fa passare per fonte affidabile per cui si potrebbero anche rivelare informazioni riservate alla persona sbagliata.
- IP spoofing: l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
- Spamming: saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio.
- Incidenti ambientali e eventi imprevisti: calamità naturali (tempeste, inondazioni, incendi e terremoti); guasti dell'hardware o del software dei componenti o dei programmi utilizzati; errore umano dell'operatore (compresi i fornitori di servizi) o dell'utente (ad esempio problemi di gestione della rete, installazione errata del software).

La conoscenza di tali minacce e l'adozione di comportamenti prudenti da parte degli utenti costituiscono un elemento fondamentale per la tutela del patrimonio informativo aziendale e per la sicurezza dei dati trattati.

5.2. Le principali misure di sicurezza aziendali

Le contromisure aziendali attualmente in essere per garantire i livelli ragionevoli di cybersicurezza sono i seguenti:

- Antivirus: ogni PDL e server aziendale è dotata di una soluzione centralizzata di end-point-protection con funzionalità di EDR/XDR per la rilevazione e la risposta alle minacce informatiche.
- Firewall perimetrale: funge da filtro per il traffico in transito dall'ASST in base alle regole di sicurezza aziendale impostate e blocca attivamente le minacce rilevate. Il sistema di firewall perimetrale ha una configurazione HA (High A sui cui è abilitato la funzione di IPS
- Antispam: sistema di sicurezza che protegge le comunicazioni via e-mail dalle minacce come spam, phishing e malware, analizzando il contenuto e gli allegati di ogni messaggio. Tale sistema impiega tecnologie avanzate come il machine learning per identificare e bloccare attacchi, inclusi quelli di phishing e ransomware.
- Monitoraggio dispositivi IoT (Internet of Things): sulla rete aziendale sono collegati dispositivi IoT quali elettromedicali, dispositivi medici smart, sensori, sistemi avanzati di monitoraggio, ecc…che spesso utilizzano protocolli di sicurezza deboli. Sulla rete aziendale è presente una sistema che monitora tali dispositivi IoT segnalandone le potenziali vulnerabilità e attuando politiche di *remediation*.
- SIEM/SOC: sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) che ha lo scopo di raccolta, aggregazione e analisi di grandi volumi di dati da applicazioni, dispositivi, server, PDL e utenti in tempo reale per fornire una visione completa della sicurezza aziendale

permettendo al centro operativo di sicurezza (SOC) di rilevare, indagare e rispondere rapidamente ed efficacemente agli incidenti di sicurezza.

ART. 6 SEGNALAZIONE ANOMALIE E MALFUNZIONAMENTI

L'utente che dovesse riscontrare anomalie o malfunzionamenti dei sistemi informatici – quali ad esempio: calo notevole delle prestazioni della propria postazione, frequenti messaggi di errore, comparsa di una nuova home page e/o di un nuovo motore di ricerca predefinito nel proprio browser di navigazione – deve prontamente segnalarlo all'Help Desk informatico mediante apertura di apposito ticket.

La gestione delle anomalie e dei malfunzionamenti ha l'obiettivo di risolvere il più velocemente ed efficacemente possibile un evento che impatta, più o meno gravemente, sulla sicurezza, riservatezza, disponibilità e integrità dei dati e sul regolare funzionamento del sistema informatico aziendale.

In caso di violazione dei dati personali (Data Breach), presunta o effettiva, ossia una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati si applica l'apposita procedura operativa pubblicata sulla Intranet aziendale.

ART. 7 CESSAZIONE DELL'UTILIZZO DEGLI STRUMENTI INFORMATICI DELL'ASST

Qualora intervenga la cessazione del rapporto di lavoro/ di collaborazione a qualsiasi titolo, il Responsabile della Struttura/Servizio del soggetto cessato deve:
- provvedere, se possibile, in tempo utile, al passaggio di consegne necessario per la corretta futura gestione dell'ufficio (documentazione, progetti, materiali di lavoro);
- verificare, in collaborazione con l'interessato, che eventuali documenti salvati nel computer assegnato all'utente siano memorizzati nella cartella di rete condivisa dell'ufficio presente sul file server aziendale;
- invitare l'interessato a cancellare eventuali file personali.

La S.C. Sistemi Informativi Aziendali, ricevuta comunicazione della cessazione del rapporto di lavoro da parte dei soggetti indicati all'art. 3, provvede a disabilitare gli accessi dell'utente ai diversi sistemi, quali:
- postazione di lavoro
- applicativi aziendali
- posta elettronica.

I dati presenti sulla postazione di lavoro, di norma, saranno cancellati alla cessazione del rapporto di lavoro.

La casella di posta elettronica, trascorsi **4 mesi** dalla cessazione del rapporto di lavoro, verrà cancellata senza possibilità di recupero.
Rimane comunque la possibilità di conservare la casella di posta elettronica per più di 4 mesi su esplicita richiesta della Direzione Strategica.

Su specifica autorizzazione della Direzione dell'Ente il dipendente o collaboratore cessato potrà richiedere alla S.C. Sistemi Informativi Aziendali copia del contenuto della casella di posta

elettronica su supporto digitale messo a disposizione dal medesimo dipendente o collaboratore cessato senza oneri per l'Ente stesso.

ART. 8 CONTROLLI E SANZIONI

I controlli sull'uso delle risorse informatiche aziendali saranno effettuati con strumenti automatici e su dati aggregati, facenti riferimento all'intera Struttura/Servizio.

Il controllo anonimo potrà concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso sarà circoscritto a dipendenti o collaboratori afferenti all'intera Struttura/Servizio in cui è stata rilevata l'anomalia.

Rimane in capo anche ai Responsabili della Strutture/Servizi la funzione di controllo degli utenti e dell'uso degli strumenti informatici aziendali.

La violazione delle norme contenute nel presente regolamento potrà dar luogo a responsabilità penale, civile, amministrativo-contabile e disciplinare.

ART. 9 NOTE FINALI

Il presente regolamento aziendali si intende dinamico, vale a dire che è soggetto a revisione e aggiornamento periodico in rapporto a nuove disposizioni e raccomandazioni internazionali / nazionali nonché a suggerimenti degli operatori dell'ASST. Referenti aziendali per il presente documento organizzativo e per gli eventuali aggiornamenti sono la S.C. Sistemi Informativi Aziendali e la S.C. Affari Generali e Legali.

ART. 10 ENTRATA IN VIGORE, PUBBLICITÀ E VALIDITÀ

Il presente Regolamento entra in vigore dalla data di adozione del decreto aziendale di approvazione, è pubblicato in "Amministrazione Trasparente – Disposizioni generali – Atti generali – Atti amministrativi generali – Regolamenti aziendali" e nella Intranet aziendale ed ha validità a tempo indeterminato, salvo incorra la necessità di apportare variazioni e/o integrazioni o di emettere procedure sostitutive.