DELIBERAZIONE DEL DIRETTORE GENERALE

Deliberazione n.ro	Data di Adozione
0000850	**09/05/2022**

OGGETTO: Adozione del Regolamento per l'uso degli strumenti informatici, Internet, posta elettronica e per la tutela dei Sistemi Informativi dell'Azienda Sanitaria Locale della Provincia di Bari.

PROPOSTA DI DELIBERAZIONE DEL DIRETTORE GENERALE N.RO 20220001910 DEL 03/05/2022
COMPOSTA COMPLESSIVAMENTE DA 5 (cinque) PAGINE
DI 1 (uno) ALLEGATI SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 39 (trentanove) PAGINE
DI 0 (zero) ALLEGATI NON SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 0 (zero) PAGINE
DI 0 (zero) DOCUMENTI ISTRUTTORI NON ALLEGATI PER UN TOTALE DI 0 (zero) PAGINE

Con la sottoscrizione in calce, i Direttori dichiarano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, alla Parte II, par. 1, lett. c) del vigente PTPCT – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

Parere del Direttore Amministrativo	Parere del Direttore Sanitario
Firmato Digitalmente il 04/05/2022 15:01 Luigi FRUSCIO	*Firmato Digitalmente il 05/05/2022 19:23* Donato SIVO

Il Segretario	Il Direttore Generale
Firmato Digitalmente il 09/05/2022 12:43 Domenico ROVETO	*Firmato Digitalmente il 09/05/2022 12:16* Antonio SANGUEDOLCE

ATTESTAZIONE DI AVVENUTA PUBBLICAZIONE

Si attesta che il presente provvedimento viene pubblicato all'Albo pretorio *on-line* della ASL BA, ai sensi dell'art. 32, c. 1, l. 69/2009, per la durata di 30 giorni naturali, decorrenti dal **09/05/2022**

Unità Operativa Affari Generali
L'Addetto alla Pubblicazione
Firmato Digitalmente il 09/05/2022 12:46
Roveto Domenico

OGGETTO: Adozione del Regolamento per l'uso degli strumenti informatici, Internet, posta elettronica e per la tutela dei Sistemi Informativi dell'Azienda Sanitaria Locale della Provincia di Bari

IL DIRETTORE GENERALE

Vista la Deliberazione n.239/DG del 16/02/2022, con l'assistenza del Segretario, sulla base della istruttoria e del Regolamento per l'uso degli strumenti informatici, Internet, posta elettronica e per la tutela dei Sistemi Informativi dell'Azienda Sanitaria Locale della Provincia di Bari redatta dall'Ing. Francesco Maurizio Mangini, Dirigente Analista della U.O. Analisi e Sviluppo del Sistema Informativo, condiviso con il Dirigente della UOS Privacy/DPO e della proposta formulata dall'Ing. Mario Cisternino, Direttore della U.O. Analisi e Sviluppo del Sistema Informativo, che ne attesta la regolarità formale del procedimento ed il rispetto della legalità, considera e determina quanto segue.

PREMESSO CHE

- Il Garante per la Protezione dei dati Personali, con Deliberazione del 01/03/2007 "Lavoro: le linee guida del Garante per posta elettronica e internet", interviene in materia di corretto utilizzo della posta elettronica e della rete internet da parte dei lavoratori nell'ambito delle funzioni lavorative, dettando regole in materia di trattamento dei dati dei dipendenti da parte dei datori di lavoro.

- con Deliberazione del Direttore Generale n.ro 925 del 16/05/2011, in ottemperanza al D.L.gs. 196/2003 – Codice della Privacy è stato adottato il "Regolamento per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche aziendali".

- Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 (GDPR), relativo alla protezione delle persone fisiche ridisegna una serie di regole volte alla tutela e alla riservatezza dei cittadini, al fine di garantire il trattamento dei dati personali, disciplinando, tra l'altro le modalità di adempimento degli obblighi del Titolare del trattamento in materia di sicurezza e riservatezza.

PRESO ATTO

- Della Legge 23 dicembre 1993 n. 547 – "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

- Della Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri – Dipartimento della funzione pubblica: "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

- Della Circolare AgID n° 1/2017 – "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). (17A02399)".

VISTO

- che, alla luce della normativa citata, il datore di lavoro ha l'onere di indicare chiaramente le corrette modalità di utilizzo degli strumenti informatici e le modalità con cui vengono effettuati controlli.

ACQUISITO

- il parere del DPO Aziendale, per gli aspetti di competenza.

CONSIDERATO

- di dover procedere alla adozione di un nuovo regolamento in linea con il GDPR e le direttive emanate da AgID.

Assunto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

DELIBERA

per i motivi esposti in premessa, che qui si intendono integralmente riportati per costituirne parte integrante:

1. di approvare il *«Regolamento per l'uso degli strumenti informatici, Internet, posta elettronica e per la tutela dei Sistemi Informativi»* che, allegato al presente provvedimento, ne costituisce parte integrante e sostanziale;
2. di demandare al Direttore U.O. Analisi e Sviluppo del Sistema Informativo, in quanto responsabile, o ad un suo un delegato, le istruttorie per la gestione delle modifiche e degli aggiornamenti futuri del medesimo Regolamento;

3. di trasmettere copia del presente provvedimento ai Direttori/Dirigenti/Responsabili delle macrostrutture/unità organizzative dell'azienda che, a loro volta, dovranno dare massima divulgazione nelle forme e modalità più opportune a tutti i dipendenti della ASL Bari e rendere disponibile il Regolamento sul Portale Dipendenti.

ASL Bari
PugliaSalute

Azienda Sanitaria Locale
della provincia di Bari

REGOLAMENTO AZIENDALE PER L'USO DEGLI STRUMENTI INFORMATICI, INTERNET, POSTA ELETTRONICA E PER LA TUTELA DEI SISTEMI INFORMATIVI

Versione 1.1	Data versione
Redatto da U.O.C. Sistemi Informativi	
Approvato con delibera n°	

ASL Bari PugliaSalute | Azienda Sanitaria Locale della provincia di Bari

INDICE

ASL Bari
PugliaSalute
Azienda Sanitaria Locale
della provincia di Bari

1 Introduzione

L'Azienda Sanitaria Locale della Provincia di Bari (nel seguito indicata come ASL BA) con il presente documento si prefigge l'obiettivo di salvaguardare il proprio patrimonio informativo aziendale, inteso quale complesso di risorse informatiche e di informazioni di cui dispone, definendo le procedure e le istruzioni per una loro corretta ed adeguata gestione.
Tale regolamento aggiorna, integra e sostituisce le eventuali disposizioni aziendali emanate in precedenza e costituisce parte rilevante delle misure tecniche ed organizzative adottate dall'Azienda per fare fronte alle esigenze di sicurezza nel trattamento dei dati personali e per minimizzare il rischio di violazioni dei dati, nel rispetto del regolamento UE 2016/679.

2 Riferimenti normativi

NORMATIVA EUROPEA

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

NORMATIVA ITALIANA

- DPCM 14 aprile 2021, n. 81 «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.» (GU Serie Generale n. 138 del 11-06-2021).
- D.Lgs. 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali», come modificato ed integrato dal D.Lgs. 101/2018.
- Legge n. 300 del 20 maggio 1970 recante «Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento».

- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica avente oggetto «Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro».
- Art. 23 del D.lgs. n. 151/2015 che modifica la fattispecie integrante il divieto dei controlli a distanza.

PROVVEDIMENTI AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Provvedimento del Garante per la protezione dei dati personali «Linee guida per posta elettronica e internet» del primo marzo 2007 (Gazzetta Ufficiale 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» del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008).
- 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» del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009).
- Provvedimento del Garante «Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali» del 13 ottobre 2008 (Gazzetta Ufficiale n. 287 del 9 dicembre 2008).

AGENZIA PER L'ITALIA DIGITALE – AGID

- Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativa a «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

3 Obiettivo e ambito di applicazione

Il presente documento regola le condizioni di utilizzo delle risorse informatiche che ASL BA mette a disposizione del personale dipendente e non dipendente per l'esecuzione delle funzioni di competenza. Sono disciplinate, inoltre, le modalità con le quali ASL BA può

accertare e inibire le condotte illecite degli utilizzatori di beni aziendali informatici, quali postazioni di lavoro (PdL), tablet, smartphone, di Internet e della posta elettronica, nonché dell'accesso alle risorse di archiviazione di massa. Nel caso di impiego di dispositivi di proprietà dell'utente, autorizzati dall'Azienda per motivi di lavoro quali, ad esempio, lo smart-working, la presente policy di sicurezza è estesa anche a tali dispositivi personali, per quanto compatibile.

Sono obbligati a rispettare le presenti disposizioni tutti gli utenti interni ed esterni che siano autorizzati ad accedere al sistema informatico aziendale e ad utilizzare le strumentazioni elettroniche fornite per l'esecuzione delle mansioni lavorative. Per utenti interni devono intendersi le persone fisiche che, in virtù di rapporti contrattuali o di convenzione, possono adoperare gli strumenti informatici aziendali all'interno del dominio di ASL BA.

Si considerano utenti esterni le persone fisiche, le aziende private e pubbliche e le ditte fornitrici che, sulla base di rapporti contrattuali o di convenzione autorizzati dalla Direzione di ASL BA, accedono dall'esterno del dominio ad alcune componenti del sistema informatico aziendale.

Prerequisito indispensabile sia per gli utenti interni sia per quelli esterni, è che essi siano autorizzati ai trattamenti dei dati da loro effettuati mediante gli strumenti informatici.

Non si riportano indicazioni specifiche, per quel che concerne le tipologie di dispositivi informatici e le informazioni di interesse aziendale, in quanto il contesto è in continua evoluzione; pertanto è essenziale comprendere la logica e le finalità sottese al presente documento per poter applicare in modo efficace le indicazioni fornite.

Il regolamento di cui trattasi è redatto in ossequio alle leggi vigenti e al Provvedimento a carattere generale, inerente l'utilizzo della posta elettronica e di Internet nel rapporto di lavoro, emesso Garante per la protezione dei dati personali in data primo marzo 2007.

Una corretta applicazione delle disposizioni previste presuppone il pieno assolvimento, da parte di ASL BA, degli obblighi contenuti nella Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017, relativa alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» e s.m.i., nonché di eventuali provvedimenti in materia emanati da organismi operanti nel medesimo settore.

Infine, tale documento aziendale costituisce adeguata informazione sul trattamento dei dati personali, sulle modalità d'uso delle risorse informatiche e sull'effettuazione dei controlli, ai sensi del regolamento UE 2016/679 e dell'art.4 della Legge n. 300 del 20 maggio 1970.

4 Il regolamento UE 2016/679

Le risorse informatiche e telematiche di ASL BA devono essere adoperate evitando comportamenti che, anche inconsapevolmente, possono arrecare danni o minacce alla protezione dei dati personali. Dunque, nell'espletamento delle proprie attività, ciascun operatore deve sempre improntare la propria azione alle previsioni del regolamento UE 2016/679. Quest'ultimo classifica i dati in:

- **Dati personali**
  Qualsiasi dato inerente una persona fisica identificata o identificabile; si considera tale la persona fisica direttamente o indirettamente individuata, con particolare riferimento ad elementi quale il nome, un codice identificativo, i dati relativi all'ubicazione, uno o più tratti caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Sono dati personali: nome e cognome, indirizzo, codice fiscale, foto, l'indirizzo IP o qualsiasi ripresa audiovisiva, ma anche altre notizie che, pur non essendo direttamente associabili, permettono di identificare l'individuo.

- **Dati particolari**
  Qualsiasi dato che, per la propria delicatezza, richiede particolari cautele; si tratta di quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici utili a identificare in modo univoco una persona fisica, e i dati relativi alla salute o all'orientamento sessuale della persona.

- **Dati relativi a condanne penali e reati**
  Qualsiasi dato inerente le condanne penali, i reati o le connesse misure di sicurezza. Si tratta dei dati personali idonei a rilevare provvedimenti emessi dalle Autorità

Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di Procedura Penale.

Il regolamento UE 2016/679 definisce il trattamento dei dati come una "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, 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 dei dati". Le operazioni di trattamento possono essere associate alle seguenti tre fasi:

1. **Reperimento delle informazioni.**
   Tale fase consiste nella raccolta dei dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: direttamente dall'interessato, mediante terzi o attraverso la consultazione di elenchi o siti web.

2. **Trattamento interno.**
   In questa fase ricadono tutte le operazioni messe in atto da colui che raccoglie le informazioni per organizzarle e renderle agevolmente fruibili. Esse sono:

   - La registrazione dei dati, ossia il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i trattamenti successivi.
   - L'organizzazione dei dati in senso stretto, inteso come il processo di lavorazione che ne consente la fruibilità mediante aggregazione o disaggregazione, accorpamento, catalogazione e così via.
   - L'elaborazione, intesa come il complesso delle operazioni che attribuiscono significatività ai dati, in relazione all'obiettivo per il quale essi sono stati raccolti.
   - La selezione, l'estrazione ed il raffronto.
   - La modifica dei dati registrati a seguito di variazioni o nuove acquisizioni.
   - L'interconnessione, ossia l'individuazione di relazioni tra banche dati diverse, al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto.

- Il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti.
- La conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza.
- La cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare determinati adempimenti.

3. **Uso delle informazioni nelle relazioni con l'esterno.**
   Questa fase racchiude i trattamenti più delicati, ossia quelli che hanno maggiore probabilità di ledere la sfera della riservatezza altrui. Essi vengono genericamente definiti come utilizzo, inteso come la concretizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni. L'utilizzo può essere:

   - Diretto, instaurando un rapporto con la persona sul conto della quale si sono raccolte informazioni.
   - Indiretto, che consiste nel mettere a disposizione di terzi le informazioni raccolte. Le operazioni cui la legge dedica le maggiori attenzioni – in quanto si tratta di quelle potenzialmente più lesive dei diritti e delle libertà degli interessati – sono quelle con cui si mettono a disposizione di terzi i dati personali.
     Tali operazioni sono:
     - La comunicazione, ovvero il portare a conoscenza dei dati personali uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
     - La diffusione, ovvero il portare conoscenza dei dati personali soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

È di tutta evidenza che qualsiasi trattamento, sia esso eseguito con o senza l'ausilio di mezzi elettronici, è assoggettato alla normativa privacy. Per quanto di competenza del presente documento, ASL BA, in qualità di titolare del trattamento, nell'esecuzione delle attività lavorative quotidiane, si avvale di risorse informatiche e telematiche per l'espletamento di

molteplici compiti. Le conseguenze di un uso improprio di tali risorse si possono presentare non solo sul piano tecnico, in termini di blocco della funzionalità o perdita di dati, ma anche sul piano giuridico, con l'insorgere di responsabilità sia penali sia civili a carico, contestualmente, del titolare e dell'operatore coinvolto.

Pertanto i dati personali devono sempre:

- Essere trattati in modo lecito, corretto e trasparente.
- Essere raccolti per finalità legittime ed individuate fin dall'inizio, e successivamente devono essere trattati in modo non incompatibile con tali finalità.
- Essere trattati esclusivamente quelli indispensabili, quindi pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- Essere corretti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
- Essere conservati in una forma che consenta l'identificazione degli interessati per il tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati e, successivamente cancellati, nel rispetto dei termini previsti dalle vigenti procedure di scarto degli archivi documentali.
- Essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

5 Politiche di sicurezza

Le politiche di sicurezza, indispensabili per un corretto utilizzo del sistema informativo di ASL BA da parte di ciascun utente, si prefiggono le seguenti finalità:

- Garantire la sicurezza, l'integrità, la disponibilità e la riservatezza del sistema informativo.

- Tutelare i beni e le risorse informatiche aziendali, i servizi ICT e le reti informatiche di ASL BA.

- Mitigare il rischio di data breach, ossia di violazioni di sicurezza che comportano in modo illecito o accidentale la distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali trasmessi, conservati o comunque trattati.

- Prevenire ed impedire condotte illecite, scorrette o inconsapevoli da parte degli operatori che potrebbero esporre l'Azienda a sanzioni amministrative, danni patrimoniali e di immagine.

6 Responsabilità personale dell'utente

Ogni utente è tenuto ad un comportamento consapevole, ispirato ai principi di diligenza, fedeltà, correttezza ed idoneo a preservare l'integrità delle risorse aziendali e la riservatezza delle informazioni, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del Codice Civile e della normativa vigente in materia di protezione dei dati personali.
Ciascun operatore è personalmente responsabile dei dati trattati e delle risorse informatiche a lui affidate, nonché dell'utilizzo appropriato delle risorse stesse.
Tutti gli strumenti informatici, intranet, Internet e posta elettronica messi a disposizione dell'utente dall'Azienda sono strumenti di lavoro e come tali possono essere utilizzati solo per scopi strettamente professionali e lavorativi. Ciascun utente, dunque, è tenuto ad usarli esclusivamente per ragioni di servizio, in linea con quanto previsto dal vigente impianto legislativo, contrattuale e regolamentare.
Pertanto l'operatore, oltre a non dover compromettere la sicurezza, integrità, la disponibilità e la riservatezza del sistema informativo, non deve utilizzare per fini privati materiale ed attrezzature di cui dispone per ragioni di ufficio.
Comportamenti difformi rispetto a quanto previsto dal presente regolamento espongono l'utente a responsabilità disciplinare – qualora dipendente – ed in ogni caso penale e civile, con conseguente risarcimento di eventuali danni causati all'Azienda ed a terzi.

7 Norme comportamentali per la gestione degli strumenti informatici

7.1 Disposizioni di carattere generale

Per strumenti informatici si deve intendere l'insieme di dispositivi fisici: postazioni di lavoro ("PdL" – PC, laptop), tablet, smartphone, stampanti, lettori portatili ed altri apparati, messi a disposizione degli operatori per il perseguimento delle finalità aziendali. Ad ogni dispositivo è associato un numero di inventario, un identificativo dell'utente assegnatario e l'ubicazione fisica, al fine di catalogare il parco dispositivi aziendale e definire le responsabilità in caso di furto, smarrimento o guasto volontario.
La U.O. Sistemi Informativi (UOASSI) valuta periodicamente lo stato di obsolescenza del materiale affidato e implementa dei piani di sostituzione del medesimo.
In caso di trasferimento ad altra unità, tutti i dispositivi assegnati all'operatore restano in uso presso la struttura originaria, salvo esplicita autorizzazione congiunta, del responsabile della struttura coinvolta e del responsabile della UOASSI.
Nel caso in cui si abbia la necessità di operare l'assegnazione di un determinato dispositivo ad un altro reparto, si deve acquisire il parere favorevole dei responsabili dell'Area Gestione del Patrimonio e della UOASSI ed informare l'amministratore di sistema allo scopo di consentirne la tracciabilità.
Qualora se ne ravvisi la necessità, i dispositivi possono anche essere utilizzati in condivisione con altri operatori dell'Azienda, con espressa avvertenza che, in tale frangente, dovranno essere previste sessioni individuali di lavoro per ciascun utente e specifiche credenziali di identificazione ed autenticazione.
Le PdL sono fornite agli utenti con una configurazione software predefinita che non può essere modificata dai medesimi autonomamente. La configurazione dei profili abilitativi di tutti gli utenti aziendali è eseguita con privilegi che non consentono l'installazione o l'esecuzione di programmi non autorizzati sulle macchine client e sui server.
Nell'uso dei dispositivi informatici quali strumenti di lavoro, l'utente è tenuto alle seguenti disposizioni di carattere generale:

- ✓ Custodire con cura e diligenza i dispositivi fisici per evitare la sottrazione, la distruzione o il danneggiamento. Utilizzare sistemi di cifratura dei dati personali, al fine di evitare l'accesso di soggetti non autorizzati in caso di furto o smarrimento.
- ✓ Preservare l'integrità delle informazioni e dei dati contenuti nei dispositivi.
- ✓ Utilizzare gli strumenti fisici con consapevolezza, appropriatezza e professionalità, unicamente per finalità compatibili con le attività aziendali.
- ✓ In caso di furto, smarrimento o incidente di sicurezza, effettuare segnalazione immediata – nel termine massimo di 24 ore dal momento in cui si è venuti a conoscenza dell'evento – al Titolare e al Responsabile della Protezione dei Dati aziendale (DPO), al fine di attivare la procedura aziendale per il data breach, pubblicata in intranet nella sezione privacy. Tale adempimento è indispensabile sia per registrare quanto accaduto al dispositivo, sia per ottemperare agli obblighi imposti dal regolamento UE 2016/679 per quel che concerne le eventuali notifiche al Garante ed agli interessati, sia per sporgere le eventuali denunce agli organi competenti.
- ✓ È fatto assoluto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi, di rimuovere, danneggiare o asportare componenti hardware, ovvero di modificare la configurazione hardware e software del proprio dispositivo.
- ✓ Non è consentito l'uso di strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche.

7.2 Disposizioni sull'utilizzo di PdL e dispositivi mobili

Le PdL e i dispositivi mobili sono strumenti di lavoro affidati agli operatori, di cui i medesimi sono responsabili sia per la parte hardware sia per quella software. Tali strumenti devono essere adoperati solo per finalità attinenti l'attività lavorativa; eventuali informazioni salvate su di essi – anche temporaneamente – devono essere pertinenti con la propria attività lavorativa. Ogni uso improprio può contribuire ad innescare disservizi, costi di assistenza e manutenzione e, soprattutto, minacce alla sicurezza dell'intera rete aziendale o delle reti telematiche e dei sistemi informatici di terzi, esponendo ASL BA ed eventuali terzi a crimini informatici. Pertanto, è vietato connettere alla rete aziendale qualsiasi dispositivo che non appartenga ad ASL BA, senza preventiva autorizzazione dell'Azienda stessa, del responsabile

UOASSI e dell'amministratore di sistema. È proibito, altresì, l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dagli amministratori di sistema; l'inosservanza di quest'obbligo, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre a gravi responsabilità civili, oltre che penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.

Inoltre, prima della riconsegna degli strumenti per restituzione o riparazione, è fatto obbligo agli assegnatari di cancellare eventuali file elaborati o utilizzati, nonché di rimuovere tutti i dati personali eventualmente presenti; particolare attenzione deve essere prestata in caso di un uso temporaneo di dispositivi mobili.

La UOASSI ha facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza aziendale ovvero acquisito o installato in violazione delle presenti disposizioni.

Qualora l'operatore sia costretto ad assentarsi dal luogo in cui è ubicata la PdL o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima, egli è tenuto ad eseguire lo spegnimento, il blocco o il log-out dalla sessione di lavoro; lasciare incustodita la postazione di lavoro con la sessione utente attiva può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne, in seguito, l'indebito uso.

Le PdL e gli altri dispositivi devono essere spenti ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

Come già precedentemente regolamentato, il disco fisso locale di ciascuna PdL deve essere adoperato unicamente ai fini della memorizzazione di file di interesse aziendale. Tale memorizzazione deve essere limitata a poche ore lavorative, atteso che questi dischi non sono sottoposti a backup.

Tutti i file di rilevanza aziendale devono essere salvati nell'area personale, riservata a ciascun utente, o nell'area della struttura di appartenenza da prevedersi nell'ambito del cloud aziendale. È opportuno prevedere una pulizia periodica di tali archivi, con cadenza almeno semestrale, in quanto deve essere assolutamente evitata la conservazione in rete di file obsoleti, ridondanti o inutili e, per questo stesso motivo, si invita anche ciascun operatore ad un attento ed ordinato utilizzo dello spazio di rete.

Il regolamento UE 2016/679 stabilisce che ogni file contenente dati che ricadono nelle categorie particolari deve essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni da parte di soggetti diversi da quelli autorizzati.

Nello specifico, i dati archiviati, appartenenti alle categorie particolari, possono essere conservati per un periodo non superiore a quello necessario ad adempiere gli obblighi o i compiti istituzionali.

Qualsiasi file non attinente all'attività lavorativa, se non espressamente autorizzato, non può essere memorizzato sulle PdL nemmeno transitoriamente e, tanto meno, nelle aree aziendali dedicate.

La competenza e la gestione delle aree di memorizzazione di struttura è attribuita ai responsabili di ciascuna area. I privilegi di lettura e scrittura delle cartelle di rete sono definiti dal responsabile di ciascuna struttura o suo delegato, valutando il bilanciamento delle esigenze della produttività e della necessaria riservatezza. Non è ammessa la modifica dei permessi di accesso alle cartelle da parte degli operatori.

I responsabili di struttura, qualora ne ravvisino la necessità, richiedono la messa a disposizione, da parte della UOASSI, di cartelle di rete per determinati utenti afferenti alla loro struttura. Tali utenti si attengono alle modalità operative impartite dai loro responsabili di struttura e utilizzano in maniera esclusiva e riservata le aree condivise, per il solo salvataggio dei dati di natura strettamente aziendale.

A chiusura del rapporto di lavoro, l'Area Gestione Risorse Umane notifica l'interruzione del rapporto alla UOASSI indicandone la tipologia: cessazione o sospensione. Fatte salve specifiche indicazioni, richieste e casi particolari che verranno opportunamente esaminati, entro 3 giorni dal ricevimento della comunicazione, il personale della UOASSI procede alla variazione dei permessi della cartella di rete concessa in maniera esclusiva, affinché sia consentito al responsabile di struttura, o altra figura delegata, di effettuare l'accesso ai file contenuti per l'esecuzione di eventuali backup.

Per i soli di casi di cessazione del rapporto di lavoro per mobilità in uscita, pensionamento, dimissioni o decesso, trascorsi ulteriori 60 giorni – periodo stimato congruo e non eccedente a garantire l'operatività e la continuità di servizio – salvo diverse indicazioni degli assegnatari o dei responsabili, specifiche richieste e casi particolari che verranno opportunamente vagliati, il personale della UOASSI procede alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva, e non sarà più possibile recuperare i dati in essa contenuti.

I dati immagazzinati nelle menzionate aree in sharing, che sono parte integrante dello storage aziendale, devono essere protetti da opportune procedure di backup automatico, debitamente gestite e monitorate.

7.3 Disposizioni sull'utilizzo di supporti rimovibili

Premesso che, generalmente, l'uso di supporti di memorizzazione rimovibili è da evitarsi, si precisa quanto segue. È obbligatorio che tutti i file di provenienza incerta o esterna siano sottoposti a controllo antimalware, prima di essere aperti o comunque utilizzati. Se il programma antivirale aggiornato rileva anomalie, si deve avvertire immediatamente il personale della UOASSI.
Sui supporti rimovibili non devono essere conservati, nemmeno temporaneamente, file aziendali insieme a file personali. In ogni caso, non è mai consentito scaricare o copiare file in supporti rimovibili esterni che non siano attinenti alla propria attività lavorativa.
Nel caso in cui si riceva in assegnazione un dispositivo di memoria esterno USB, il suo impiego è autorizzato solo se:

- ✓ Il dispositivo è stato preventivamente cifrato con Bitlocker o VeraCrypt.
- ✓ L'assegnatario si impegna a non scaricare i file contenuti nella memoria USB su dispositivi diversi da quelli aziendali.
- ✓ L'assegnatario si obbliga a non diffondere, né comunicare a terzi per alcuna ragione la chiave di cifratura, a conservarla in luogo protetto – separatamente dal dispositivo stesso – e a non modificare detta chiave, senza previa ed esplicita autorizzazione della UOASSI.

Se si salvano su supporti removibili dei dati – siano essi riservati o meno – è obbligatorio conservare, custodire e controllare tali supporti, affinché nessun soggetto terzo non autorizzato ne prenda visione o possesso. L'assegnatario è l'unico responsabile della custodia dei supporti e dei dati in essi contenuti.
I supporti rimovibili su cui siano presenti dati appartenenti alle categorie particolari previste dal regolamento UE 2016/679 o comunque riservati, devono essere protetti con sistemi di crittografia, avendo cura di permettere la lettura solo agli aventi diritto, ovvero, in mancanza, utilizzare sistemi di pseudonimizzazione o sistemi di anonimizzazione.
Tali dispositivi devono essere custoditi dagli utenti con le medesime modalità imposte per la documentazione cartacea contenente la stessa tipologia di informazioni.

I supporti rimovibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto, o, successivamente alla cancellazione, recuperato. Qualora i dispositivi non siano più utilizzati, devono essere consegnati alla UOASSI per il loro corretto ricondizionamento o dismissione.

7.4 Disposizioni per la firma digitale

È obbligo di ciascun assegnatario di dispositivi di firma digitale:

- ✓ Utilizzare personalmente il dispositivo di firma.
- ✓ Custodire i codici di accesso PIN e PUK e non comunicarli a nessuno.
- ✓ Assicurare la custodia del dispositivo di firma e degli eventuali strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, nonché adottare tutte le misure organizzative e tecniche idonee ad evitare danni a terzi.

7.5 Disposizioni sull'utilizzo di stampanti e fotocopiatori

La stampa di documenti deve essere limitata ai casi per cui esiste l'assoluta necessità di disporre della copia cartacea per lo svolgimento dell'attività lavorativa. Il materiale stampato non deve essere lasciato incustodito e deve essere ritirato immediatamente, in modo che non si trovi nella disponibilità di persone non autorizzate.
In caso di stampante condivisa, qualora possibile, si deve attivare la funzione che genera un PIN da digitare sulla stampante per consentire la stampa al momento del ritiro.
Nelle stampanti multifunzione, la scansione dei documenti potrebbe venir configurata come invio del documento digitalizzato ad una casella di posta oppure come salvataggio delle scansioni su una cartella locale della multifunzione o su una cartella di rete. In caso di utilizzo secondo la prima modalità, è vietato l'invio di scansioni dalla multifunzione verso email non aziendali. Qualora si desideri inviare una scansione ad un soggetto non appartenente all'Azienda, è necessario inoltrare in primo luogo il documento alla propria email istituzionale; solo dopo averne verificato il contenuto, si potrà inoltrare l'allegato al destinatario, adoperando tassativamente il proprio account di posta elettronica.

La modalità di scansione su disco potrebbe indirizzare i documenti acquisiti nella memoria interna del dispositivo, oppure in una cartella condivisa. In entrambi i casi, l'utente ha l'obbligo di cancellare o spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile, al fine di non rendere noto a terzi il contenuto dei file acquisiti.

7.6 Disposizioni di sicurezza e privacy per lo smart-working

L'Azienda può prevedere, per alcuni operatori, la possibilità di accedere alle proprie risorse informatiche dall'esterno mediante rete VPN (Virtual Private Network), intesa come un canale privato e criptato verso la rete interna; ciò è quanto accade, per esempio, nel caso di concessione dello smart-working.
In questa fattispecie l'utente è tenuto, comunque, a conformarsi a tutti gli obblighi di sicurezza previsti nel presente regolamento, per quanto compatibili.
Conseguentemente l'utente abilitato ad accedere alle risorse informatiche aziendali dall'esterno deve:

- ✓ Utilizzare il dispositivo aziendale solo ed esclusivamente per le attività lavorative.
- ✓ Collocare la propria postazione lavorativa in uno spazio idoneo, da utilizzare in modo esclusivo, ponendo la massima attenzione per impedire che ai dati possano accedere persone non autorizzate.
- ✓ Verificare che la postazione individuata sia sicura da un punto di vista ambientale.
- ✓ Verificare la conformità delle prese elettriche scelte per alimentare il dispositivo o i dispositivi aziendali.
- ✓ Non lasciare incustodita la postazione di lavoro e, al termine di ogni sessione lavorativa, posizionare gli strumenti di lavoro in un luogo sicuro.
- ✓ In caso di allontanamento dalla propria postazione di lavoro, anche per un lasso di tempo molto limitato, bloccare la PdL.
- ✓ Adoperare meccanismi di sicurezza, quali cifratura dei dati e password, che impediscano l'accesso ai dati a chi dovesse entrarne in possesso.
- ✓ Adoperare misure di sicurezza nell'uso dei dispositivi che impediscano la visuale laterale al vicino.

- ✓ Non caricare documenti aziendali riservati ovvero dati personali su sistemi di memorizzazione esterni cloud quali Google Drive, o altre simili o, comunque, su piattaforme diverse da quella aziendale o indicata da ASL BA. Ciò in quanto tali sistemi possono essere soggetti ad attacchi informatici e i dati possono essere sottratti o manipolati illegalmente. A ciò si aggiunga che molti di tali sistemi sono ospitati in paesi non soggetti a regolamentazioni sulla privacy analoghe a quella italiana.
- ✓ Al termine della prestazione lavorativa giornaliera, conservare e proteggere i documenti eventualmente stampati, eseguendo la loro eventuale distruzione con particolare attenzione, in modo da non renderli più ricostruibili.

Nel caso in cui l'utente sia stato autorizzato all'impiego di un dispositivo client remoto di sua proprietà, egli deve comunque attenersi alle seguenti disposizioni, per garantire il medesimo livello di sicurezza dei dispositivi client aziendali:

- ✓ Adoperare solo dispositivi client con sistemi operativi per i quali è garantito l'aggiornamento.
- ✓ Eseguire costantemente gli aggiornamenti di sicurezza del sistema operativo del dispositivo client.
- ✓ Installare un adeguato sistema antimalware da tenere costantemente aggiornato.
- ✓ Collegare supporti rimovibili solo se si conosce la loro provenienza e, in ogni caso, effettuare preventivamente una scansione.
- ✓ Non utilizzare il dispositivo impiegato per lo smart-working per l'uso di social network o altre applicazioni social facilmente aggredibili.
- ✓ Verificare che gli accessi al sistema operativo siano protetti da password sicura, conforme alle disposizioni del presente regolamento.
- ✓ Non installare sul dispositivo in questione software proveniente da sorgenti o repository non ufficiali.
- ✓ Consentire l'accesso solo a reti adeguatamente protette.
- ✓ Non utilizzare PC pubblici o comunque di terzi, né reti wifi pubbliche, le quali possono essere un mezzo che consente di condurre più facilmente attacchi.
- ✓ Effettuare sempre il logout dai servizi utilizzati, dopo che si è conclusa la sessione lavorativa.

- ✓ Non cliccare su collegamenti o allegati contenuti in email sospette.
- ✓ Utilizzare strumenti di crittografia in caso di condivisione di dati particolari per posta elettronica.

I canali di accesso permessi tra il dispositivo dell'utente ed il server aziendale sono solo connessioni sicure tramite VPN Virtual Private Network. Nel caso in cui la connessione venga adoperata per attività che comportano il trattamento di dati personali, i medesimi non potranno essere prelevati dal sistema informativo aziendale e memorizzati sulla postazione di lavoro da cui ha origine la VPN senza esplicito consenso scritto del Titolare degli stessi, nella persona del Direttore Generale di ASL BA.
Le connessioni VPN comportano la registrazione degli accessi in file di log, ossia di alcune informazioni tra cui nome utente, indirizzo IP di provenienza e orari in cui tali operazioni sono state effettuate, per finalità di tutela della sicurezza, riservatezza ed integrità dei dati aziendali trattati.
In relazione alla concessione di un accesso VPN, l'utente si impegna a:

- ✓ Accedere esclusivamente ai servizi e ai sistemi informativi di ASL BA ai quali è stato espressamente autorizzato e a farlo secondo le modalità consentite.
- ✓ Garantire, sotto la propria personale responsabilità, il mantenimento della necessaria riservatezza sulle proprie credenziali.
- ✓ Comunicare immediatamente alla UOASSI lo smarrimento, il furto o l'appropriazione da parte di terzi delle proprie credenziali.
- ✓ Segnalare immediatamente qualsiasi incidente o malfunzionamento dei sistemi di collegamento in VPN.
- ✓ Bloccare la propria postazione informatica in tutte le occasioni in cui ci sia necessità di allontanamento anche temporaneo dalla stessa.
- ✓ Non recare danno o pregiudizio ai dati o ai software in uso presso gli uffici di ASL BA e a non interferire con l'utilizzo dei servizi di rete da parte di altri utenti.
- ✓ Adoperare le credenziali assegnate ai soli fini di fruizione dei servizi per i quali è stata concessa autorizzazione.
- ✓ Non condividere le proprie credenziali con terzi per nessuna motivazione.

- ✓ Disconnettere immediatamente la connessione VPN non appena terminate le attività lavorative necessarie.
- ✓ Rispettare la vigente normativa posta a tutela della riservatezza e dei dati personali.

L'amministratore di sistema è tenuto al controllo della sicurezza delle postazioni di lavoro esterne remote, negando o interrompendo l'accesso alla rete agli utenti che utilizzino dispositivi non adeguatamente protetti o aggiornati che possano costituire una concreta minaccia per la sicurezza informatica di ASL BA.

8 Norme comportamentali per l'uso della rete locale (LAN) e Internet

La rete locale, basata su protocollo TCP/IP, è una risorsa strategica per ASL BA in quanto connette ciascun dispositivo e permette lo scambio di informazioni tra di essi. Ogni disservizio o interruzione comporta notevoli disagi per l'operatività dell'Azienda, in quanto tutte le PdL operano interconnesse alla LAN e hanno accesso ai dati secondo determinate abilitazioni.
La rete aziendale non può esser utilizzata per finalità differenti da quelle a cui è deputata; l'utente deve osservare i principi di prudenza nella trasmissione di dati personali, come prescritto dal regolamento UE 2016/679, avendo cura di non assumere comportamenti che possono procurare rischi per l'integrità, la riservatezza e la disponibilità delle informazioni aziendali. Pertanto è fatto divieto assoluto di accedere alla rete con un codice d'identificazione di un altro operatore, alterare la configurazione di rete dei dispositivi, nonché scaricare, copiare, distribuire documenti, o altro, in violazione delle leggi sul diritto di autore.
Qualora un utente si accorga che nella rete interna circolano dati o informazioni non attinenti all'attività lavorativa o che costituiscono illecito, è obbligato, immediatamente, a darne notizia al proprio responsabile e alla UOASSI; la medesima strategia deve essere adottata nel caso in cui il software antimalware rilevi la presenza di anomalie.
È vietato compiere atti intenzionali che portino, in qualunque modo, alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune.
La configurazione e la gestione di tutti gli apparati attivi e dell'infrastruttura di collegamento sono affidati al personale della UOASSI, congiuntamente a fornitori esterni. Pertanto non è

consentito a chiunque altro l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualsiasi impianto o cavo.
Non è permessa in nessun caso la connessione alla rete aziendale di apparati destinati a realizzare connessioni con altre reti verso l'esterno quali, ad esempio, router, bridge, impianti wireless ed altri ancora.
Un eventuale impiego di tali apparati, se indispensabile, dovrà essere richiesto alla UOASSI e sarà vincolato all'autorizzazione del Direttore competente; parimenti non è consentito l'impiego di dispositivi per la duplicazione dei punti rete.
È assolutamente proibito collegare in rete qualsiasi dispositivo informatico, se non a valle di formale autorizzazione della UOASSI. È di tutta evidenza, infatti, che la connessione di un device non autorizzato, potrebbe causare un conflitto di indirizzo IP con un server o qualsiasi altro dispositivo della rete e generare gravi malfunzionamenti della medesima.
È assolutamente proibito configurare servizi messi a disposizione in modo centralizzato quali ad esempio, DHCP, DNS, nonché aggiungere protocolli di rete o servizi per la condivisione di stampanti in rete, il browsing di risorse di rete e altro ancora.
È fatto assoluto divieto di intercettare ed analizzare i pacchetti in transito sulla LAN, utilizzando sniffer sia software che hardware. Queste operazioni sono consentire solo al personale tecnico della UOASSI, mediante analyzer, e al solo fine di monitorare le prestazioni della rete.
Se il personale della UOASSI rileva la presenza di un dispositivo che genera traffico anomalo o che danneggia le prestazioni dell'intero sistema, ha facoltà, previ doverosi riscontri, di eseguire il blocco selettivo di tale attività.
A completamento della rete locale menzionata, alcune strutture di ASL BA dispongono anche di una wireless LAN. Tramite un insieme di access point viene distribuito l'SSID: "ASL-BA".
La rete wifi costituisce un'estensione non cablata della rete locale, quindi, i client ad essa connessi possono accedere alle stesse risorse. È assolutamente vietato collegarsi a tale infrastruttura con dispositivi che non siano aziendali, e che non siano stati precedentemente configurati dalla UOASSI.
Le PdL abilitate alla navigazione in Internet sono uno strumento per l'espletamento dell'attività lavorativa. Conseguentemente è proibito accedere a siti il cui contenuto non sia pertinente con la medesima. Per impedire agli utenti la navigazione Internet non consona, si rende noto che è previsto l'uso un sistema di protezione che prevede il filtraggio automatico

del traffico per categorie di contenuti ed è inoltre presente la funzionalità di gestione di specifiche blacklist di url.
Non è consentito scaricare o copiare file o software di qualsiasi natura accedendo abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza. Si precisa che il download di qualsiasi file ricade nella responsabilità esclusiva dell'utente che lo esegue e deve essere necessariamente preceduto da un'analisi volta a prevenire azioni malevole che possano minare l'integrità del patrimonio aziendale.
Non è consentito l'uso di programmi di file sharing, di programmi peer-to-peer, di social network e di servizi di messaggistica istantanea, ad esclusione di quelli esplicitamente autorizzati dall'Azienda, nonché la registrazione e partecipazione a forum non professionali.
È tassativamente proibita l'esecuzione di qualsivoglia genere di transazione finanziaria, comprese le operazioni di remote banking, acquisti online e simili, eccezion fatta per le fattispecie direttamente autorizzate dai Direttori competenti che, comunque, si svolgano in ossequio alle ordinarie procedure di acquisto.
Non è ammessa alcuna attività legata ad azioni di pirateria informatica o hacking.
Atteso che le apparecchiature, i servizi e le tecnologie utilizzati per accedere a Internet sono beni aziendali, si comunica che potranno essere eseguiti eventuali controlli sul traffico Internet, mediante file di log della navigazione svolta.
Tali log sono indispensabili all'Azienda per il perseguimento di finalità organizzative e di sicurezza e saranno trattati in maniera tale da fornire informazioni in maniera aggregata, precludendo l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni per accedere alle informazioni di tipo nominativo.

9 Attribuzione degli account e gestione delle password

La sicurezza delle informazioni prevede che l'accesso ai dati deve essere consentito solo a quegli utenti che ne abbiano necessità per l'espletamento di attività legittime. Pertanto, in modo coerente con le prescrizioni del regolamento UE 2016/679 e del Garante per la protezione dei dati personali, ciascun sistema informatizzato deve prevedere la possibilità di definire profili di abilitazione, tramite i quali dettagliare i privilegi dei differenti ruoli professionali in termini di funzionalità eseguibili e di dati accessibili.

Ad ogni operatore si attribuisce un'identità digitale aziendale, costituita da credenziali di accesso, cui vengono associati specifici permessi di accesso ai dati, in virtù del ruolo, del reparto o unità di appartenenza e delle attività permesse.
Tali credenziali sono costituite da un identificativo univoco dell'utenza, lo userId, e da una password da cambiare obbligatoriamente al primo accesso ed al massimo ogni sei mesi, ovvero ogni tre mesi se i dati trattati sono particolari e o giudiziari.
L'account utente è lo strumento per l'autenticazione dell'operatore nel sistema informatico e, quindi, ciò che regola l'accesso alle risorse informatiche aziendali. Conseguentemente gli operatori devono accedere alle risorse informatiche ed alla rete solo ed esclusivamente con le proprie credenziali di identificazione ed autenticazione, le quali sono strettamente personali e non cedibili. Quest'ultime devono essere gestite in modo tale da garantirne la segretezza, ossia devono essere mantenute strettamente riservate e vanno custodite con cura e diligenza. Pertanto gli utenti sono obbligati ad osservare le seguenti disposizioni:

- ✓ Cambiare la password al primo accesso ed ogni volta che viene richiesto dal sistema (al massimo ogni 6 mesi o 3 mesi se i dati trattati sono particolari e o giudiziari), ovvero in caso vi sia il dubbio che ne sia stata violata la segretezza.
- ✓ Evitare la digitazione in presenza di terzi e la conservazione in luogo accessibile ad altri.
- ✓ Non condividere le proprie password con nessuno compresi colleghi, amministratori e assistenti tecnici, né rivelare la password al telefono, o inviarla via email.
- ✓ Evitare di trascrivere le proprie password su qualsiasi tipo di supporto, digitale o cartaceo.
- ✓ Avere cura di evitare di essere vittima di truffe online mirate al furto di credenziali di accesso o altri dati personali.
- ✓ In caso di smarrimento e o furto della password o se si rilevino accessi non autorizzati a sistemi che trattano dati personali, darne immediata comunicazione al proprio responsabile ed al DPO e, se necessario, attivare la procedura di data breach aziendale.
- ✓ Non tentare di acquisire i privilegi di amministratore di sistema.

L'obiettivo principale che bisogna prefiggersi nel definire la propria password è quello di rendere quanto più difficile possibile il tentativo di terze parti di indovinarla o ricostruirla.

Quindi ogni operatore, nell'individuazione della propria password, deve rispettare quanto segue:

- ✓ Le password devono avere una lunghezza di almeno 8 caratteri e devono essere formate dalla combinazione di caratteri alfabetici (almeno un carattere maiuscolo ed uno minuscolo), numerici (almeno un carattere) e di simboli come ad esempio @, $£! (almeno un carattere).
- ✓ Non utilizzare più di due caratteri consecutivi identici.
- ✓ Non utilizzare sequenze di cifre consecutive.
- ✓ Non utilizzare elementi o informazioni semplicemente associabili al possessore: per esempio, la password non deve contenere il nome dell'utente, o la sua userId, o in generale parole allo stesso riferibili quali, ad esempio, il nome dei genitori, il nome della moglie o dei figli, il luogo o la data di nascita, il numero di matricola, il numero di telefono e così via.
- ✓ Non deve essere costruita su parole di uso comune quali, ad esempio, personaggi, nomi di luoghi, mesi, giorni della settimana e così via.
- ✓ Non deve essere uguale ad una delle ultime 5 già utilizzate.
- ✓ Non impiegare per il proprio account lavorativo una password già usata per un account personale.
- ✓ Modificare immediatamente la password ogniqualvolta si abbia il sospetto che possa essere stata violata.

Si rende noto che la mancata osservanza delle istruzioni inerenti la riservatezza delle credenziali di autenticazione danneggia l'intero sistema di gestione dei profili utente ed ha gravi ricadute sulla sicurezza dell'intero sistema.
In caso di interruzione, a qualsiasi titolo, del rapporto di lavoro con ASL BA, è fatto divieto agli operatori di continuare ad usare i propri account che devono essere disattivati.
Le credenziali di autenticazione sono revocate quando viene meno la necessità di disporre delle risorse o delle informazioni aziendali concesse; è il caso, ad esempio, di cambiamento di mansioni o spostamento in altra unità o reparto.
Il sistema informativo aziendale traccia tutte le operazioni svolte da ciascun utente, identificato tramite le sue credenziali di accesso, inclusi gli accessi da remoto mediante VPN,

registrando in uno specifico file di log ogni azione compiuta dal medesimo: accesso ai dati, modifica dei dati, uso di risorse informatiche aziendali locali o remote e altre ancora.
I file di log possono essere oggetto di esame da parte dell'amministratore di sistema per individuare eventuali responsabilità in caso di errore o violazioni di legge.

10 Norme comportamentali per la gestione della posta elettronica

Il servizio di posta elettronica ordinaria (PEO) è fornito da ASL BA per consentire la comunicazione, l'amministrazione ed altre attività strumentali correlate ai fini istituzionali.
Il servizio è subordinato all'osservanza integrale delle condizioni di seguito riportate. L'utilizzo del servizio da parte dell'utente costituisce implicita accettazione delle condizioni menzionate.

Un account di posta elettronica ordinaria prevede uno username, una password ed un indirizzo di posta associati ad un determinato spazio disco.

Sono assegnati account PEO agli organi, alle strutture ed articolazioni aziendali centrali e periferiche (PP.OO. e DD.SS.SS.), alle aree di gestione, agli uffici di staff e alle unità aziendali. Tali account sono condivisi dagli operatori assegnati a ciascuna di esse e hanno formato del tipo: nomeservizio@asl.bari.it (es. uoassi@asl.bari.it).

Al personale dipendente in servizio attivo sono assegnati indirizzi di posta aziendali personali aventi il formato: nome.cognome@asl.bari.it, con eccezioni previste per i casi di omonimia.

L'attivazione dell'account avviene, a cura dell'amministratore del sistema, su richiesta scritta autorizzata dal Dirigente responsabile della struttura, dopo verifica dei requisiti richiesti. La richiesta deve essere sottomessa all'indirizzo **mail-desk@asl.bari.it**.

Le persone assegnatarie delle caselle si impegnano a salvaguardare, anche in modo proattivo, la riservatezza delle password ed a segnalare qualsiasi violazione. Ciascuno è responsabile dell'attività espletata mediante il proprio account.

Il carattere personale degli account non implica assolutamente la facoltà di uso per scopi privati, atteso che si tratta di strumenti di esclusiva proprietà aziendale, messi a disposizione di ciascuno al solo fine dello svolgimento delle proprie mansioni lavorative.

L'invio tramite posta elettronica di dati appartenenti alle categorie particolari, in ossequio al regolamento UE 2016/679, deve essere eseguito sotto forma di file allegato e non come corpo del messaggio. In particolare, poi, tale allegato dovrà essere protetto con modalità idonee a impedirne l'illecita o fortuita acquisizione da parte di soggetti diversi dal destinatario. In base alla normativa vigente, le misure da mettere in atto possono essere costituite da una password per l'apertura del file o da una chiave crittografica, rese note agli interessati attraverso una distinta comunicazione (ad esempio per lettera o per telefono).

10.1 Doveri, divieti, limiti di utilizzo e responsabilità dell'utente

L'account PEO assegnato ai dipendenti da ASL BA è uno strumento di lavoro di proprietà aziendale concesso in uso agli operatori per un più proficuo svolgimento della prestazione. Pertanto gli assegnatari sono responsabili del corretto utilizzo delle caselle di posta. Ciascuno è responsabile del contenuto dei messaggi inviati; per garantire la sicurezza dei sistemi informativi aziendali, è vietato avvalersi delle caselle di posta assegnate, per l'invio di messaggi personali o di contenuto extra lavorativo, eccezion fatta per l'esercizio dei diritti normativamente tutelati per l'invio e la ricezione di informazioni di natura sindacale.

Ciascun assegnatario si impegna a gestire quotidianamente la propria casella di posta, non solo aprendo e leggendo i messaggi, ma anche monitorando costantemente l'occupazione di spazio per non superare il limite consentito. L'assegnatario si obbliga, altresì, a non utilizzare il servizio per scopi illegali o difformi dal presente regolamento o che, comunque, possano recare danno o pregiudizio ad ASL BA o a terzi. Inoltre egli deve utilizzare il servizio in modo da non danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo da parte di altri operatori.

L'operatore si assume ogni responsabilità civile e penale derivante dall'uso improprio del servizio e, fin d'ora, esonera ASL BA da qualsiasi azione o pretesa che da ciò possa scaturire.

L'assegnatario non può assolutamente adoperare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato, messaggi che costituiscano:

- ✓ Materiale discriminatorio per sesso, lingua, religione, razza, origine etnica, opinioni e appartenenza sindacale o politica.
- ✓ Materiale pornografico o pedopornografico, in particolare in violazione della Legge 269/1998 – "Norme contro lo sfruttamento sessuale dei minori degli anni 18".
- ✓ Violazione della normativa vigente sulla protezione dei dati personali.
- ✓ Violazione dei diritti di proprietà di terzi.
- ✓ Altri contenuti illegali o diffamatori.
- ✓ Comunicazioni commerciali private.
- ✓ Pubblicità non istituzionale, manifesta o occulta.

Non è consentito all'operatore provare ad accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.
È assolutamente proibito usare la posta elettronica per diffondere codici dannosi per i computer quali malware e simili.
Nel caso di messaggi provenienti da mittenti sconosciuti o dal contenuto insolito, prima di aprirli, è obbligatorio ispezionarli con una verifica approfondita e, nell'eventualità, cancellare i messaggi senza aprirli per non rischiare di essere infettati da codice maligno. Se tali messaggi contengono allegati sospetti, aventi estensione .exe .scr .pif .bat .cmd .msi o altri non noti, è vietato non solo salvarli ed eseguirli, ma anche semplicemente aprirli. In ogni caso, l'accaduto dovrà essere notificato al personale della UOASSI e all'amministratore di sistema.

L'assegnatario si impegna a non diffondere messaggi di natura ripetitiva quali, ad esempio, catene di varia denominazione. Ciò anche quando il contenuto abbia come finalità la segnalazione di veri o presunti allarmi per virus o altro. In quest'ultima evenienza l'operatore dovrà limitarsi a contattare la UOASSI.

È fatto divieto assoluto di comunicare a terzi informazioni confidenziali, segrete o che siano comunque di rilievo per ASL BA e per la sua attività, nonché di qualsiasi altra informazione di

natura riservata della quale il dipendente sia venuto a conoscenza durante lo svolgimento della propria attività. È vietato divulgare notizie, dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti.

L'assegnatario accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e si assume l'onere di comunicare tempestivamente all'amministratore di sistema, la ricezione di posta indesiderata per le opportune contromisure.

ASL BA si riserva la facoltà di segnalare alle Autorità competenti le eventuali violazioni alle presenti condizioni di utilizzo, per gli accertamenti ed i provvedimenti del caso.
Infine l'assegnatario accetta che l'Azienda possa revocargli l'account, ovvero sospenderne temporaneamente l'utilizzo, per violazione del presente regolamento.
In caso di interruzione del rapporto di lavoro a qualsiasi titolo, l'Area Gestione Risorse Umane notificherà l'evento alla UOASSI specificandone la tipologia: cessazione o sospensione. Salvo diverse indicazioni, specifiche richieste e casi particolari che verranno opportunamente trattati, entro 3gg dal ricevimento della comunicazione, la UOASSI procederà con la disattivazione dell'utenza associata all'account di posta, impedendone l'accesso.

10.2 Posta Elettronica Certificata

Nel caso di messaggi in cui sia necessario conservare la ricevuta di invio, di ricezione o entrambe, risulta essenziale utilizzare la posta elettronica certificata (PEC). La PEC, infatti, è un sistema di comunicazione simile alla PEO, ma tra indirizzi mail certificati, a cui si aggiungono caratteristiche di sicurezza e di certificazione della trasmissione, tali da aggiungere valore legale ai messaggi trasmessi.

La casella PEC è lo strumento attraverso il quale l'azienda trasmette e riceve documenti informatici soggetti a registrazione di protocollo.

Non possono essere concesse caselle di posta certificata personalizzate, a meno di specifiche disposizioni normative o richieste preventivamente autorizzate dal Direttore Generale.

Nell'uso della PEC è obbligatorio, per assicurare la corretta conservazione a norma di legge, allegare esclusivamente determinate tipologie di file, privilegiando, qualora possibile, l'utilizzo del formato PDF/A.

11 Norme per l'uso degli applicativi aziendali

Gli applicativi aziendali sono l'insieme dei software che consentono l'inserimento, la consultazione, l'elaborazione e l'archiviazione dei dati aziendali, sfruttando i dispositivi hardware e la connettività di rete di ASL BA.
Tali applicativi devono assicurare i requisiti di confidenzialità, integrità e disponibilità dei dati, e permettere di ricondurre ciascuna azione ad un singolo operatore, come da previsioni del regolamento UE 2016/679.
Gli utenti e gli amministratori di sistema devono essere in possesso solo delle autorizzazioni strettamente necessarie a portare a termine i loro compiti. E, comunque, ognuno deve astenersi da eseguire operazioni che, ancorché tecnicamente consentite dai sistemi, esulano dalla propria mansione specifica.
Conseguentemente gli applicativi software devono permettere profili di autorizzazione diversi per i differenti ruoli, in modo da consentire che solo alcuni operatori abbiano facoltà di gestire determinati trattamenti o accedere a certi tipi di dato.
Il processo di abilitazione di un utente ad un determinato applicativo aziendale è innescato da un'esplicita richiesta avanzata all'amministratore di sistema dal responsabile dell'unità cui l'operatore appartiene.
Gli ambiti di ciascun trattamento consentito agli addetti devono essere aggiornati periodicamente con cadenza almeno annuale; tale operazione è in carico all'amministratore di sistema con il supporto dei responsabili delle UU.OO.CC..
Per un corretto uso degli applicativi aziendali l'utente deve:

- ✓ Garantire la correttezza del dato, prevenendo il rischio di trattamenti impropri come, ad esempio, nel caso di inserimento di dati non corretti, di mancato inserimento di dati, di accesso a dati non pertinenti e così via.
- ✓ Non utilizzare account assegnati ad altri utenti.

- ✓ Non comunicare ad altri le proprie credenziali personali di autenticazione, anche se solo temporaneamente.
- ✓ Effettuare la pronta segnalazione di qualsiasi malfunzionamento.

12 Manutenzione e assistenza tecnica

Le attività di manutenzione e assistenza tecnica sono espletate da dipendenti, nominati designati al trattamento a cui vengono impartite specifiche direttive ai sensi dell'art. 29 del GDPR, ma anche da professionisti esterni, nominati responsabili esterni del trattamento ai sensi dell'art. 28 del GDPR.
Questi ultimi, cui sono imposti specifici obblighi di riservatezza, devono essere in grado di fornire adeguate garanzie, in modo da assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di assicurare la tutela dei diritti dell'interessato.
A seguito di chiamata da parte di un utente o nell'eventualità di rilevazione di problemi tecnici del sistema informatico, l'amministratore di sistema ed il menzionato personale incaricato del servizio sono autorizzati a compiere interventi nel medesimo sistema per risolvere problemi tecnici o manutentivi, nonché per garantire la sicurezza e la salvaguardia del sistema stesso. Tali interventi tecnici possono anche comportare l'accesso ai dati trattati da ciascun operatore, incluso l'accesso agli archivi di posta elettronica e la consultazione dei siti Internet che sono stati visitati dagli operatori abilitati.
I tecnici di cui trattasi potranno collegarsi e visualizzare da remoto il desktop di singole postazioni, dandone preventiva comunicazione all'interessato, qualora non si pregiudichi la necessaria tempestività e l'efficacia dell'intervento tecnico.

13 Accesso ai dati trattati dagli utenti informatici

ASL BA, in qualità di Titolare del trattamento dei dati personali, informa gli assegnatari di strumenti informatici – eventualmente abilitati ad Internet, posta elettronica, connessione VPN – che i dati personali raccolti per le finalità indicate nel presente regolamento costituiranno oggetto di trattamento nel rispetto della normativa vigente.

Il trattamento dei dati in questione sarà improntato al rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati, esattezza, integrità e riservatezza.
I dati personali degli operatori quali, ad esempio, nome utente, indirizzo IP, registrazione degli accessi in file di log – che contengono informazioni relative agli accessi alle risorse informatiche circa la paternità, l'orario delle operazioni ed altro ancora – saranno trattati esclusivamente per le seguenti finalità:

- ✓ Esecuzione di verifiche per riscontrare il rispetto delle regole previste dal presente documento.
- ✓ Esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale quali, ad esempio, sicurezza del sistema informativo, assistenza tecnica e sistemistica e altro ancora.

Il periodo di conservazione di tali dati dovrà essere pari a 6 mesi.
Si fa presente che l'articolo 23 del D.Lgs. 151/2015 ha riformato l'articolo 4 della Legge 300/1970, al fine di rivedere il divieto dei controlli a distanza, nella consapevolezza di dover tener conto di ulteriori strumenti "dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" e di quelli "utilizzati dal lavoratore per rendere la prestazione lavorativa".
La Suprema Corte di Cassazione ha confermato che le garanzie poste in materia di divieto di controlli a distanza dal secondo comma dell'articolo 4 della Legge 300/1970, si applicano ai controlli difensivi, volti ad accertare comportamenti illeciti dei lavoratori "quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso", stabilendo che sono legittimi quei controlli diretti ad accertare comportamenti illeciti del lavoratore e lesivi del patrimonio aziendale (Cfr. Cass. n. 3122/2015 e Cass. n. 2722/2012).
Pertanto ASL BA ha facoltà di effettuare controlli sugli strumenti informatici adoperati dai dipendenti per rendere la prestazione lavorativa, senza necessità di accordi sindacali preventivi.
I log relativi all'operatività degli strumenti, reperibili nella memoria degli stessi, ovvero sui server o sui router, inclusi i file di log riferiti al traffico web ed alla connessione VPN, sono

registrati e possono essere oggetto di controllo da parte dell'amministratore di sistema. Le informazioni registrate sono utilizzabili per tutte le finalità connesse al rapporto di lavoro.

Si rende noto che il presente regolamento aziendale costituisce adeguata informazione in ordine al trattamento dei dati personali, alle modalità d'uso degli strumenti e di esecuzione dei controlli, ai sensi del regolamento UE 2016/679 e dell'art.4 della Legge 300/1970.

I controlli da remoto saranno eseguiti da ASL BA in conformità della normativa vigente, con particolare riferimento al regolamento UE 2016/679, al D.Lgs. 101/2018, al D.Lgs. 151/2015 ed ai provvedimenti emanati dal Garante.

Le azioni di cui trattasi saranno proporzionate allo scopo e saranno effettuate nel rispetto dei principi di necessità, pertinenza e non eccedenza, proporzionalità e gradualità. Esse saranno condotte in modo da non interferire con i diritti e le libertà fondamentali dei lavoratori e di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

Per quanto possibile i controlli avranno come obiettivo dati aggregati, riferiti ad un'intera unità organizzativa. Tuttavia, nel caso di reiterate anomalie o irregolarità, o di specifiche segnalazioni di attività non conformi alla normativa vigente ed al presente regolamento, saranno effettuati controlli su base individuale. In ogni caso non saranno messe in atto azioni di controllo prolungate, costanti o indiscriminate.

La base giuridica del trattamento dei dati personali è da rinvenirsi:

- Nell'esecuzione di un compito di interesse pubblico.
- Nell'esecuzione del contratto di cui ciascun interessato è parte.
- Nell'adempimento degli obblighi e nell'esercizio dei diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro, in conformità alle norme vigenti in materia.

Per quanto sopra, il conferimento dei dati personali è obbligatorio e, in mancanza, all'utente non potrà essere permesso di avvalersi della strumentazione informatica di lavoro.
I dati saranno trattati da personale dipendente o da altri soggetti che collaborano con l'Azienda, tutti debitamente a ciò autorizzati dal Titolare o da un suo Delegato, nonché da soggetti appositamente designati dal Titolare, quali Responsabili del trattamento dei dati personali. Saranno messe in atto idonee misure tecniche ed organizzative per garantire adeguati livelli di sicurezza.

I dati personali non verranno in alcun modo diffusi, ma potranno essere comunicati all'Autorità Giudiziaria o all'Autorità di Pubblica Sicurezza o ad altri Soggetti, solo nei casi espressamente previsti dalla legge.

I dati personali acquisiti da ASL BA verranno conservati nel rispetto dei termini previsti dalle disposizioni di legge e dalle vigenti procedure di scarto degli archivi documentali.

Gli utenti, in qualità di interessati al trattamento, hanno diritto di:

- Ottenere l'accesso ai propri dati personali ed alle informazioni relative agli stessi.
- Ottenere l'aggiornamento, la rettifica dei dati inesatti o l'integrazione di quelli incompleti.
- Ottenere la cancellazione, nei casi previsti.
- Ottenere la limitazione del trattamento dei dati personali che li riguardano, nei casi previsti.
- Opporsi al loro trattamento, in tutto o in parte, per motivi legittimi.
- Ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che li riguardano forniti al Titolare del trattamento, e hanno diritto di trasmettere tali dati ad un altro Titolare del trattamento.
- Proporre reclamo all'Autorità Garante per la Protezione dei dati personali, qualora ne ricorrano i presupposti, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorità Garante: www.garanteprivacy.it.

Per l'esercizio dei suddetti diritti, i soggetti interessati potranno presentare istanza in forma scritta a:

TITOLARE DEL TRATTAMENTO
AZIENDA SANITARIA LOCALE DI BARI nella persona del Direttore Generale
Sede legale: Lungomare Starita, n°6, 70123 - BARI
Email: direzione.generale@asl.bari.it; Pec: protocollo.asl.bari@pec.rupar.puglia.it

RESPONSABILE DELLA PROTEZIONE DEI DATI
Indirizzo: Lungomare Starita, n°6, 70123 - BARI
Email: dpo@asl.bari.it; Pec: protocollo.asl.bari@pec.rupar.puglia.it

14 Norme comportamentali per la gestione della sicurezza dei sistemi

ASL BA si prefigge l'obiettivo di attuare le misure minime di sicurezza AGID conseguendo, in modo graduale, il livello di implementazione avanzato.

14.1 Back up

Le informazioni, i software e le macchine virtuali residenti sui server aziendali o sui NAS sono protette da procedure di backup automatico gestite e monitorate da un fornitore esterno; la policy attuale prevede backup incrementali sia giornalieri sia settimanali, sulla base di valutazioni circa la criticità e la frequenza di aggiornamento dei dati.
Il backup incrementale salva i dati inseriti o modificati rispetto all'ultimo effettuato; qualora un file abbia subito una cancellazione, può essere ripristinato dai salvataggi. Ogni mese viene eseguita un'archiviazione completa dei dati, intesa come fotografia di quanto presente in quel momento. Questo salvataggio viene mantenuto nei backup per 1 anno. Alla fine dell'anno il salvataggio viene cancellato. Per il ripristino dei dati accidentalmente persi o modificati, è necessario informare tempestivamente la UOASSI.
Al fine di non dare in pasto all'azione di backup, dati ridondanti, si invita coloro che ne hanno responsabilità a mettere in atto una pulizia periodica degli archivi, con cadenza almeno semestrale.

Almeno una copia di ciascun backup deve essere memorizzata su supporto offline, custodito fisicamente in locali ad accesso controllato, in modo da non risultare direttamente accessibile dal sistema da proteggere. D'altro canto, per assicurare il disaster recovery, le copie di backup devono essere replicate in un datacenter secondario o, in alternativa, una replica delle copie offline deve essere custodita in un luogo remoto rispetto all'unico datacenter.

14.2 Protezione da malware

Le informazioni e le infrastrutture informatiche aziendali devono essere inderogabilmente protette da malware. Pertanto è fatto obbligo di installare su tutti gli apparati, sia server sia PdL, opportuni software antimalware che devono essere mantenuti costantemente aggiornati. È compito di ciascun operatore accertarsi che tale software funzioni correttamente, che non siano generati messaggi di mal funzionamenti o segnalazioni della presenza di programmi maligni, oltre a riscontrare che siano realmente eseguiti gli aggiornamenti e che il programma sia attivo nel monitoraggio del dispositivo.
Gli operatori sono invitati a lanciare periodicamente delle scansioni su tutto il disco locale del proprio PC.
Nel caso in cui il programma antimalware rilevi delle anomalie o dei malware, l'utente dovrà sospendere ogni elaborazione in corso, senza spegnere il computer, e segnalare l'accaduto al personale della UOASSI per le opportune verifiche.
L'operatore è obbligato, inoltre, a sottoporre a scansione, mediante il programma antimalware, qualsiasi dispositivo rimovibile di provenienza esterna all'Azienda prima del suo utilizzo.
Infine, qualora si abbia necessità di modificare la configurazione del software antimalware, si deve contattare la UOASSI.

14.3 Sospensione automatica della sessione di lavoro

Su ogni postazione di lavoro deve essere prevista, dopo un tempo minimo di inattività, la sospensione automatica della sessione di lavoro, gestita da policy centralizzata definita dalla UOASSI; ogni PdL deve essere dotata di uno screensaver automatico protetto da password che

oscuri la videata, avviato dal sistema operativo quando sia trascorso un determinato tempo di inattività.
Il tempo minimo di inattività è scelto da ciascuna unità organizzativa in base alle proprie esigenze di servizio.

14.4 Cifratura dei dati

I dati personali salvati su sistemi di archiviazione digitale devono essere cifrati, da ciascun utente, avvalendosi di idonei sistemi di protezione individuati dalla UOASSI. Analogamente, quando vengono trasmessi da un sistema digitale ad un altro, i dati, prima della trasmissione, devono essere criptati con i medesimi sistemi di cifratura.

14.5 Dismissione digitale

In caso di dismissione dei dispositivi o di necessità di riassegnazione dei medesimi ad altro utente, i Direttori delle strutture devono avanzare specifica richiesta alla UOASSI, che si farà carico di quanto necessario. È indispensabile, infatti, mettere in atto un'accurata politica di cancellazione delle informazioni, per prevenire accessi non consentiti ai dati personali in esse contenuti.
In ossequio agli obblighi imposti dal regolamento UE 2016/679 e dal provvedimento del Garante per la protezione dei dati del 13 ottobre 2008, in caso di riuso o dismissione di apparecchiature digitali, occorre cancellare in modo sicuro, definitivo e permanente tutte le informazioni in esse residenti, adottando misure tecniche che consentano di garantire la loro non intelligibilità o l´effettiva cancellazione dei dati, come meglio descritte negli allegati A e B del menzionato provvedimento del Garante per la protezione dei dati.
In merito ai supporti rimovibili contenenti dati particolari o dati giudiziari, i medesimi, se non più impiegati, devono essere distrutti o resi inutilizzabili; conseguentemente, gli stessi possono essere ceduti ad altri soggetti, solo se le informazioni in essi precedentemente contenute non sono più intelligibili, né in alcun modo tecnicamente ricostruibili.
È compito di un fornitore esterno, cui sono impartite precise istruzioni al riguardo, occuparsi della descritta attività di bonifica digitale; il servizio di dismissione digitale è sottoposto alla supervisione dell'amministratore di sistema.

14.6 Trasmissione di dati personali

Per la trasmissione di dati personali, tramite posta elettronica o PEC, riconducibili in particolare allo stato di salute o dati giudiziari degli interessati, devono essere osservate le seguenti istruzioni:

1. Non includere nel contenuto o nell'oggetto del messaggio dati personali riferiti a persone fisiche, se non quelli strettamente indispensabili all'invio dello stesso (es.: indirizzi di posta dei destinatari)
2. Inserire i dati da trasmettere in uno specifico documento da allegare al messaggio (es.: formato Word, Excel, pdf, ecc…)
3. Cifrare il documento mediante opportuno applicativo (7-zip o applicativo equivalente reso disponibile dall'UOASSI) secondo le seguenti indicazioni:
    a. Utilizzare il formato archivio "ZIP";
    b. Selezionare come algoritmo di cifratura (o metodo crittografico) l'opzione "AES-256";
    c. Inserire una password con caratteristiche di sicurezza adeguate;
4. Allegare al messaggio di posta elettronica o PEC il documento in formato ZIP creato (presente nella medesima posizione dei documenti di origine);
5. Comunicare al destinatario la password impostata mediante canale diverso dalla posta elettronica o PEC (es.: SMS, WhatsApp, canale telefonico).

Nel caso in cui l'applicativo di cui sopra non sia già disponibile sulla postazione di lavoro, richiederne l'installazione all'UOASSI.

15 Norme comportamentali per la gestione dei data breach

Per data breach si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" dal Titolare del trattamento.
Atteso che a norma dell'art. 33 del regolamento UE 2016/679 ogni violazione di sicurezza che comporti un rischio per i diritti e le libertà delle persone fisiche deve essere notificata

all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione, ogni utente è obbligato a segnalare immediatamente ogni incidente, seguendo le istruzioni contenute nella Procedura aziendale di gestione della violazione dei dati, pubblicata nella sezione privacy della Intranet aziendale, a cui si rinvia.

16 Conclusioni

Le disposizioni del presente documento sono valide, per quanto compatibili, anche nei casi di connessione alla rete aziendale da postazioni esterne ad ASL BA, nonché per il lavoro agile, anche nel caso sia permesso l'uso di strumenti propri dell'utente.
La violazione degli obblighi espone ogni utente a responsabilità di carattere penale e civile, con conseguente risarcimento di eventuali danni causati all'Azienda e a terzi; se l'operatore è un dipendente di ASL BA, saranno irrogate nei suoi confronti le sanzioni disciplinari previste dal CCNL di categoria e dal Codice disciplinare aziendale, a conclusione del procedimento disciplinare a suo carico.

L'utente manleva ASL BA da qualsiasi danno, perdita e responsabilità, dagli oneri di spesa che dovessero derivare da atti, fatti, comportamenti non corretti o illeciti o omissioni allo stesso imputabili, in quanto è personalmente responsabile sia dell'utilizzo delle risorse ad egli affidate, sia dei dati trattati per finalità aziendali, sia dell'adozione di tutte le misure di sicurezza necessarie a prevenire eventuali violazioni di dati.

Per quanto non previsto dal presente regolamento, si rinvia alle vigenti disposizioni legislative e regolamentari in materia di protezione dei dati personali.

PROFILI CONTABILI

☐ RILEVANTE, a valere su: ☒ NON rilevante

ONERI DI PUBBLICAZIONE OBBLIGATORIA EX D. LGS. 33/2013:

☐ SOGGETTA a pubblicazione ☒ NON soggetta a pubblicazione

ONERI DI RISERVATEZZA:

☐ CONTIENE dati personali da NON pubblicare ☒ NON contiene dati personali

DESTINATARI NOTIFICA/TRASMISSIONE

PROPOSTA N.RO 20220001910 APPROVATA CON DELIBERAZIONE N.RO 20220000850 DEL 09/05/2022

Con la sottoscrizione in calce al presente provvedimento, i firmatari di cui sopra, ciascuno in relazione al proprio ruolo come indicato e per quanto di rispettiva competenza, attestano che il procedimento istruttorio è stato espletato nel rispetto della normativa regionale e nazionale applicabile e che il provvedimento predisposto è conforme alle risultanze istruttorie agli atti d'ufficio.

I medesimi soggetti dichiarano, inoltre, di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale (DDG n. 132/2019) e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, alla Parte II, par. 1, lett. c) del vigente PTPCT – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

RUOLO	NOME E COGNOME	FIRMA
Dirigente PTA	Mangini Francesco Maurizio	*Firmato digitalmente il 03/05/2022 12:10*
DPO Aziendale	Fortunato Elisabetta	*Firmato digitalmente il 03/05/2022 12:12*
Direttore/Responsabile di Struttura	Cisternino Mario Giuseppe Rocco	*Firmato digitalmente il 03/05/2022 19:14*