Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Agenzia di Tutela della Salute di Brescia
Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.ats-brescia.it
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

DECRETO n. 533 del 29/08/2023

Cl.: 1.1.02

OGGETTO: Aggiornamento del Regolamento dell'Agenzia sull'utilizzo dei Sistemi Informatici (in sostituzione del Regolamento di cui al Decreto D.G. n. 179/2013).

Il DIRETTORE GENERALE - Dott. Claudio Vito Sileo
nominato con D.G.R. XI/1058 del 17.12.2018

Acquisiti i ***pareri*** del
DIRETTORE SANITARIO Dott.ssa Laura Emilia Lanfredini
del
DIRETTORE SOCIOSANITARIO Dott. Franco Milani
e del
DIRETTORE AMMINISTRATIVO Dott.ssa Sara Cagliani

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

IL DIRETTORE GENERALE

Premesso che:
- è dovere dell'Ente individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità di differente natura;
- è, quindi, necessario porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità come sancito dallo Statuto dei Lavoratori (legge n. 300/1970);
- con Decreto D.G. n. 179 del 05.04.2013, era stato approvato il Regolamento per l'utilizzo dei sistemi informatici aziendali;

Richiamato il Piano di Organizzazione Aziendale Strategico dell'ATS di Brescia, adottato con proprio Decreto n. 308 del 26.05.2022 ed approvato con D.G.R. n. XI/6809 del 02.08.2022, provvedimento di cui si è preso atto con proprio Decreto n. 475 del 12.08.2022;
Ritenuto di dover adeguare il Regolamento sopra richiamato alla realtà organizzativa e funzionale dell'Agenzia mediante l'adozione di un nuovo testo regolamentare, come proposto dal Direttore della SC Sistemi Informativi qui allegato e composto da n. 19 pagine;
Vista la proposta presentata dal Direttore della SC Sistemi Informativi, Ing. Ivan Campa, che, anche in qualità di Responsabile del procedimento, attesta la regolarità tecnica del presente provvedimento;
Dato atto che dal presente provvedimento non discendono oneri per l'Agenzia;
Acquisiti i pareri del Direttore Sanitario, Dott.ssa Laura Emilia Lanfredini, del Direttore Sociosanitario, Dott. Franco Milani e del Direttore Amministrativo, Dott.ssa Sara Cagliani che attesta, altresì, la legittimità del presente atto;

D E C R E T A

a) di approvare, per le motivazioni di cui in premessa e con contestuale revoca del Decreto D.G. n. 179 del 05.04.2013, l'Allegato "A" (composto da n. 19 pagine), parte integrante e sostanziale del presente provvedimento, recante il Regolamento del Regolamento sull'utilizzo dei Sistemi Informatici dell'Agenzia di Tutela della Salute di Brescia;
b) di dare atto che il regolamento di cui sopra entra in vigore dalla data di pubblicazione del presente atto;
c) di demandare alla SC Sistemi Informativi ogni conseguente informativa a tutte le articolazioni dell'Agenzia;
d) di dare atto che dal presente provvedimento non discendono oneri per l'Agenzia;
e) di disporre la pubblicazione dei contenuti del presente provvedimento nella sezione "Amministrazione Trasparente" del sito web dell'Agenzia, in conformità al D.Lgs. 33/2013 e ss.mm.ii. nei tempi e con le modalità della Sezione Anticorruzione e Trasparenza del PIAO vigente;
f) di dare atto che il presente provvedimento è sottoposto al controllo del Collegio Sindacale, in conformità ai contenuti dell'art. 3-ter del D.Lgs. n. 502/1992 e ss.mm.ii. e dell'art. 12, comma 14, della L.R. n. 33/2009;
g) di disporre, a cura della SC Affari Generali e Legali, la pubblicazione all'Albo on-

line – sezione Pubblicità legale - ai sensi dell'art. 17, comma 6, della L.R. n. 33/2009, e dell'art. 32 della L. n. 69/2009, ed in conformità alle disposizioni ed ai provvedimenti nazionali e comunitari in materia di protezione dei dati personali.

Firmato digitalmente dal Direttore Generale
Dott. Claudio Vito Sileo

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Regolamento dell'Agenzia sull'utilizzo dei sistemi informatici

1 I principi

Art.1 - Introduzione definizioni e finalità

Il presente regolamento ha l'obiettivo di definire l'ambito di applicazione, i comportamenti, le modalità e le norme che gli utenti (dipendenti, collaboratori ecc.) devono rispettare al fine di tutelare i beni dell'Agenzia ed evitare condotte inconsapevoli o scorrette che potrebbero esporre la società a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti degli utenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.

A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 01/03/2007).

Art.2 - Ambito di applicazione

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche dell'Agenzia ovvero utilizzatore di servizi e risorse informative.

Per utente pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura dell'Agenzia utilizzandone beni e servizi informatici.

Per ente si intende, invece, la società, l'organizzazione e in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art.3 - Titolarità dei beni e delle risorse informatiche

Le risorse informatiche, i servizi ICT (*Information and Communication Technologies*) e le reti informative costituiscono beni dell'Agenzia rientranti nel patrimonio e sono da considerarsi di esclusiva proprietà dell'ente.

Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti all'attività svolta per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi dell'Agenzia.

A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura aziendale e non riservata.

Art.4 - Responsabilità personale dell'utente

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'ente, nonché dei relativi dati trattati.

A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'ente e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale da utilizzi impropri o non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse dell'Agenzia.

Ogni utente è tenuto a operare a tutela della sicurezza informatica aziendale, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente.

Art.5 - Controlli

L'ente esclude la configurabilità di forme di controllo aventi direttamente a oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, statuto dei lavoratori).

Ciononostante, non si esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro. Per tali evenienze, eventualmente, sarà onere dell'ente sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali. In difetto di accordo e su istanza dell'ente sarà l'ispettorato del lavoro a indicare le modalità per l'uso di tali impianti.

I controlli posti in essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.

L'ente, riservandosi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici dell'agenzia (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della gradualità. In attuazione di tale principio:

- i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
- nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici dell'Agenzia, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;
- in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

L'ente titolare non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

2 Misure organizzative

Art.6 - Amministratori di sistema

L'ente conferisce all'amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche dell'Agenzia. È compito dell'amministratore di sistema:

- gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;
- gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- provvedere alla sicurezza informatica dei sistemi informativi dell'Agenzia;
- utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (o *designato*) all'interno dell'ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Deve essere redatto un elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, aggiornato con cadenza annuale ovvero ogni volta che si rilevino modifiche.

L'ente si avvale di un servizio di prima assistenza tecnica (Helpdesk) che ha il compito di fornire immediata assistenza ai problemi più comuni riscontrati dagli utenti. Tale personale dispone di accessi amministrativi verso le macchine per poter svolgere il compito indicato, inoltre si occuperà di ricondurre problemi che esulino dalle proprie competenze verso le funzioni dell'Agenzia preposte (ad esempio verso gli amministratori di sistema).

Art.7 - Assegnazione degli account e gestione delle password

7.1 Creazione e Gestione degli Account

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche dell'Agenzia per singola postazione lavorativa.

Gli account utenti vengono creati dagli amministratori di sistema e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", ad esempio costituite da username e password, comunicate all'utente dall'amministratore di sistema che le genera con

modalità tali da garantirne la segretezza. Per l'accesso a determinati servizi e obbligatorio utilizzare l'Autenticazione Multifattoriale (MFA Multi Factor Authentication).

Le credenziali di autenticazione costituiscono dati dell'agenzia da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'ente.

Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al responsabile privacy di riferimento.

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive dell'Agenzia o per la sicurezza e operatività delle risorse informatiche, l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento dell'amministratore di sistema.

I beni e la strumentazione informatica oggetto del presente regolamento rimangono di esclusivo dominio dell'ente, che in conseguenza dei rapporti instaurati con gli utenti ne disciplina l'assegnazione.

7.2 Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni 90 giorni.

L'utente, nel definire il valore della password, deve rispettare le seguenti regole:

- Non dovrà essere stata utilizzata in precedenza (le precedenti 24 volte)
- La durata massima sarà 90 giorni
- La durata minima sarà 1 giorno (significa che ogni nuova password deve essere usata per almeno un giorno, non può essere subito cambiata)
- La lunghezza minima sarà 14 caratteri
- Dovrà contenere almeno tre delle seguenti caratteristiche
    - lettere maiuscole (A-Z)
    - lettere minuscole (a-z)
    - numeri (0-9)
    - caratteri non alfabetici (ad esempio /&%$£"!=?<>,;.:-_@#§()[]{}^)
- Non dovrà contenere il nome utente o parti del nome e cognome costituite da più di due caratteri
- L'utenza verrà bloccata al terzo tentativo di digitazione password errato, e si sbloccherà automaticamente dopo 15 minuti

L'utente dovrà proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;

Appuntare la password su post-it o altri supporti non è conforme alla normativa, compromette in maniera pressoché totale le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

L'ente si riserva in ogni momento di adottare criteri più vincolanti e sistemi di autenticazione più evoluti nonché di applicare restrizioni ulteriori al fine di rafforzare la sicurezza della rete. Avrà cura di darne tempestiva comunicazione agli utenti (secondo le modalità indicate nell'*Art.22 - Accesso e*

aggiornamento del documento) e di organizzare, laddove necessaria, la formazione all'utilizzo dei nuovi strumenti o sistemi.

7.3 Cessazione Degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 30 (trenta) giorni da quella data; entro 90 (novanta) giorni, invece, si disporrà la definitiva e totale cancellazione dell'account utente.

Art.8 - Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito PC), laptop, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (*device*) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici dell'Agenzia ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di disciplinare un corretto utilizzo di tali beni l'ente ha adottato le seguenti regole tecniche:

- ogni PC, laptop (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (*device*), sia esso acquistato, noleggiato o affidato in locazione, rimane di esclusiva proprietà dell'ente ed è concesso all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti all'attività svolta;
- è dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
- il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'ente; per utilizzare software o applicativi non presenti nella dotazione standard fornita è necessario presentare richiesta come indicato nell'5Art.21 - Art.21 - Richieste di autorizzazione;
- le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive; quando un utente si allontana dalla propria postazione di lavoro deve bloccare o effettuare il log-out dalla sessione.
- l'utente deve segnalare con la massima tempestività all'assistenza tecnica (Helpdesk) eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature;
- è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici dell'Agenzia a soggetti terzi;
- l'ente si riserva la facoltà di rimuovere o disabilitare d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche dell'agenzia salvo preventiva autorizzazione.

Art.9 - Accesso documenti dell'Agenzia

Tutti i documenti dell'Agenzia vanno collocati esclusivamente nelle apposite condivisioni di rete, per le quali viene eseguito regolare backup e monitorato l'accesso.

Non è consentito memorizzare documenti dell'Agenzia su dispositivi esterni (chiavette USB, hard disk mobili, cloud personali ecc.). Le abilitazioni degli utenti alle singole cartelle di pertinenza vanno formalizzate con una richiesta da parte del Dirigente responsabile.

Non è consentito utilizzare la memoria di massa delle Postazioni di Lavoro per memorizzare documenti dell'Agenzia, se non delle copie per uso temporaneo. Non viene effettuato alcun backup delle postazioni client (PC, tablet, laptop) né tantomeno gestito il trasferimento dei dati locali della postazione, in caso di sostituzione della stessa.

3 Criteri di utilizzo degli strumenti informatici

Art.10 - Dispositivi (*devices*): Desktop, Laptop, Tablet, Smartphone, etc.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (*devices*) di proprietà dell'ente e sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio dispositivo, se non previa esplicita autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'Art.21 - Richieste di autorizzazione) che la esegue per mezzo dell'amministratore del sistema;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'ente;
- è onere dell'utente, in relazione alle sue competenze lavorative, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'Helpdesk e al proprio responsabile;
- è onere dell'utente spegnere il proprio PC giornalmente al termine dell'attività lavorativa.
- l'utente ha l'obbligo di custodire con diligenza e in luogo protetto durante gli spostamenti computer e degli altri dispositivi portatili,
- non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

Gli utenti dotati di strumenti informatici sono responsabili della loro custodia e utilizzo, secondo quanto previsto dalle disposizioni degli specifici articoli del presente Regolamento.

L'utente che, venendo meno al dovere di diligenza nella custodia, causi il danneggiamento o smarrimento delle dotazioni informatiche affidate, risponderà del danno patrimoniale e/o non patrimoniale arrecato all'ente e/o a terzi, secondo quanto previsto dal codice disciplinare e dai documenti in esso richiamati.

Gli Utenti sono tenuti a comunicare tempestivamente alla SC Sistemi Informativi eventuali furti e/o danneggiamenti, di tali strumenti, nonché eventuali anomalie di funzionamento che ne possano pregiudicare la regolare funzionalità.

Nel caso di furto o smarrimento di un qualsiasi dispositivo appartenente all'ente il dipendente che ne abbia conoscenza, deve:

- sporgere denuncia, entro 24 ore dal furto o dallo smarrimento, presso le forze dell'ordine quali polizia o carabinieri (specificando il codice IMEI nel caso di cellulari o di SIM inserita all'interno del tablet o portatile);
- richiedere il blocco SIM all'operatore telefonico;
- informare immediatamente la SC Sistemi Informativi anche ai fini della tenuta, da parte della struttura stessa, dell'apposito registro delle violazioni. Sarà quindi sempre cura della SC Sistemi informativi comunicare all'ufficio Privacy l'accadimento in modo che lo stesso possa effettuare ogni

valutazione del contenuto del dispositivo rubato o smarrito a fini della eventuale necessità di attivazione delle procedure previste dalla normativa europea in materia di privacy;
- richiedere una nuova dotazione informatica allegando la denuncia fatta alle forze dell'ordine.

Quanto sopra riportato al fine di evitare violazioni della sicurezza dei dati contenuti nei sopra indicati dispositivi che possano comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a tali dati.

Una volta acquisita la denuncia di furto o smarrimento, la SC Sistemi informativi potrà procedere al "reset" del dispositivo se e in quanto raggiungibile da remoto.

Art.11 - Software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'Art.21 - Richieste di autorizzazione) per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio *freeware* o *shareware*.

Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun utente è tenuto a osservare per un corretto utilizzo del software in azienda:

- le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza;
- non è consentito eseguire il download o la condivisione di software non autorizzato;
- considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione;
- la duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

Art.12 - Dispositivi mobili di connessione (internet key)

Agli assegnatari di computer o dispositivi portatili può essere concessa in dotazione anche una chiavetta internet o dispositivo similare per la connessione alla rete dell'Agenzia per consentire lo svolgimento delle mansioni lavorative anche da remoto.

I suddetti dispositivi mobili di connessione devono essere utilizzati esclusivamente sui computer forniti in dotazione dall'ente e non è consentito concederne l'utilizzo a soggetti terzi né utilizzarli su altri computer sia personali che di terzi.

Stessi criteri devono essere adottati per l'utilizzo della modalità Tethering o hotspot dei dispositivi mobili dell'Agenzia (Thetering o hotspot sono sistemi che permettono di condividere la connessione Internet attiva su dispositivi mobili come smartphone iOS, Android e Windows phone con altri dispositivi).

Art.13 - Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi fisici che consentono di copiare o archiviare dati, files, o documenti esternamente al computer: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.

L'utilizzo, salvo provate esigenze di servizio e dietro esplicita autorizzazione, di tali dispositivi non è consentito. In ogni caso l'ente ne scoraggia l'utilizzo favorendo invece le alternative messe a disposizione basate su tecnologia cloud e cartelle condivise.

Laddove espressamente autorizzato l'utilizzo di tali supporti deve rispondere alle direttive di seguito riportate:

- non è consentito utilizzare supporti rimovibili personali, se non approvati preventivamente dall'ente (per le modalità operative fare riferimento a quanto riportato all'Art.21 - Richieste di autorizzazione);
- se autorizzati in base alle procedure previste, una volta connessi all'infrastruttura informatica dell'ente, i dispositivi personali saranno soggetti (ove ciò sia compatibile) al presente regolamento;
- è onere dell'utente custodire i supporti contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere visualizzato da personale non autorizzato, trafugato, alterato o distrutto;
- dato l'elevato rischio di danneggiamento e perdita dei dati contenuti, tali supporti devono essere utilizzati esclusivamente per il trasferimento temporaneo di dati e non devono in nessun caso essere utilizzati per l'archiviazione a lungo termine. L'utente è responsabile del trasferimento dei dati verso supporti appropriati per l'archiviazione.

Art.14 - Stampanti, fotocopiatrici e fax

L'utilizzo di tali strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'ente.

Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Gli strumenti dotati di memoria, connessi o meno in rete, sono gestiti dall'Amministratore di Sistema che può provvedere alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

Art.15 - Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione del singolo utente, l'ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.

Come per qualsiasi altra dotazione dell'Agenzia, il dispositivo mobile rappresenta un bene dell'Agenzia concesso in uso per scopi esclusivamente lavorativi.

Al fine di controllo del corretto utilizzo dei servizi di fonia dell'Agenzia. l'ente può richiedere ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.

I controlli saranno eseguiti secondo criteri e modalità descritte all'Art.5 - del presente regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.

L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

- ciascun utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione;
  Nello specifico, dal momento in cui gli viene affidato, l'utente è ritenuto responsabile di tutto ciò che riguarda il telefono, includendo (a titolo esemplificativo e non esaustivo) programmi installati, impostazioni degli stessi, registrazioni multimediali effettuate, documenti memorizzati, dati ai quali si è acceduto e configurazioni generali dello strumento; deve inoltre attenersi a quanto indicato dall'ente per la gestione dello stesso;
- i dispositivi devono essere dotati di password di sicurezza, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:
  - il codice PIN dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione;
  - il codice PIN o altri codici di accesso dovranno essere modificati dall'assegnatario con cadenza al massimo semestrale;
  - ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'ente;
- in caso di furto, danneggiamento o smarrimento del dispositivo mobile l'utente assegnatario dovrà darne immediato avviso all'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
- in caso di furto o smarrimento l'ente si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;
- l'ente non è responsabile per la perdita o compromissione di dati personali che l'utente ha trasferito o memorizzato sul dispositivo;
- il telefono non è un dispositivo di archiviazione; ciascun utente deve provvedere personalmente al backup dei dati rilevanti contenuti con cadenza opportuna; l'ente si riserva di cancellare in qualsiasi momento e senza preavviso tutti i dati memorizzati, qualora fosse necessario ad esempio per ripristinare la funzionalità del dispositivo o per motivi di sicurezza;
- non è consentito all'utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano preventivamente autorizzate dall'ente;
- è vietato installare applicazioni al di fuori di quelle presenti sui marketplace ufficiali; l'utente è responsabile di tutte le applicazioni installate sul dispositivo e risponde personalmente degli

eventuali costi derivanti dall'utilizzo di applicazioni che ne prevedano (salvo i casi esplicitamente autorizzati).

4 Gestione delle comunicazioni Telematiche

Art.16 - Gestione utilizzo della rete internet

Ciascun utente potrà essere abilitato alla navigazione Internet e pertanto si richiamano tutti gli utenti a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere, è associata all'indirizzo internet pubblico assegnato all'ente.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- l'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- l'accesso garantito è nominale e concesso esclusivamente ad uso personale. Non è consentito condividere la rete o dare accesso a soggetti diversi dal titolare delle credenziali di accesso a meno di esplicita autorizzazione.
- non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'ente;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book;
- non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- è consentito l'utilizzo di soluzioni di Instant Messaging o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente;
- non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo, salvo casi espressamente autorizzati dall'ente;
- non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro;
- non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente approvata.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'ente.

Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole, l'ente si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

Periodicamente potranno essere effettuati controlli a campione sugli accessi internet effettuati dagli utenti stessi.

Si ribadisce che i controlli rispettano i principi di pertinenza e di non eccedenza. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori etc.) tanto della rete Internet che della posta elettronica. Nell'esercizio del potere di controllo l'ATS di Brescia si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

Art.17 - Social Media

In particolare sui social network, è fatto divieto di divulgare con qualunque mezzo (compresi siti web, social network, blog e forum, anche di natura privata e al di fuori dell'ambito lavorativo) informazioni lavorative riservate, come la corrispondenza interna, informazioni di terze parti (soggetti privati, altri dipendenti, altre pubbliche amministrazioni ecc.) di cui si è a conoscenza, o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, fatte salve le informative e gli accordi sindacali. È necessario rispettare la privacy dei colleghi ed evitare riferimenti al lavoro che si sta svolgendo o in generale alle attività svolte nell'ambito dell'ente, fatte salve le informazioni di dominio pubblico.

È vietato "aprire" blog, pagine o altri canali a nome dell'Agenzia o che trattino argomenti e notizie apprese in ambito lavorativo riferite all'attività istituzionale, salvo il diritto di esprimere valutazioni e diffondere informazioni nell'esercizio dell'attività sindacale, nonché utilizzare il logo dell'ente in account privati.

Il personale dell'ente è autorizzato ad accedere con proprio account personale ai social media e può liberamente condividere sui propri profili privati i contenuti già diffusi dai canali social istituzionali. Qualora l'appartenenza all'ente sia desumibile dal profilo dell'utente o rilevabile dal contenuto di un intervento, è opportuno specificare che le opinioni espresse hanno carattere personale e non impegnano in alcun modo la responsabilità dell'ente.

Art.18 - Gestione e utilizzo della posta elettronica e suite Microsoft Office web app aziendale

18.1 Principi Guida

Per ciascun utente titolare di un account, l'ente provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: sono strumenti di proprietà dell'ente conferiti in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso utente possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento.

Attraverso le caselle e-mail aziendali gli utenti rappresentano pubblicamente l'ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine dell'Agenzia.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica dell'agenzia conformemente alle presenti regole. Gli stessi devono:

- conservare la password nella massima riservatezza e con la massima diligenza;

- mantenere la casella di posta e gli spazi di archiviazione in ordine, cancellando documenti inutili e allegati ingombranti;
- monitorare periodicamente la percentuale di occupazione della casella email e dell'archiviazione online, provvedendo a rimuovere comunicazioni, allegati, e documenti vecchi o comunque non più necessari;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta; gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
- accertarsi dell'identità del mittente e controllare con software antivirus gli allegati di posta elettronica prima del loro utilizzo;
- rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre, considerando come certamente pericolosa ogni comunicazione sospetta, ad esempio evitando di inoltrarla a chicchessia (assistenza tecnica inclusa);
- collegarsi a link verso siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.

Inoltre, non è consentito agli utenti:

- diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet;
- utilizzare la casella di posta elettronica dell'agenzia per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video aziendali;
- inoltrare comunicazioni email o allegati che risultino sospetti verso altri utenti, nemmeno nel caso in cui lo scopo sia verificarne l'attendibilità;
- Connettersi tramite dispositivi personali agli strumenti aziendali (ad es. posta, applicativi office) qualora essi non rispettino standard di sicurezza pari o superiori a quelli adottati aziendalmente e descritti in questo documento (ad esempio protezione antivirus, accesso protetto da password complesse o sistemi equivalentemente robusti); è responsabilità dell'utente verificare la sussistenza delle condizioni appena indicate e dovrà rispondere direttamente dei danni provocati in caso di accertata negligenza.

Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto si richiede agli utenti di limitare quanto possibile l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale" tramite questo canale.

Occorre infine che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.

Nei casi in cui l'ente si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

18.2 Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano di inviare automaticamente messaggi di risposta. Tali messaggi dovranno contenere le coordinate di altro soggetto

cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

In caso di assenze non programmate, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'ente disporrà, lecitamente e mediante personale appositamente incaricato (l'Amministratore di Sistema oppure un suo incaricato), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.

Nel caso in cui l'ente necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente;
- di tale attività sarà redatto apposito verbale e informato l'utente interessato alla prima occasione utile nel rispetto della vigente normativa sulla privacy.

18.3 Cessazione dell'indirizzo di Posta Elettronica Aziendale

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni e si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

5 Sanzioni, comunicazioni, approvazione

Art.19 - Sanzioni

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare, fatte salve eventuali altre responsabilità, l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).

Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici dell'Agenzia.

In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

Art.20 - Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici dell'Agenzia e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'Art. 5 - , vale quale informativa ex art. 13 del Regolamento (UE) 2016/679 che integra, per gli aspetti non incompatibili, l'informativa generale pubblicata sul sito web di ATS Brescia nella Sezione Privacy.

Art.21 - Richieste di autorizzazione

Le richieste di autorizzazione o concessione previste dal presente regolamento possono essere inoltrate all'ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

Per qualsiasi richiesta, comprese quelle appena menzionate, è possibile in primo luogo rivolgersi al servizio di assistenza tecnica di primo livello (Helpdesk).

Art.22 - Accesso e aggiornamento del documento

Contestualmente all'assegnazione di un account il presente regolamento è messo a disposizione degli utenti per la consultazione. La versione più aggiornata dello stesso è pubblicata in formato digitale allo scopo di facilitarne la diffusione a tutti gli interessati.

Per ogni aggiornamento del presente regolamento sarà data comunicazione sulla intranet aziendale e tramite l'invio di specifico messaggio e-mail. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata.

A causa di urgenti motivi di sicurezza o al fine di tutelare il patrimonio dell'ente potrebbe essere necessario rendere immediatamente effettive modifiche al presente regolamento, prima ancora di poterlo aggiornare secondo le consuete modalità.

In tali casi sarà inoltrata immediatamente una comunicazione (ad esempio tramite email e con pubblicazione su intranet) che illustri nel dettaglio i cambiamenti adottati con riferimento al vigente regolamento informatico. La successiva revisione di tale documento sarà redatta in modo da includere le modifiche comunicate.

In ogni momento quindi il regolamento vigente è composto dal più recente documento (regolamento informatico) e dalle integrazioni che afferiscono allo stesso pubblicate sulla intranet.