REGIONE PIEMONTE

AZIENDA SANITARIA LOCALE DI BIELLA

SEDE LEGALE
Via dei Ponderanesi n. 2 – 13875 Ponderano (BI)
P.IVA 01810260024

DELIBERAZIONE DEL DIRETTORE GENERALE

IL DIRETTORE GENERALE

Dr. Mario Sano'

(nominato con D.G.R. n. 18 - 3300 del 28 Maggio 2021)

L'anno 2022, il giorno 12 del mese di Luglio, presso l'Azienda Sanitaria Locale BI con sede legale in Ponderano (BI) - Via dei Ponderanesi n. 2

ha assunto la seguente deliberazione:

Deliberazione n. 319 del 12/07/2022

OGGETTO: APPROVAZIONE NUOVO REGOLAMENTO AZIENDALE RELATIVO ALL'USO DEL SISTEMA ICT E DELLA POSTA ELETTRONICA DELL'ASL BI

REGIONE PIEMONTE

AZIENDA SANITARIA LOCALE DI BIELLA

Deliberazione n. 319 del 12/07/2022

SEDE LEGALE
Via dei Ponderanesi n. 2 – 13875 Ponderano (BI)
P.IVA 01810260024

OGGETTO: APPROVAZIONE NUOVO REGOLAMENTO AZIENDALE RELATIVO ALL'USO DEL SISTEMA ICT E DELLA POSTA ELETTRONICA DELL'ASL BI

IL DIRETTORE GENERALE

Su proposta n. 257 della SS AFFARI ISTITUZIONALI E LEGALI:

PREMESSO:

- che Il Regolamento (UE) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (General Data Protection Regulation o GDPR), attribuisce al titolare del trattamento il potere di adottare le misure che ritiene più idonee ed opportune per garantire la protezione dati personali;
- che il "Sistema Privacy" delineato dal GDPR implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrate dell'intero *asset* organizzativo;
- che con Deliberazione n. 149 del 03/04/2020 ad oggetto: "Approvazione nuovo regolamento aziendale relativo all'uso del Sistema ICT e della posta elettronica dell'ASL BI" è stato approvato il regolamento vigente oggetto di revisione;
- che in data 10.05.2022 il Direttore della SC Amministrazione e Controllo, Dr.ssa Elvira Zampese ha trasmesso il testo del Regolamento revisionato per l'approvazione;
- che in data 31.05.2022 si è provveduto a trasmettere il suddetto Regolamento al Referente Privacy e al Direttore della SC Personale per gli adempimenti di competenza;
- che le Organizzazioni Sindacali del Comparto e della Dirigenza Medica, Sanitaria non Medica, Amministrativa e Professionale, debitamente informate con e-mail in data 31.05.2022, non hanno formulato alcuna osservazione o richiesta sul Regolamento in oggetto;
- che con nota e-mail del 28.06.2022 il Direttore della SC Amministrazione e Controllo, Dr.ssa Elvira ZAMPESE ha ritrasmesso il Regolamento aggiornato, recepite le osservazioni pervenute da parte del DPO (*Slalom Consulting srl*), richieste dal Referente Privacy dell'ASL BI;

RITENUTO pertanto di approvare per i motivi sopra esposti il nuovo regolamento che si allega a formare parte integrante del presente provvedimento;

CONSIDERATO che il presente provvedimento non comporta oneri aggiuntivi a carico del Bilancio Aziendale;

PRESO ATTO dei pareri conformi del Direttore Amministrativo, Dr. Paolo GARAVANA e del Direttore Sanitario, Dr. Claudio Camillo SASSO, ai sensi del D.Lg.vo n. 502/1992 e successive modificazioni ed integrazioni;

Deliberazione n. 319 del 12/07/2022

SEDE LEGALE
Via dei Ponderanesi n. 2 – 13875 Ponderano (BI)
P.IVA 01810260024

D E L I B E R A:

1) di approvare il Nuovo Regolamento relativo all'uso dei sistemi ICT e della posta elettronica dell'ASL BI, che si allega in parte integrante al presente atto deliberativo;
2) di dare atto che dal presente provvedimento non derivano oneri aggiuntivi a carico del Bilancio Aziendale;
3) di dare mandato alla Struttura Affari Generali, Legali e Istituzionali di trasmettere copia della presente deliberazione alla Struttura Amministrazione e Controllo per gli adempimenti consequenziali e all'Ufficio Comunicazione e URP per la pubblicazione del Regolamento sul sito aziendale.

REGIONE PIEMONTE

AZIENDA SANITARIA LOCALE DI BIELLA

SEDE LEGALE
Via dei Ponderanesi n. 2 – 13875 Ponderano (BI)
P.IVA 01810260024

DELIBERAZIONE DEL DIRETTORE GENERALE

Deliberazione n. 319 del 12/07/2022

Per approvazione

IL DIRETTORE GENERALE

Dr. Mario Sano'

Regolamento Aziendale uso sistema ICT e posta elettronica

Revisione	Data	Paragr.	Descrizione della revisione	Elaborato
Rev.0	27/06/2022	19	Prima emissione	27/06/2022

Indice

I. INTRODUZIONE

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete Internet dai Personal Computer, espone l'ASL di Biella e gli utenti interessati (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa. In questo senso viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare, conseguentemente, eventuali usi scorretti.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'ASL di Biella ha adottato una policy interna diretta ad evitare che determinati comportamenti possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. I controlli sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione - essendo le dotazioni oggetto della presente policy strumenti di lavoro la cui utilizzazione personale è preclusa - quanto il diritto del lavoratore a non vedere invasa la propria sfera personale ed il conseguente diritto alla riservatezza ed alla dignità, così come sanciti dallo Statuto dei Lavoratori, dal d.lgs. 196/03 integrato con il D. Lgs. 10 agosto 2018, n. 101 e dal Regolamento UE 2016/679.

Questo regolamento viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dalle Linee Guida del Garante della Privacy per Posta Elettronica ed Internet – Del. dd. 01/03/2007 e della legislazione cogente in materia di responsabilità amministrativa delle persone giuridiche (D.lgs. 231/01 e s.m.i.) e fornendo informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Allo scopo di rappresentare agli utenti il quadro normativo di riferimento si specifica che le principali fonti normative in materia sono le seguenti:

- Decreto Legislativo n.196 del 30 giugno 2003;
- D. Lgs. 10 agosto 2018, n. 101;
- Regolamento EU 216/679;

II. SCOPO E CAMPO DI APPLICAZIONE

1. Generalità

Il documento è redatto in conformità ai principi di cui all'art. 4 della Legge n. 300/1970 e s.m.i., nonché in applicazione della Deliberazione Garante "Linee Guida per posta elettronica e internet" del 10 marzo 2007.

I rapporti tra l'Ente e l'utenza si ispirano a principi di trasparenza e leale collaborazione.

2. Applicazione

La presente Policy si applica a:

- tutti gli Utenti che utilizzano le risorse informatiche dell'Azienda, siano essi dipendenti a tempo pieno o parziale, collaboratori, consulenti, tirocinanti, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri individui a cui ne è concesso l'uso;
- tutte le operazioni di accesso a informazioni registrate ed archiviate elettronicamente tramite risorse informatiche aziendali;
- tutte le forme di comunicazione operate attraverso Internet e la posta elettronica.
- Provvedimento del "Garante della Privacy" n. 13 del 01/03/2007 (di seguito "Provvedimento".

L'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l'incaricato e per l'azienda per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

Si ricorda inoltre che talune attività come ad esempio la produzione e duplicazione di materiale pornografico e pedopornografico, oltre a provocare azioni disciplinari da parte dell'Azienda, comportano responsabilità penale per la persona che compie questa attività.

Si ricorda infine che eventuali violazioni delle procedure di accesso e sicurezza dei sistemi informativi, di cui ciascun utente dovesse venire a conoscenza nell'ambito dell'attività lavorativa, devono essere prontamente segnalate al Settore Informatico dell'Azienda.

III. RIFERIMENTI

1. Riferimenti normativi e bibliografici

- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali". -

- Legge 04 aprile 2012 n.35 "Conversione in legge, con modificazioni, del decreto legge 9 febbraio 2012, n. 5, recante disposizioni urgenti in materia di semplificazione e di sviluppo".

- Provvedimento del Garante: "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009" G.U. n. 149 del 30 giugno 2009.

- Linee Guida del Garante: "Lavoro: le linee guida del Garante per posta elettronica e Internet" - G.U. n. 58 del 10 marzo 2007.

- Provvedimento del Garante: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" - G.U. n. 300 del 24 dicembre 2008.

- Legge 20 maggio 1970 n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento".

- Decreto Legislativo 29 dicembre 1992 n.518 "Attuazione della Direttiva n. 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore".

- Legge 18 agosto 2000 n. 248 "Nuove norme di tutela del diritto d'autore" - Decreto del Presidente della Repubblica 16 aprile 2013 n.62 "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165"

IV. TERMINI E DEFINIZIONI

1. Terminologie

"autenticazione informatica": l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"banca di dati": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

"comunicazione": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal Rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"comunicazione elettronica": qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica;

"credenziali di autenticazione": le informazioni e/o i dispositivi, in possesso di una persona, solo da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

"dati anonimi": i dati che in origine, o a seguito di trattamento, non possono essere associati ad un Interessato identificato o identificabile;

"Dati Giudiziari": Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

"Dati Particolari": Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

"dati identificativi": i dati personali che permettono l'identificazione diretta dell'Interessato;

"dati personali": qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

"diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
"Garante": l'autorità di cui all'art. 51- del Regolamento Europeo 679/2016;

"Addetti al Trattamento/Incaricati": le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;

"Interessato': la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

"oscuramento": rendere non visibile l'evento clinico revocabile nel tempo ovvero con modalità tali da garantire che tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta (oscuramento dell'oscuramento);

"parola chiave/password": componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

“Policy”: documento che riporta obiettivi ed indirizzi generali, relativi alle principali funzioni ed attività assistenziali e gestionali;

"profilo di autorizzazione": insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

"Responsabile": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;

“Responsabile del Sistema Informatico aziendale”: il Responsabile della sicurezza e della gestione delle Risorse informatiche aziendali;

"rete di comunicazione elettronica": i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, wireless, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportata;

“risorse informatiche aziendali”: qualsiasi combinazione di apparati tecnologici dell'Azienda, hardware o software, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati;

"scopi statistici": le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informatici statistici;

“screensaver”: salvaschermo ovvero applicazione per computer che provoca l'oscuramento dello schermo o la comparsa di un'animazione o di una serie di immagini in successione sullo stesso dopo un periodo programmato di inattività del mouse e della tastiera (non dell'elaboratore in sé), impostabile attraverso un timer;

“server di rete”: è un Personal Computer dedicato a cui competono funzioni di "computer centrale" in una rete locale di Personal Computer;

"servizi informatici aziendali": l'insieme delle apparecchiature e delle risorse (ivi compresi i programmi per elaboratore, i dispositivi elettromedicali e gli apparati per l'accesso alla rete di comunicazione elettronica Internet) che consentono all'Utente di accedere, visualizzare, modificare, e compiere ogni altra operazione su dati a qualunque titolo memorizzati nei dispositivi informatici aziendali, o da questi accessibili, nonché gli eventuali servizi ausiliari al loro funzionamento;

"sistema di autorizzazione": l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

“situazione d'emergenza”: circostanza nella quale, il venir meno di un'azione, può provocare un serio pregiudizio a persone o cose, comportare il danneggiamento o la perdita di dati o impedire la verifica di una grave responsabilità dell’Azienda o degli Utenti della stessa;

“spyware”: sono programmi concepiti per raccogliere informazioni relative al PC e al suo possessore ed inviare il tutto via Internet al loro ideatore. La tipologia di informazioni sottratte può includere ma non essere limitata a: siti visitati, corredati di permanenza e file scaricati, siti Preferiti, contenuto della Cache e/o Cronologia del browser, configurazione hardware e software del PC, e molto altro. Il più delle volte lo scopo della sottrazione di informazioni è quello del marketing, ma potrebbe anche essere più dannoso.

"strumenti elettronici": gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"Titolare": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, la decisione in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo delta sicurezza;

"Responsabile": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

"trattamento": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

"trojan horse": cavallo di troia, un programma apparentemente utile che nasconde le sue funzionalità; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto. Spesso i trojan sono usati come veicolo alternativo ai worm e ai virus;

"username": il nome (identificativo) con il quale l'Utente viene riconosciuto da un computer, da un programma o da un server;

"Utente": ciascuna persona che acceda alle Risorse informatiche aziendali;

"web": l'abbreviazione di World Wide Web, è un servizio di Internet che permette di navigare ed usufruire di un insieme vastissimo di contenuti collegati tra loro attraverso legami (link); *"webfiltering":* un filtro web è un programma in grado di schermare una pagina Web in ingresso per determinare se alcuni o tutti vi accedono. Il filtro controlla l'origine o il contenuto di una pagina Web in base a una serie di regole fornite da società o persona che ha installato il filtro web ed inoltre, consente di bloccare le pagine di siti web che possono includere pubblicità discutibile, contenuti pornografici, spyware, virus ecc..., e altri contenuti discutibili;

"web security": consiste nel monitoraggio di tutte le informazioni sul traffico Internet;

"worm": sono programmi realizzati per riprodursi da un computer all'altro ma, a differenza dei virus, questa operazione avviene automaticamente. Per prima cosa i worm assumo il controllo delle funzioni del computer destinate al trasporto dei file o delle informazioni. Una volta presente nel sistema, il worm è in grado di viaggiare autonomamente.

2. Abbreviazioni

*BIOS: (*Basic Input-Output System) è un insieme di routine software, che fornisce una serie di funzioni di base per l'accesso all'hardware e alle periferiche integrate;

PEO: Posta Elettronica Ordinaria. La PEO può essere "*ad personam*", associata ad una AOO, associata ad un ufficio, associata ad una specifica funzione/progetto o servizio.

PEC: Posta Elettronica Certificata;

IP: Internet Protocol è un'etichetta numerica che identifica univocamente un dispositivo collegato a una rete informatica (protocollo di comunicazione). Un indirizzo IP assolve due funzioni principali: identificare un dispositivo sulla rete e di conseguenza fornirne il percorso per la sua raggiungibilità da un altro terminale o dispositivo di rete. Può essere statico o dinamico;

LAN: Local Area Network: è un gruppo di computer connessi in un'area locale per comunicare tra loro e condividere risorse quali le stampanti, ecc...;

NAS: Nucleo Anti Sofisticazioni e Sanità dei Carabinieri;

PDA: (Personal Digital Assistant) termine usato per definire personal computer portatili. Simile ai personal computer palmari si differenzia da questi perché non utilizza una tastiera per impartire i comandi ma una sorta di penna che interagire attraverso il display.

VNC: Virtual Network Computing: è un sistema di visualizzazione remota che permette di ottenere un ambiente 'desktop' non solo sulla macchina personale ma ovunque;

VPN: Virtual Private Network: è una rete che permette a computer ubicati in sedi fisiche diverse di stabilire un collegamento.

V. SISTEMA DI GESTIONE PRIVACY

Considerato che l'ASL di Biella (nel seguito per brevità "Ente"), nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori, apparecchiature informatiche e mezzi di comunicazione (Personal Computer, Notebook, Tablet, accesso alla rete aziendale, accesso alle procedure aziendali, casella di posta elettronica, accesso alla rete Internet, etc.), la presente Policy fornisce le regole che ciascuno deve osservare.
Il presente documento ha pertanto l'obiettivo di regolamentare l'utilizzo dei sistemi informatici, di internet e della posta elettronica per gli utenti dell'Ente e di informare i dipendenti sul trattamento dei dati connesso all'attività di verifica e controllo.
Il regolamento persegue, inoltre, la finalità di garantire la sicurezza e prevenire il danneggiamento delle risorse informatiche aziendali.

VI. RESPONSABILITÀ E AUTORITÀ

Le responsabilità e le autorità del processo di tenuta sotto controllo dello stato di applicazione del presente regolamento sono descritte, per ogni risorsa coinvolta nel processo, nel paragrafo VII.

VII. RISORSE COINVOLTE NEL PROCESSO

1. Responsabilità generale

La responsabilità generale per garantire la corretta applicazione del Regolamento spetta al Gruppo di lavoro privacy aziendale, con la collaborazione del Responsabile dei Sistemi Informativi.

Le presenti istruzioni si applicano:

- a tutto il personale dipendente ed al personale autorizzato (ivi compresi consulenti, convenzionati, aziende esterne legate da contratti di fornitura e/o servizi o altri individui in possesso di specifiche credenziali di autenticazione alle quali è consentito l'accesso alle risorse aziendali), senza distinzione di ruolo e/o livello che si trovano ad operare sui dati di cui l'ASL di Biella è Titolare (di seguito "utenti");
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

2. Utilizzatori

L'utilizzo delle risorse informatiche aziendali e delle banche dati, è riservato ai dipendenti dell'Ente e ad altri soggetti espressamente autorizzati dal Titolare.

VIII. DESCRIZIONE DEL PROCESSO

1. Utilizzi consentiti

Le risorse informatiche aziendali sono strumenti di lavoro e, come tali, possono essere utilizzate solo per scopi strettamente professionali e lavorativi compresi quelli di ricerca e di didattica. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, ecc.), sia per quelle affidate al singolo Utente (Personal Computer fisso o portatile e relativi programmi e/o applicazioni, periferiche, stampanti locali, etc.).

Le risorse informatiche affidate al singolo Utente sono strumenti di lavoro appartenenti al patrimonio aziendale e, pertanto, devono essere custodite in modo appropriato. Il verificarsi di alcune azioni quali il furto, il danneggiamento, lo smarrimento, etc. deve essere prontamente segnalato alle Forze dell'Ordine ed alla Direzione Aziendale.

Il personale interessato dalle disposizioni del presente Regolamento, è tenuto a contattare il Servizio Informativo Aziendale (ove presente) prima di intraprendere qualsiasi attività tecnica non esplicitamente compresa nel presente Regolamento, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

I dati particolari non possono essere salvati sui supporti di memorizzazione locali dei computer a meno di adeguati sistemi di protezione (crittografia, etc).

2. Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete vengono predisposte dagli amministratori del Servizio Informativo Aziendale all'atto dell'assunzione del nuovo dipendente.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente "User Id", associato ad una parola chiave "password" personale e riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata.

Per quanto concerne gli applicativi gestionali, saranno fornite a ciascun lavoratore, delle credenziali con diversi profili di gestione.

Il Titolare è tenuto ad organizzare e conservare un registro delle credenziali richieste per i propri collaboratori; in tal modo, in caso di sopraggiunta necessità, potrà essere correttamente istanziata la richiesta di disabilitazione degli accessi agli applicativi.

In caso di estinzione del rapporto contrattuale con il Personale Autorizzato al Trattamento (Addetto), si provvederà ad inibire l'accesso alle postazioni entro tre giorni lavorativi dal ricevimento della comunicazione.

Qualora, per motivate ragioni di efficienza ed efficacia, un incaricato venga abilitato all'utilizzo della propria postazione con il ruolo di amministratore locale, è comunque tenuto a rispettare il presente regolamento (a titolo puramente esemplificativo e non esaustivo, si ribadisce che è assolutamente vietata l'installazione di qualsiasi tipologia di applicazione senza preventiva formale autorizzazione del Servizio Informativo Aziendale).

3. Utilizzo del personal computer

Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione, come meglio descritto nella sezione "GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE" della presente Policy.

Il PC dato in affidamento all'utente permette l'accesso, alla rete dell'Ente ed alla rete esterna, solo attraverso apposita configurazione e necessita di specifiche credenziali di autenticazione.

L'Ente rende noto che il personale incaricato operante presso l'U.O. Servizio Informativo Aziendale è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento dell'utente e non sia possibile procedere altrimenti.

Il personale incaricato ha la facoltà di collegarsi e visualizzare da remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. A tale scopo, saranno installati sui PC client appositi software (agent), normalmente in commercio, per la rilevazione automatica della configurazione hardware e software, che tenga traccia delle modifiche effettuate e della versione dei software installati.

L'intervento è effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, sarà data comunicazione della necessità dell'intervento stesso.

Le postazioni di lavoro sono predisposte e configurate per le esigenze dell'utente finale. Ai fini della manutenzione del sistema, su tutte le postazioni di lavoro è creata un'utenza amministrativa la cui password potrà essere modificata dal servizio informativo ogni qual volta si renda necessario. L'utente del PC si impegna a mantenere la corretta configurazione della stazione di lavoro che utilizza e a non modificare o cancellare il profilo amministrativo di cui al precedente paragrafo; non è consentito pertanto all'utente variare le caratteristiche impostate sul proprio PC né procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (es. masterizzatori, modem, etc.) senza il preventivo consenso.

Non è consentita l'attivazione in autonomia della password di accensione (BIOS), senza preventiva autorizzazione da parte del Titolare e/o Servizio Informativo Aziendale.

L'accesso alle postazioni di lavoro è subordinato all'inserimento delle credenziali assegnate (di dominio) ad uso individuale delle singole utenze.

Ai fini della conservazione dei beni, di prevenire possibili problemi di sicurezza fisica e logica e di permettere l'integrazione di alcune policy aziendali, il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o di suo inutilizzo. L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un elaboratore incustodito e connesso alla rete può essere

causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Si raccomanda pertanto di bloccare la postazione prima di allontanarsi dalla stessa.

4. Utilizzo dei laptop (personal computer portatili)

L'utente utilizzatore è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.

Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in rete. Particolare attenzione è rivolta nel caso di un utilizzo temporaneo del PC portatile assegnato, per ciò che attiene alla rimozione da parte dell'utente utilizzatore di eventuali file elaborati ed utilizzati, prima della riconsegna dello stesso al servizio a cui è assegnato.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Tutti i laptop devono collegarsi periodicamente (con frequenza almeno mensile) alla rete interna per consentire l'aggiornamento dell'antivirus e del sistema operativo.

5. Utilizzo di stampanti, multifunzioni e fax-server

È vietato l'utilizzo delle stampanti, delle fotocopiatrici (MF) e dei Fax aziendali per fini personali, salvo preventiva, eccezionale ed esplicita autorizzazione da parte del Titolare.

Si raccomanda agli utenti di prestare la massima attenzione nella stampa, soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone. Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.

La stampa di documenti informatici dovrà essere limitata all'attività lavorativa e in ogni caso per documenti per cui esiste l'assoluta necessità di disporre della copia cartacea. In particolare per motivi di economicità per quanto riferito alle stampe a colori.

Nell'utilizzare il Fax occorre prestare attenzione, in particolare, all'ipotesi in cui vengano inviati documenti contenenti dati particolari: digitare correttamente il numero di telefono, controllare l'esattezza del numero di telefono digitato prima di premere il tasto "invio", verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli, attendere la stampa del rapporto di trasmissione e verificare la corrispondenza del numero di pagine da inviare con quelle effettivamente inviate.

Nell'utilizzare il Fax in ricezione e/o stampanti poste al di fuori della propria postazione lavorativa è opportuno presidiare la postazione in maniera da assicurare una tempestiva acquisizione dei documenti al fine di evitare l'accesso di persone non autorizzate.

Nelle stampanti multifunzione (MF), la scansione dei documenti potrebbe venir configurata come "scan-to-mail" e/o "scan-to-disk".

Lo "scan-to-mail" consiste nell'invio del documento digitalizzato ad una casella di posta. Nell'utilizzo dello "scan-to-mail" è proibito l'invio di scansioni dalla multifunzione verso e-mail non aziendali. Qualora si desideri inviare una scansione a un soggetto terzo afferente all'Ente, è necessario dapprima inoltrare il documento alla propria e-mail personale – per verificarne il

contenuto - e solo successivamente, utilizzando la mail, inoltrare l'allegato al destinatario. Nel caso di invio di allegati pesanti è opportuno, dopo aver salvato la scansione, cancellare la mail dalla posta in arrivo e, successivamente, dal cestino.

La modalità "scan-to-disk" consiste nel salvataggio delle scansioni su una cartella locale della multifunzione o su cartella di rete. In tal caso, l'utente ha l'onere di spostare il file in una cartella non consultabile da soggetti non autorizzati alla visione del documento.

La modalità "scan-to-disk" potrebbe indirizzare i documenti acquisiti nella memoria interna del dispositivo, oppure in una share di rete. In entrambi i casi previsti per la modalità "scan to disk", al fine di preservare lo storage ed evitare il blocco del dispositivo per insufficienza di spazio, potrebbero essere impostate delle policy che eliminano i documenti più vecchi di 24h. In seguito all'eliminazione non sarà possibile procedere al recupero degli stessi, è pertanto consigliato il recupero immediato dei documenti scansionati e l'eliminazione degli stessi dalle aree condivise. La cancellazione periodica non dispensa tuttavia l'utente dall'obbligo di cancellare/spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile (al fine di non rendere accidentalmente noto a terzi il contenuto dei file scansione).

Si raccomanda di porre la massima attenzione nella scansione di documenti contenenti dati personali particolari.

6. Hardware e software

Tutto l'hardware e il software potrà essere acquistato solo previa autorizzazione del Titolare che controllerà le richieste al fine di valutarne la compatibilità con i sistemi in uso e con l'infrastruttura di rete.

È fatto assoluto divieto all'utente di intervenire in qualunque modo sull'hardware in dotazione. In caso di malfunzionamento delle apparecchiature assegnate, l'utente si impegna a darne tempestiva segnalazione al Titolare.

Come meglio specificato nella sezione "UTILIZZO DELLA RETE FISICA (LAN)", non è consentito l'utilizzo di hardware di tipo personale salvo specifica autorizzazione del Servizio Informativo Aziendale.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal Titolare, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti. Nuove necessità andranno pertanto presentate al Titolare (valutazione di compatibilità) ed eventuale seguente installazione. A tal fine le richieste di acquisto dell'hardware e del software dovranno essere indirizzate al Titolare. Il nuovo software acquisito dovrà venire registrato a nome dell'azienda.

È vietato provare ad installare arbitrariamente il software scaricato da Internet o contenuto nei vari supporti distribuiti con le riviste, con i libri e con i quotidiani anche se si tratta di software allegato a riviste del settore. Prima di installare questi programmi, qualora l'uso fosse legato ad esigenze lavorative, sarà necessario il benestare del Titolare.

È assolutamente vietato installare, anche solo temporaneamente, programmi ottenuti o sbloccati illegalmente (programmi "crackati", codici di sblocco ottenuti da internet, etc.). Un programma "crackato", oltre a costituire una violazione alle norme che regolano il Diritto d'Autore, costituisce anche un'autentica minaccia alla sicurezza della rete ed all'affidabilità del sistema di elaborazione su cui viene installato. Lo sblocco del programma ("crack") viene

effettuato modificando i codici originali del programma per aggirare le protezioni. Questo implica sostituire pezzi del programma originale con parti modificate e queste nuove aggiunte, oltre ad aggirare le protezioni, possono anche introdurre codice dannoso.

Non è consentita la disinstallazione dei programmi, sia software di base che software applicativi. I suddetti interventi sono effettuati, in caso di necessità, solo a cura dei tecnici del titolare funzionalmente alla segnalazione dell'utente.

Non è consentita l'installazione, anche se necessaria, di eventuali driver per stampanti o altri supporti come ad esempio masterizzatori, scanner, etc.; in questo caso l'utente dovrà richiedere ai tecnici del Titolare di intervenire per effettuare l'installazione.

È facoltà del Titolare, bloccare automaticamente il download di files potenzialmente infetti da siti non istituzionali o non affidabili. Nel caso in cui sia necessario "scaricare" ulteriori files, anche gratuiti, dalla rete, l'utente dovrà formulare una richiesta preventivamente autorizzata dal Titolare, che provvederà ad autorizzare il download ovvero ad effettuare direttamente l'installazione del programma.

L'utente è responsabile del corretto utilizzo del software installato sulla propria postazione - sia software di base che software applicativo di vario genere. Se ne raccomanda, pertanto, un uso diligente e consapevole.

Al fine di proteggere l'integrità dell'Ente, il personale non può utilizzare software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

Non è consentita l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro - per quanto attinente ai supporti removibili consultare la sezione “UTILIZZO E CONSERVAZIONE DEI SUPPORTI REMOVIBILI”.

Il Titolare si riserva la facoltà di bloccare in qualsiasi momento le interfacce USB delle stazioni di lavoro per impedire la possibilità di utilizzo di supporti di massa esterni (principale ingresso di codice malevole).

Non sono consentiti sia l'installazione sia l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o di documenti informatici.

In senso generale tutti i dati personali in possesso dell’ASL Biella in qualità di Titolare del trattamento, compresi i dati particolari, non possono essere spostati o salvati su supporti esterni quali dischi o penne USB o tramite siti internet che offrono servizi di trasferimento su sistemi cloud esterni (Es. We Transfer, Drop box, Azure, Google Drive, One Drive, etc). Mentre è ovviamente possibile fare uso dei servizi cloud messi a disposizione dall’Ente (es. google Workspace aziendale, Netapp,ecc.) verificando con attenzione che le eventuali condivisioni siano rivolte ai soli destinatari aziendali autorizzati.

Il Titolare esegue automaticamente regolari scansioni sui sistemi installati al fine di rilevare la presenza di software non autorizzato. L’identificazione di eventuali software non autorizzati comporterà un ticket per la rimozione degli stessi e la segnalazione alla direzione aziendale per i derivanti provvedimenti.

7. Aggiornamento del sistema operativo e del software

Gli aggiornamenti del sistema operativo sono necessari, oltre che essere un obbligo di legge, al fine di proteggere il PC e l'intera rete. È stato implementato il Sistema WSUS che effettua il download degli aggiornamenti stabiliti in maniera automatizzata.

Tutte le postazioni sono connesse a tale istanza che - legata in modo diretto con il produttore distribuisce prontamente eventuali aggiornamenti di pattern, antivirus e antispyware. Nelle postazioni eventualmente off-line tali aggiornamenti vengono installati non appena si ripresenteranno in linea (di norma alla prima accensione). Tale modalità permette di elevare al massimo la protezione contro virus ed agenti esterni.

È tassativamente vietato all'utente ogni sorta di aggiornamento manuale del software installato se non espressamente autorizzato. Gli aggiornamenti del software e dei driver necessari al buon funzionamento della postazione di lavoro saranno effettuati direttamente dai tecnici del Titolare configurando gli aggiornamenti automatici per ciò che attiene la protezione antivirus ed il sistema operativo, ed intervenendo dietro segnalazione dell'utente per ogni ulteriore update si dovesse rendere necessario.

8. Utilizzo e conservazione dei supporti removibili

È obbligatorio limitare l'uso di dispositivi esterni (dischetti, CD e DVD riscrivibili, supporti USB, ecc.) a quelli strettamente necessari per le attività aziendali. In tali supporti non devono essere conservati, nemmeno provvisoriamente, file aziendali congiuntamente a file personali. Non è consentito l'utilizzo di cd, dvd, nastri magnetici, chiavette USB, hard disk esterni ecc., di dubbia provenienza.

Ogni dispositivo di memorizzazione di provenienza esterna dell'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo (consultare sezione ANTIVIRUS).

I supporti rimovibili contenenti dati particolari o giudiziari devono essere ridotti ai casi di assoluta necessità e, se non utilizzati, sono distrutti o resi inutilizzabili. I supporti magnetici rimovibili contenenti dati particolari nonché informazioni costituenti il know-how aziendale, devono essere trattati con particolare cautela (utilizzando processi di crittografia) onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto, o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati particolari, ciascun utente dovrà utilizzare gli strumenti messi a disposizione dal sistema operativo in uso per procedere alla formattazione a basso livello del supporto.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti. In ogni caso, qualora indispensabili all'attività lavorativa, i supporti magnetici contenenti dati particolari devono essere adeguatamente custoditi dagli utenti in appositi archivi come previsto dalla normativa in vigore.

È assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Ogni utente deve prestare la massima attenzione nell'utilizzo di memorie di massa esterne, nel caso in cui siano rilevati virus seguire le indicazioni impartite nella sezione (ANTIVIRUS).

9. Dismissione apparecchiature elettriche ed elettroniche

La dismissione dei dispositivi elettronici contenenti dati personali, comuni e particolari, dovrà avvenire secondo le indicazioni contenute nella "*Procedura sullo smaltimento o sul reimpiego di apparecchiature elettriche ed elettroniche*", contenente la previsione delle misure di sicurezza idonee allo smaltimento e/o al reimpiego degli stessi.

10. Utilizzo della rete fisica (LAN)

La rete fisica (LAN – Local Area Network) si basa sul protocollo TCP/IP ed è una risorsa strategica per la Società in quanto connette ogni dispositivo informatico veicolando i dati conservati negli archivi centrali. Funge da mezzo di trasporto per altri tipi di informazioni, pertanto, ogni disservizio o sua interruzione, comporta notevoli disagi per l'operatività della Società medesima. Tutte le postazioni di lavoro operano interconnesse alla rete geografica aziendale e possono così accedere ai dati secondo precise abilitazioni.

Non è ammessa la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, impianti wireless, ecc.). Un eventuale uso di tali apparati, qualora necessario, dovrà essere richiesto al Titolare. Analogamente non è ammesso l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub).

Viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro ed ogni altro dispositivo informatico (es. computer e portatili non aziendali) se non previa esplicita e formale autorizzazione. Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti alla rete.
È fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali, ad esempio, e non solo, DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, accesso remoto, proxy server.

È fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware, l'utilizzo di tali strumenti è strettamente riservato al personale tecnico del Titolare al fine di monitorare le prestazioni della rete aziendale. Nel caso si riscontrasse la presenza di PC che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del Titolare procedere al blocco, se necessario, dell'attività di rete della postazione.

È fatto divieto di svolgere attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti.
Non è consentito l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto. Non è consentito depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio.
È obbligatorio interpellare il Titolare prima di ogni spostamento di postazioni informatiche, per valutarne l'impatto e la fattibilità e per predisporre le configurazioni adeguate.

11. Utilizzo della rete Wireless (WLAN)

Ad integrazione della rete LAN descritta nella precedente sezione "UTILIZZO DELLA RETE FISICA (LAN)", alcune aree dell'Ente potrebbero essere servite da reti senza fili, Wireless LAN, per consentire la trasmissione dei dati attraverso canali senza fili.
Utilizzando apparati Access Point vengono distribuiti due SSID (service set identifier – nome con cui una rete senza fili si identifica ai suoi utenti), "area- ospiti" ed "aslbi-aria" secondo specifiche esigenze.

La WiFi-LAN “aslbi-aria”risulta a tutti gli effetti un’estensione della rete LAN, pertanto, i client connessi, avranno la possibilità di accedere alle medesime risorse della rete locale cablata.
I responsabili possono chiedere, per motivate esigenze di mobilità, per i propri collaboratori l’accessibilità all’infrastruttura “aslbi-aria”.
La tecnologia è configurata e governata dai tecnici del Titolare, e l’Ente dispone il rilascio delle abilitazioni per il funzionamento alle richieste inviate dai Delegati/Responsabili.

12. Unità di rete, memorizzazione file e backup

Si ricorda che tutti i dischi o le altre unità di memorizzazione locali (es. il disco rigido della propria postazione di lavoro) non sono soggette al salvataggio, pertanto, si esorta a non memorizzazione informazioni in tali locazioni. La responsabilità del salvataggio degli eventuali dati ivi contenuti è pertanto a carico del singolo utente.
Le cartelle di rete presenti negli storage sono aree di condivisione di informazioni strettamente professionali e non devono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, in queste unità.

Su queste unità vengono svolte regolari attività di controllo e amministrazione. I dati conservati in tali aree sono protetti da procedure di backup automatico gestite e monitorate dal concessionario stesso (la policy attuale è configurata per un backup incrementale giornaliero e archiviazione full mensile con profondità 1 anno).

Non è consentita la modifica dei permessi di accesso delle cartelle di rete da parte degli utenti. Al momento dell’assunzione, se non diversamente specificato, le nuove utenze vengono abilitate in modalità predefinita di “lettura/scrittura” sulle risorse dati (files e cartelle) della struttura di afferenza.

Ove possibile, il Titolare metterà a disposizione degli utenti che ne facessero richiesta una cartella di rete. L'utente potrà utilizzare in maniera esclusiva e riservata tale unità per il salvataggio dei dati di natura aziendale.

Per i soli di casi di cessazione del rapporto di lavoro (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi 30gg, il Titolare procederà alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti.

Il personale tecnico del Titolare, senza necessità di esplicita autorizzazione, può in qualunque momento procedere alla rimozione di file o applicazioni che riterrà pericolosi per la sicurezza sia sui PC degli incaricati, sia sulle unità di rete.
Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È assolutamente da evitare un'archiviazione ridondante.

Analogamente a quanto indicato per gli archivi locali, è assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Nel caso vengano attuati trattamenti idonei a rivelare lo stato di salute o la vita sessuale dei soggetti è onere del responsabile l’adozione degli strumenti messi a disposizione al fine di applicare opportune tecniche di cifratura atte a rendere non accessibili le informazioni trattate.

13. Antivirus

La politica di sicurezza aziendale prevede l'installazione su tutte le postazioni di lavoro di uno stesso software antivirus che viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un server dedicato. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzati dal Servizio Informativo.

Per quanto concerne le modalità di aggiornamento del servizio, consultare la relativa sezione "AGGIORNAMENTO DEL SISTEMA OPERATIVO E DEL SOFTWARE".

Ogni utente è tenuto a controllare la presenza del software antivirus verificandone la presenza dell'icona sulla systray sul desktop del proprio sistema operativo; nell'eventualità si ravvisasse la mancanza di tale software l'utente dovrà darne immediata segnalazione al Titolare per attivare le successive azioni inerenti l'installazione.

Nel caso il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'accaduto al Titolare.

Ogni dispositivo di memorizzazione esterno dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato e immediatamente scollegato.

Per ottemperare a quanto previsto dalle misure minime di sicurezza Agid, all'interno dell'Ente è stata abilitata di default, su tutti i client, la modalità "Scanallfiles in removable storage device safter plugin", atta ad effettuare la scansione di tutte le periferiche rimovibili che vengono collegate. È, inoltre, attivo il blocco dell'esecuzione "autorun" che disinnesca l'esecuzione automatica di contenuti al momento della connessione dei dispositivi mobili. Qualora si riscontrasse da parte del dipendente il mancato rispetto di quanto sopra indicato - e quindi un comportamento non corretto - ogni danno provocato dalla presenza di un malware (virus, worm, trojanhorse, backdoor, spyware, etc.) potrà essere direttamente imputabile al dipendente stesso.

14. Internet e navigazione

Il PC in uso all'utente, qualora abilitato alla navigazione in Internet, costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. L'abilitazione alla navigazione è assegnata a livello di utenza e non di postazione. L'abilitazione alla navigazione su internet deve essere accordata dal responsabile del trattamento. Qualora l'utente non fosse stato abilitato alla navigazione in internet è fatto divieto assoluto di connettersi autonomamente alla rete Internet. È fatto divieto di utilizzare credenziali di accesso ad Internet diverse da quelle di cui si è assegnatari.

L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.

È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa e durante l'attività stessa. A titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:

- l’upload o il download di software gratuiti (freeware) e shareware, nonché l’utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all’attività lavorativa e previa verifica dell’attendibilità dei siti in questione;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalTitolare;
- il download di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di file o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio;
- ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
- diffusione di virus, malware, trojanhorse o altri programmi, la cui azione consista nel sabotaggio, distruzione o alterazione del contenuto informativo delle stazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
- registrarsi a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line, di social networks, e bacheche;
- per attività di furto di dati di altri utenti, organismi e/o aziende;
- per attività di hackeraggio e pirateria informatica in generale

L'Ente regolamenta la navigazione in Internet attraverso l'utilizzo di sistemi di web filtering che inibiscono, preventivamente, l'accesso a siti dal contenuto chiaramente non attinente alle attività istituzionali, contrario al buon costume, potenzialmente pericoloso per la sicurezza e l’integrità dei dispositivi e dei servizi informatici aziendali.

Il Titolare ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi aziendali ed ha facoltà di accesso ai file di log dell’infrastruttura proxy. Il sistema di navigazione per mezzo di proxy aziendale effettua il monitoraggio dei siti visitati dai dipendenti. Tali dati vengono conservati al fine di rispondere ad eventuale legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

15. Posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro di proprietà aziendale concesso in uso al lavoratore al fine di un più proficuo svolgimento della prestazione. Al momento dell’assunzione, il personale viene dotato di credenziali di accesso alle postazioni e di indirizzo di posta elettronica ordinaria (PEO). La PEO può essere rilasciata “ad personam”, associata ad una Area, associata ad un ufficio o associata ad una specifica funzione/progetto o servizio.

Le caselle di posta nominative, vengono assegnate utilizzando il seguente formato: nome.cognome@aslbi.piemonte.it (in caso di omonimia verrà aggiunto un progressivo numerico: nome.cognome2@aslbi.piemonte.it, nome.cognome3@aslbi.piemonte.it).

L’accesso alla casella di posta elettronica aziendale avviene mediante un codice di identificazione personale e una parola chiave segreta.

Qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad uscire dalla casella di posta elettronica.

È assolutamente proibito l'accesso a caselle di posta aziendali diverse da quella/e assegnate.

L'accesso alla casella di posta elettronica è possibile tramite la suite Google Workspace utilizzando le credenziali di autenticazione personali fornite al momento della presa in servizio nella forma "userID" e "password".

Seguendo le precedenti indicazioni l'utente potrà consultare la propria casella direttamente via web; tale soluzione offre all'utente la possibilità di accedere alla propria cassetta postale anche al di fuori dell'ambiente lavorativo.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o altro codice malware (worm, trojan, spyware, backdoor, ecc). È buona norma, ad esempio, non aprire mail o relativi allegati sospetti. È obbligatorio porre la massima attenzione nell'aprire i file in allegato ai messaggi di postaelettronica prima del loro utilizzo - non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga saturano lo spazio disponibile. Si ricorda a tal fine che sarà necessario eliminare anche i messaggi contenenti allegati di grandi dimensioni presenti nelle cartelle POSTA IN ARRIVO, POSTA INVIATA e CESTINO; si raccomanda inoltre di procedere all'eliminazione definitiva dei messaggi che vengono spostati nella cartella CESTINO utilizzando la voce SVUOTA evidenziando con il tasto destro del mouse la voce CESTINO.

È fatto divieto di utilizzare le caselle di posta elettronica su dominio @aslbi.piemonte.it per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo e non esaustivo, l'utente non potrà utilizzare la posta elettronica per:

- inviare e/o ricevere allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- inviare e/o ricevere messaggi personali o per partecipare a dibattiti, aste on line, concorsi, forum o mailing-list;
- partecipare a catene telematiche (o di Sant'Antonio). Non si dovrà in alcun caso procedere all'apertura degli allegati contenuti in tali messaggi;
- aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);
- rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- invio intensivo di posta elettronica indesiderata o invasiva (spam).

È possibile ottenere, nelle comunicazioni esterne ed interne all'Ente, una segnalazione relativamente al recapito del messaggio e all'avvenuta lettura; si ricorda, però, che la conferma

dell'avvenuta lettura è a discrezione del destinatario. Per avere garanzia di quanto sopra espresso è, pertanto, opportuno chiedere al destinatario di confermare esplicitamente.

Nel caso di messaggi in cui sia essenziale conservare la ricevuta di ricezione (e per l'invio ricezione di posta elettronica certificata per fini aziendali) è appropriato utilizzare sempre la posta elettronica certificata (PEC), accessibile tramite gli strumenti messi a disposizione dal Titolare.

Di norma non vengono concesse caselle di posta certificata personalizzate a meno di disposizioni normative diverse o specifiche richieste preventivamente autorizzate dal direttore generale.

Si raccomanda di prestare attenzione alla dimensione degli allegati, poiché il gestore di posta blocca i messaggi (in ingresso ed in uscita) la cui dimensione ecceda i 20MB. È, pertanto, consigliato, nel caso di invii di documenti pesanti, l'utilizzo di formati compressi (*.zip, *.rar, *.tar, ..).

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso la funzionalità deve essere attivata manualmente dall'utente.

Come previsto dalle Linee Guida del Garante in materia, in previsione 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 potrà delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi e a inoltrare a chi di dovere quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa affidandogli, in modalità protetta, la password del proprio personal computer.

In caso di assenza non programmata (dovuta ad esempio a "malattia"), qualora non sia possibile acquisire ordinariamente informazioni o comunicazioni che, se non ricevute o recepite con ritardo, potrebbero arrecare un evidente danno all'Ente e, nel caso non sia stato nominato il fiduciario di cui al punto precedente, sarà consentito al superiore gerarchico dell'utente, di accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario e non sia possibile procedere altrimenti cambiando la password e informando il lavoratore interessato alla prima occasione utile. Quest'ultimo accesso, deve essere formalmente motivato e sottoscritto dal superiore gerarchico. Il provvedimento di cui sopra e il verbale a rappresentazione delle operazioni eseguite sono poi consegnati al lavoratore al momento della ripresa in servizio.

Il personale tecnico del Titolare, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potràaccedere alla casella di posta elettronica per le sole finalità atte a garantire la sicurezza e la salvaguardia del sistema, nonché per motivi tecnici e/o manutentivi.

Si raccomanda di prevedere, con la funzione di inserimento automatico della firma in calce all'email, la seguente avvertenza sulla privacy e sulla confidenzialità dei messaggi inviati:

- *VERSIONE ITALIANA*

Le informazioni, i dati e le notizie contenute nella presente comunicazione ed i relativi allegati sono di natura privata e come tali possono essere riservati e sono, comunque, destinate esclusivamente ai destinatari indicati in epigrafe. La diffusione, distribuzione e/o la copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., sia ai sensi della Normativa privacy Reg. (UE) n. 679/2016 e D. Lgs. n. 196/2003, integrato con le modifiche introdotte dal D.lgs. n. 101/2018. Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di darcene immediata comunicazione, anche inviando un messaggio di ritorno all'indirizzo e-mail del mittente.

- *ENGLISH VERSION*

This e-mail (including attachments) is only referred to the recipient(s) named above. It may contain confidential or privileged information and must not be spread, copied or otherwise used by any other person. If you have received this message by mistake, please destroy it and give immediate notification by sending a return message to the sender's e-mail address.
The legal references are the European Union Regulation 679/2016 and the Legislative Decree 196/2003, integrated with the changes introduced by the Legislative Decree 101/2018.

I servizi di posta elettronica sono suscettibili – attraverso la tenuta di log file di traffico e-mail e archiviazione dei messaggi – di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro del contenuto della corrispondenza. I dati e la corrispondenza intercorsa sono mantenuti riservati e possono essere resi disponibili a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

Nei giorni antecedenti all'interruzione del rapporto di lavoro, siano essi cessazioni (mobilità in uscita, pensionamenti, dimissioni, ecc.) o sospensioni (aspettativa a vario titolo, congedi, utilizzo e comandi presso altri enti, ecc.), è onere del titolare della casella mail inserire idoneo messaggio automatico in relazione alla dismissione della cassetta postale.

Alla data di conclusione del rapporto di lavoro si procederà con la disabilitazione dell'utenza associata alla cassetta di posta (impedendone l'accesso) e con l'inibizione dell'invio e della ricezione di messaggi esternamente.

Per i soli di casi di cessazione del rapporto di lavoro (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi ulteriori 30gg, la cassetta di posta sarà definitivamente cancellata e non sarà possibile recuperare i dati (indirizzi, comunicazioni, ecc..) in essa contenuti.

In caso di sospensione del rapporto di lavoro, verrà valutata di concerto tra il responsabile del servizio e il soggetto interessato l'opportunità di procedere alla cancellazione o alla sospensione della casella e-mail personale.

Non è prevista la copia del contenuto della casella a favore del cessante. Si ricorda infatti, che il contenuto della casella di posta aziendale, ed il relativo utilizzo, sono di proprietà aziendale e sono regolamentati dall'Azienda ed ogni utilizzo degli stessi deve preventivamente essere autorizzato.

La cancellazione delle cassette mail di servizio non personali avviene su specifica richiesta del responsabile di struttura che ha in carico la gestione della casella stessa (o di suo superiore). In tal caso, contestualmente all'eliminazione, il Titolare procede d'ufficio creando un file archivio della cassetta da cancellare e consegnando il supporto rimovibile utilizzato (per esempio DVD, o

file su share di rete) al responsabile della casella. È onere del ricevente, istanziando eventualmente richiesta di supporto al Servizio Informativo, la verifica di integrità dell'archivio. Si ricorda che trascorsi ulteriori 30gg la cassetta non risulterà ripristinabile.

16. Spam e phishing

Qualora si ravvisassero casi di spam o di phishing - tipo di frode ideato allo scopo di rubare importanti dati personali dell'utente, come ad esempio numeri di carta di credito, password, dati relativi al proprio conto e così via - è necessario segnalarlo immediatamente ai tecnici del Titolare.

17. Memorizzazione dei log dei sistemi informatici

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete ed i sistemi informatici aziendali, memorizzano un giornale (file di log) contenente le informazioni relative agli accessi degli utenti dei sistemi ed al dettaglio delle attività svolte dagli stessi. Il Titolare, attraverso il Servizio Informativo Aziendale, ha Sistema di facoltà di accesso ai log. Tali dati vengono conservati, a norma di legge, al fine di rispondere ad eventuale legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

Tale archivio memorizza l'indirizzo IP, il nome macchina della postazione di lavoro ed i riferimenti dell'utente. I sistemi software sono programmati e configurati in modo da sovrascrivere con cadenza periodica i dati di navigazione. L'eventuale prolungamento dei suddetti tempi di conservazione é eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

18. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole in esso contenute, qualora siano ravvisabili profili quantomeno colposi nella condotta osservata, è perseguibile nei confronti del personale dipendente mediante l'attivazione di procedimenti disciplinari previsti dalla normativa vigente.

Si ammonisce, altresì, il dipendente a non intercettare, interrompere o impedire le comunicazioni informatiche/telematiche e a non danneggiare informazioni, dati o programmi informativi nonché i sistemi informatici o telematici aziendali e/o di pubblica utilità.

19. Uso personale di infrastruttura aziendale

Non sono previste modalità di utilizzo personale di mezzi informatici dell'Ente con pagamento o fatturazione a carico dell'interessato.

20. Disposizioni finali, entrata in vigore e pubblicità

Il Regolamento per l'utilizzo delle risorse informatiche, proposta dal Titolare, entra in vigore dalla data di esecutività dell'atto deliberativo.

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

Per quanto non espressamente previsto nel presente regolamento sarà fatto riferimento alla normativa vigente in materia.

Il presente Regolamento verrà debitamente e tempestivamente portata a conoscenza di tutti i dipendenti della Società attraverso la pubblicazione sul sito internet istituzionale, sarà pubblicata su un'unità di rete accessibile a tutti gli utilizzatori e verrà inoltrata nota informativa a tutte le strutture aziendali.

È fatto obbligo di adeguare i propri comportamenti alle disposizioni previste nel presente Regolamento ed a chiunque competa di osservarla.