ver. 2019_01

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Piacenza

Disciplinare sull'utilizzo degli strumenti aziendali e istruzioni in materia di trattamento dei dati personali

*Il presente documento costituisce un disciplinare sull'utilizzo delle attrezzature informatiche e di telecomunicazioni aziendali ai sensi di quanto previsto al punto 3.2 delle "**le linee guida del Garante per posta elettronica e Internet"** e nei provvedimenti del Garante della Privacy inerenti il Trattamento dei dati tramite il dossier sanitario elettronico.*

Sommario

Premessa

Le finalità del Regolamento U.E. 2016/679, applicabile a partire dal 25 maggio 2018, e del D.Lgs. 196/2003 (c.d. Codice Privacy), così come modificato dal D.Lgs 101/2018, in continuità con la normativa previgente, consistono infatti nella tutela dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riguardo al diritto alla protezione dei dati personali, pertanto qualsiasi trattamento di dati personali non può che tenere conto di questi principi fondamentali e degli altri principi fissati all'art. 5 del Regolamento (UE) 2016/679:

- *liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;*
- *limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;*
- *minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;*
- *esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;*
- *limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;*
- *integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.*

(*) Il testo integrale del Codice Privacy e quello del Regolamento U.E. 2016/679 sono consultabili sulla Intranet aziendale nella sezione speciale dedicata alla privacy

Chiunque tratti, nell'esercizio delle proprie funzioni, dati e informazioni personali e sensibili, è tenuto a conoscere e rispettare i principi sopra esposti.
In capo a chiunque effettui un trattamento di dati personali derivano pertanto una serie di obblighi: non soltanto di riservatezza e segretezza ma anche di tutela, protezione e sicurezza dei dati.

Il presente documento ha lo scopo di agevolare la lettura e l'interpretazione della normativa, dettando le necessarie prescrizioni e fornendo istruzioni operative, ed è stato redatto tenendo conto delle indicazioni contenute nella seguente normativa:

- *Legge n. 300 del 20/05/1970 "Norme sulla tutela della liberta' e dignita' dei lavoratori, della liberta' sindacale e dell'attivita' sindacale, nei luoghi di lavoro e norme sul collocamento" (GU Serie Generale n. 131 del 27/05/1970);*
- *Direttiva del Ministro per la Funzione Pubblica del 30/10/2001 n. 3/*2001 *(oggetto: sistemi di telefonia ed i sistemi connessi di telecomunicazione delle pubbliche amministrazioni)*
- *Decreto legislativo 196/2003*
- *Provvedimento n. 13 del Garante per la protezione dei dati personali del 01/03/2007, "Linee guida per posta elettronica e internet" [doc. web n. 1387522];*
- *Legge 24/12/2007 n. 244 (Finanziaria 2008 - comma 594 e 595);*
- *Direttiva del Ministro per la Pubblica Amministrazione e l'Innovazione del 26/05/2009 n. 2/09 (oggetto: utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro)*
- *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009 [1634116]*
- *Provvedimento Garante Privacy n. 3 del 10/01/2013 "Dossier sanitario e trattamento dei dati personali dei pazienti"*
- *Provvedimento Garante Privacy n. 340 del 3/07/2014 "Trattamento di dati tramite il dossier sanitario aziendale"*
- *"Linee di indirizzo per la gestione del dossier sanitario nelle aziende sanitarie di AVEN", approvato dall'assemblea dei Direttori Generali di AVEN il 9/12/2014*
- *Provvedimento Garante Privacy del 4/06/2015 "Linee guida in materia di Dossier sanitario", pubblicato in G.U. 164 del 17/7/2015 [doc. web n. 4084632]*
- *Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati"*
- *D.Lgs. n. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (18G00129) (GU n.205 del 4-9-2018)*

Le istruzioni riportate nel seguito si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina i rapporti di lavoro e la tutela dei lavoratori.

L'Azienda garantisce che per nessuna ragione i dati informatizzati gestiti dall'Azienda, i sistemi di elaborazione dati e gli strumenti di telecomunicazioni saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113 e 114, del Codice; artt. 4 e 8 l. 20 maggio 1970, n.300)

Il documento opera nei confronti di ogni dipendente dell'Azienda e di tutti coloro che a vario titolo si trovino ad utilizzare il sistema informativo dell'Azienda. Nel seguito del presente documento, per semplicità espositiva, si farà riferimento genericamente all'operatore.

Il presente documento è disponibile per la sua consultazione sulla Intranet aziendale.

Sarà cura del dipendente accertarsi se siano state pubblicate nuove versioni del presente Disciplinare e adottare comportamenti congrui a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività. Una copia del presente documento è disponibile presso l'U.O. Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo per poterne prendere visione e ottenerne copia.

Le versioni successive saranno consultabili con le stesse modalità

È comunque indispensabile che chiunque tratti dati personali o sensibili prenda visione del vigente DPS – Documento Programmatico sulla Sicurezza –.
Il testo del vigente DPS è reperibile presso UOSITRP o sulla Intranet aziendale.

Le seguenti istruzioni sono parte del sistema di sicurezza che l'Azienda adotta al fine di gestire, nel rispetto della vigente normativa, i dati trattati.

Accesso al sistema informatico aziendale e più in generale agli ausili tecnologici messi a disposizione dall'Azienda

- *tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale, devono essere intestatari di un nome di utente all'interno del dominio di sicurezza aziendale (**account**), possono richiedere l'accesso alla posta elettronica e ad Internet e saranno autorizzati o meno – in base alla mansione e a considerazioni organizzative – dal Responsabile (Delegato al trattamento dei dati personali) di riferimento*

- *all'atto dell'assunzione, comunque, a tutto il personale, sia appartenente alla dirigenza che al comparto, verrà assegnato automaticamente un account e una parola chiave di accesso (**password**) standard, che l'account dovrà modificare all'atto del primo accesso al sistema. L'account assegnato, permetterà la navigazione nella Intranet aziendale.*
  Al personale appartenente alla dirigenza, verrà inoltre assegnato automaticamente un indirizzo di posta elettronica esterna e la possibilità di navigazione in Internet

- *la password alla rete informatica e agli applicativi aziendali deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi*

- *la password non deve contenere riferimenti facilmente riconducibili all'operatore*

- *a tutti gli account del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della password; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile sostituirla anche prima*

- *in ogni altro caso in cui si abbia fondato sospetto che le proprie credenziali siano venute in maniera indebita a conoscenza di terzi non autorizzati, è fatto obbligo all' operatore di provvedere all'immediato cambio password e di darne comunicazione all'UOSITRP*

- *qualora si utilizzino sistemi che non siano in grado di richiedere automaticamente il cambio di password, è indispensabile che l'operatore – autonomamente - provveda a cambiarla ogni tre mesi*

- *l'operatore è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare*

- *l'autenticazione degli operatori aziendali, sia Delegati che Autorizzati, è basata su tabelle interne al sistema di Active Directory che contengono l'elenco delle coppie "ID-Password"*
  *Le password associate agli account NON sono conservate in modalità "in chiaro" nel sistema di Active Directory aziendale, ma sono **generate e conservate utilizzando due metodologie conosciute come "hashes"** [LAN Manager hash (LM hash) and a Windows NT hash (NT hash) della password]*
  Questi hash sono memorizzati nel database SAM (Security Accounts Manager) locale o in Active Directory.
  In virtù di ciò, le password associate agli account non sono riconoscibili da alcun operatore aziendale, compresi gli Amministratori di Sistema.

- *in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati, ad esempio scollegandosi o attivando un salvaschermo protetto da password*

- *il personale appartenente alla dirigenza, una volta in servizio, dovrà segnalare all'U.O. Sistemi Informativi, Telecomunicazioni e R.P. (**UOSITRP**) su quali postazioni attivare il nuovo profilo (posta elettronica, Internet, etc), informandone il proprio Direttore di U.O.*
  I tecnici addetti alla configurazione delle postazioni comunicheranno quindi all'operatore richiedente l'account assegnatogli

- *per il personale appartenente al comparto, una volta in servizio, è necessario che il Responsabile (Delegato al trattamento dei dati personali) di riferimento (dirigente o suo delegato) in base alla mansione dell'operatore, ovvero Autorizzato al trattamento dei dati personali (ex Incaricato), ed a considerazioni organizzative, richieda all'UOSITRP di attivare gli eventuali servizi necessari (casella di posta elettronica interna, casella di posta elettronica esterna, navigazione Internet), oltre che le postazioni su cui attivare tali servizi.*
  I tecnici addetti alla configurazione delle postazioni comunicheranno quindi all'operatore l'account assegnatogli

- *l'operatore una volta autenticato col sistema centralizzato di autenticazione di Active Directory, ha accesso alle risorse (computer, unità di rete associate, etc.) a lui assegnate, tra le quali la casella di posta elettronica.*

- *per gli account del dominio aziendale sono previste sui file server cartelle personali (**U:**) piuttosto che condivise con altri account appartenenti alla stessa U.O. (**J:**) su cui eseguire il salvataggio dei propri file. Tali documenti sono tutelati da perdite mediante accurate procedure di salvataggio.*
  È fatto divieto di memorizzare in locale sulle stazioni di lavoro dati sensibili, che vanno salvati invece sui file server; nel caso in cui l'account sotto la propria responsabilità memorizzi anche solo per brevi periodi dati in locale sulla stazione di lavoro, dovrà gestire i requisiti minimi di sicurezza della stessa

- *il Responsabile (Delegato al trattamento dei dati personali) di riferimento (dirigente o suo delegato) in base alla mansione dell'operatore interessato (Autorizzato), sia che appartenga alla dirigenza che al comparto, dovrà richiedere all'UOSITRP di attivare per l'operatore (Autorizzato) gli accessi ed abilitazioni alle varie procedure informatiche su cui lo stesso avrà la necessità di operare*

- *tutti i PC devono avere il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi alla competente UOSITRP*

- *è vietato manomettere o cambiare le configurazioni delle attrezzature aziendali se non esplicitamente autorizzati dalla competente UOSITRP*

- *è vietato installare attrezzature non autorizzate e collegarle alla rete aziendale se non dietro esplicita autorizzazione della competente UOSITRP*

- *è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia. Tali operazioni potranno essere consentite solo al personale aziendale espressamente autorizzato dalla Direzione, nell'esercizio del potere di controllo dell'Amministrazione datore di lavoro, in ottemperanza alle regole ed ai principi generali dettati dalla normativa richiamata in premessa*

- *il solo personale addetto alla manutenzione, al controllo e alla sicurezza delle infrastrutture tecnologiche è autorizzato a compiere le attività che garantiscano, oltre al buon funzionamento delle infrastrutture aziendali, il perseguimento dei fini istituzionali nei limiti e nel rispetto della normativa vigente*

- *gli strumenti di comunicazione aziendali e gli strumenti di produttività personale in genere – telefono fisso, telefono cellulare, stazioni informatizzate di lavoro, fax, stampanti, ecc… - concessi in uso **dovranno essere utilizzati per fini esclusivamente istituzionali e connessi alla propria mansione e attività di servizio**; nessun altro uso di tali strumenti è consentito se non espressamente autorizzato anche se nelle potenzialità della strumentazione concessa in uso ed eventualmente abilitata.*

A questo proposito è bene precisare che talvolta non è possibile disabilitare determinate funzionalità da alcuni apparati tecnologici, o che questo, anche se tecnicamente possibile, può essere organizzativamente oneroso per l'Azienda; comunque la disponibilità di una determinata funzionalità non autorizza il consegnatario di un bene all'utilizzo della stessa se non espressamente autorizzato e comunque se non necessario all'espletamento delle proprie mansioni e riconducibile ad attività istituzionali

- *nessun dispositivo personale potrà essere collegato alla rete dell'Azienda e/o utilizzato per trattare dati istituzionali aziendali; qualora l'Azienda, per l'espletamento della propria attività istituzionale si avvalga di attrezzature la cui gestione in sicurezza ricada sotto la responsabilità di personale non dipendente o a questi assimilabile, dovrà essere formalmente definito un Responsabile "Esterno" che si faccia garante degli aspetti di sicurezza e di rispondenza alla normativa vigente in tema di trattamento dei dati personali per tutti i trattamenti che avvengono su tali attrezzature*

- *l'Azienda si riserva di attivare i controlli circa l'utilizzo degli strumenti aziendali concessi in uso – ad esempio il telefono, le stazioni di lavoro informatizzate, i software aziendali, i palmari, ecc… - qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni, nel rispetto della normativa sulla tutela della riservatezza dei dati personali. Sono in ogni caso esclusi controlli prolungati, costanti e indiscriminati*

- *qualora l'istruttoria preliminare relativa ai suindicati utilizzi anomali evidenziasse anomalie, l'UOSITRP effettuerà un'analisi più dettagliata per verificare possibili abusi*

- *in caso di effettivo riscontro di abuso, l'UOSITRP provvederà a segnalare tali casistiche al Direttore responsabile dell'U.O. o articolazione organizzativa cui afferisce il dipendente che ha effettuato gli utilizzi anomali*

- *nei casi più gravi, al fine di prevenire ulteriori usi impropri che potrebbero causare consistenti problematiche di sicurezza per l'Azienda, prima della segnalazione al Direttore responsabile dell'U.O. o articolazione organizzativa cui afferisce l'assegnatario, l'UOSITRP si riserva la facoltà di bloccare, temporaneamente e senza preavviso, la possibilità di accesso ai sistemi informatici all'account oggetto di verifica;*

- *rimane comunque a carico del Direttore responsabile dell'U.O. o articolazione organizzativa cui afferisce il dipendente che ha effettuato gli utilizzi anomali esaminati comunicare la situazione anomala all'Ufficio Procedimenti Disciplinari dell'Azienda*

- *l'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso. Il personale tecnico dell'Azienda, o il personale delle Società che in nome e per conto dell'Azienda effettuano attività di manutenzione sugli strumenti aziendali - attrezzature di produttività personale, sistemi di comunicazione, ecc… - potranno accedere a detti strumenti per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto dall'operatore, come impedimento all'accesso, il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale*

Dismissione Account per i dipendenti aziendali

Allo scadere del contratto (tempo determinato, dimissione, trasferimento verso altro ente, etc.) del dipendente/operatore, sarà automaticamente disabilitato l'account associato allo stesso all'interno del dominio di sicurezza aziendale.
I dati personali (casella di posta, eventuali dati su unità di rete personale U:) rimarranno fuori linea per 90 giorni, poi saranno definitivamente cancellati, a meno di richiesta scritta presentata all'UOSITRP dal Direttore responsabile dell'U.O. o articolazione organizzativa cui afferisce l'operatore in questione, finalizzata al ripristino delle credenziali in caso di ripresa attività dell'operatore, ed in tal caso, deve essere definito un tempo limite di ripristino dell'account.

Prolungata assenza dal servizio di un operatore

Modalità da seguire per l'accesso ai dati in caso di prolungata assenza dell'operatore (Autorizzato).
È necessario distinguere due diversi casi:

- *a) i dati sono accessibili da più di un operatore (Autorizzato);*
- *b) i dati sono accessibili da parte di un unico operatore (Autorizzato).*

Nel caso in cui i dati siano accessibili da parte di più operatori – caso (a) - sarà necessario adottare le misure di seguito descritte solo nel caso in cui tutti gli operatori che hanno accesso ad un medesimo dato non siano presenti per un lungo periodo, per cui di seguito per semplicità si farà riferimento al solo caso b).

Nel caso in cui l'operatore che ha normalmente accesso al dato non possa per lungo periodo garantire ciò, sarà cura del Responsabile (Delegato al trattamento dei dati personali) di riferimento vicariare tale mancanza

Nel caso il Responsabile (Delegato al trattamento dei dati personali) di riferimento sia in grado di utilizzare le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, basterà che tale Responsabile richieda all'UOSITRP le abilitazioni necessarie ad accedere al dato; una volta ricevute le abilitazioni opportune potrà accedere ai dati al posto dell'operatore assente
Lo stesso Responsabile dovrà informare di ciò l'Autorizzato assente alla prima occasione utile

Nel caso il Responsabile (Delegato al trattamento dei dati personali) di riferimento non sia invece in grado di utilizzare direttamente le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, farà richiesta al personale dell'UOSITRP che normalmente si occupa degli aspetti tecnici dell'applicativo, di accedere ai dati necessari in qualità di Autorizzato temporaneo

La misura precedente dovrà essere utilizzata solo nel caso l'urgenza lo richieda e nella misura strettamente necessaria a risolvere la situazione contingente; se l'esigenza va oltre la singola necessità e qualora i tempi lo consentano il Responsabile (Delegato al trattamento dei dati personali) di riferimento disporrà di abilitare un diverso operatore, in aggiunta a quello assente, all'accesso dei dati. Il medesimo Responsabile dovrà informare di ciò l'Autorizzato assente alla prima occasione utile

Si ritiene opportuno che la individuazione di un diverso Autorizzato da abilitare all'accesso ai dati avvenisse da parte del Responsabile di cui sopra all'interno di una rosa di fiduciari allo scopo previsti dall'Autorizzato. Una tale gestione, se attuata, è in carico al Responsabile (Delegato al trattamento dei dati personali) di riferimento

Le richieste attinenti alla casistica descritta dovranno pervenire all'UOSITRP in forma scritta, opportunamente motivate e firmate al Responsabile (Delegato al trattamento dei dati personali) di riferimento

ver. 2019_01

Accesso alle informazioni contenute nel Clinical Data Repository (Galileo ditta Dedalus-Noemalife)

*Il **Clinical Data Repository (CDR)** è uno strumento di raccolta in formato elettronico di dati clinici relativi a tutte le prestazioni sanitarie effettuate a beneficio del paziente/utente presso tutti i servizi/strutture dell'Azienda USL di Piacenza.*
Il CDR contiene informazioni inerenti lo stato di salute del paziente/utente volte a documentare la sua storia clinica sanitaria, ed è consultabile esclusivamente all'interno di questa Azienda USL.
*I dati clinici trattati in questa Azienda USL e contenuti nel CDR fanno sì che lo stesso tenda a costituire un sistema informativo riconducibile al concetto di **Dossier Sanitario Elettronico** che come tale è sottoposto ad una stringente normativa sulla privacy.*

*Per le modalità di gestione ed accesso al CDR, si faccia riferimento allo specifico "**Regolamento aziendale per la corretta gestione del Dossier Sanitario Elettronico del Paziente",** strettamente correlato al presente documento e a cui si rimanda.*

Internet

- *è vietato l'utilizzo personale e non istituzionale della connessione a Internet aziendale*

- *tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log. Tali log tengono traccia dei seguenti dati per ogni accesso:*
  - *identificativo dell'account che ha navigato in Internet*
  - *identificazione della stazione di lavoro*
  - *data e ora*
  - *riferimento al sito visitato (URL)*

  Tutti i log sopra citati vengono conservati dall'Azienda un anno solare.
  Questi log sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema, entrambi su base anonima; i log saranno trattati in maniera tale da fornire informazioni in maniera aggregata in modo da precludere l'immediata identificazione degli operatori, a meno che non vi siano specifiche ragioni per accedere al dettaglio massimo, cioè alle informazioni di tipo nominativo

- *l'Azienda si riserva di filtrare l'accesso a siti che risultino pericolosi o non in relazione con le attività istituzionali; il filtraggio verrà attuato tramite l'appartenenza o meno del sito a categorie giudicate pericolose o non attinenti all'attività lavorativa. La lista dei siti inaccessibili o delle categorie potrà essere chiesta alla Direzione dell'UOSITRP; in caso di motivate ragioni, potrà essere dalla stessa autorizzata la navigazione su un sito normalmente precluso, mediante rimozione dalla lista di esclusione. L'esclusione dei siti verrà operata periodicamente in base agli aggiornamenti del software utilizzato*

- *a titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:*
  - *servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività non istituzionali, attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente*
  - *scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste all'UOSITRP che provvederà a eseguire fisicamente lo scarico da stazione protetta, applicare le misure antivirus relative e consegnare il software al richiedente*
  - *utilizzare Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato*
  - *usare la rete in modo difforme da quanto previsto da questo documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete*
  - *produrre e pubblicare propri siti Web sulla infrastruttura tecnologica dell'Azienda; ogni eventuale necessità di realizzare siti Web personali o di struttura dovrà essere espressamente autorizzata dal Direttore responsabile dell'U.O. o articolazione organizzativa di riferimento*

- *l'Azienda concede l'utilizzo di Internet ai dipendenti per svolgere attività che non rientrano tra i compiti istituzionali, nei seguenti casi:*
  - *per consultare la propria posta elettronica personale via Web (a meno di situazioni particolari che mettano a rischio l'integrità del sistema aziendale – p.e. pericolo di infezione da virus tipo CriptoLocker)*
  - *per assolvere incombenze amministrative e burocratiche (ad esempio per effettuare adempimenti on-line nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con Istituti bancari ed assicurativi), nel rispetto delle seguenti indicazioni:*
    - *avvertire ogni volta il proprio Direttore responsabile dell'U.O. o articolazione organizzativa della necessità di ricorrere all'utilizzo delle risorse aziendali per il disbrigo delle pratiche di cui sopra*
    - *contenere l'impegno delle risorse aziendali ai tempi strettamente necessari allo svolgimento delle transazioni*

Tutto ciò deve comunque avvenire in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda

Posta elettronica

- *è vietato l'utilizzo personale e non istituzionale della posta elettronica aziendale, fatto salvo quanto previsto dalla normativa e dai regolamenti aziendali*

- ***è vietato l'utilizzo della posta elettronica per l'invio di dati sensibili**. In particolare è vietato un uso di tale strumento dal quale possa derivare la possibilità, anche indiretta o preterintenzionale, di rilevare le opinioni politiche, religiose o sindacali dell'operatore, le sue inclinazioni sessuali, il suo stato di salute*

- *fatto salvo quanto previsto in seguito circa l'utilizzo del servizio di posta elettronica dell'Azienda, ad ogni operatore viene assegnato un determinato spazio per la memorizzazione sul server centrale di posta. Esaurito il predetto spazio sul server, l'operatore potrà ricevere o spedire messaggi solo dopo aver liberato spazio sufficiente attraverso la cancellazione o lo "scarico in locale" dei messaggi di posta*

- *se l'operatore non ritenesse opportuno memorizzare in locale, ovvero presso un particolare Personal Computer aziendale a sua disposizione, i messaggi di posta elettronica inviati o ricevuti, i messaggi stessi vengono mantenuti sui server aziendali di posta sine die, ovvero finché l'operatore non decide di cancellare fisicamente i messaggi oppure di trasferirli in locale*

- *i messaggi di posta presenti sui server aziendali sono sottoposti a politiche di backup per consentirne il recupero in caso di cancellazione o perdita accidentale degli stessi*

- *qualora l'account "scarichi" sulla propria postazione di lavoro, ovvero cancelli i messaggi di posta ancora presenti sul server, tali messaggi non saranno oggetto di backup*

- *il sistema di posta elettronica aziendale NON tiene traccia delle informazioni inerenti le e-mail inviate e ricevute, ovvero non sono presenti file di log che memorizzano tali informazioni*

- *tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail contenenti o infette da virus, effettua i seguenti controlli:*
  - *blocco delle e-mail con allegati potenzialmente pericolosi (es. file con estensioni EXE, .COM, .VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK)*
  - *blocco delle e-mail (interne) con dimensioni complessive (messaggio di posta + allegati) superiori a 20 Mb, con un massimo di 5000 destinatari*
  - *blocco delle e-mail (esterne) con dimensioni complessive (messaggio di posta + allegati) superiori a 10 Mb, con un massimo di 100 destinatari*

- *in particolari situazioni, ad esempio massicce ricezioni di e-mail infette, l'UOSITRP si riserva di bloccare e cancellare le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi riconducili alla violazione di sicurezza o a codice pericoloso*

- *al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in termine tecnico viene chiamato SPAM – l'Azienda ha in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Le regole di filtraggio possono causare:*
  - *il passaggio di SPAM qualora non sufficientemente selettive;*
  - *il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM.*

  Per le ragioni sopra indicate, si vieta l'utilizzo della posta elettronica di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario

- *nel caso in cui il sistema AntiSPAM succitato, per motivazioni varie (p.e. non tempestivo aggiornamento rispetto a nuove tipologie di minaccia, apparente "scarsa pericolosità" del contenuto della mail, etc.) non riesca ad intercettare particolari messaggi, si raccomanda di eliminare immediatamente la mail nel caso in cui si ritenga che sia "sospetta" (p.e. mittente non riconosciuto, contenuto non riferibile alla propria attività o interessi personali) e soprattutto di NON interagire con possibili richieste contenute nel corpo della mail stessa.*
  Pertanto, nel caso l'indirizzo di posta elettronica fosse raggiunto da messaggi che invitano ad effettuare azioni del tipo "Clicca sul link allegato" oppure "Clicca qui per aggiornare il tuo account", si raccomanda di:
  - *NON considerare queste comunicazioni*
  - *NON cliccare sui link indicati*
  - *eliminare immediatamente la mail stessa*

- *ad uno stesso operatore possono essere assegnate più caselle di posta elettronica anche condivise con altri operatori dello stesso gruppo/dipartimento. Tali caselle condivise devono essere utilizzate esclusivamente per la ricezione dei messaggi, mentre per le risposte o gli invii, si deve sempre utilizzare la propria casella personale di posta*

- *i dipendenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale e sono tenuti ad utilizzarla in modo conforme alle presenti regole*

- *è buona norma quindi che gli stessi adottino le seguenti regole comportamentali:*
  - *mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti*
  - *inviare preferibilmente files in formato PDF*
  - *prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta*
  - *cancellare il messaggio e gli eventuali allegati qualora ci si renda conto di aver ricevuto per errore il messaggio stesso ed informare il mittente con lo stesso mezzo*

  Inoltre, come già indicato in precedenza:
  - *gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus)*
  - *accertarsi quindi dell'identità del mittente e controllare per mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo*
  - *rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre se sospette*
  - *collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi*

- *nel caso in cui il dipendente decidesse di rendere accessibili le proprie le caselle di posta elettronica aziendali* ***mediante dispositivi personali*** *quali smartphone o tablet, al fine di evitare e/o ridurre al minimo il possibile accesso ai dati personali contenuti nelle email aziendali, è necessario che il dipendente metta in esercizio i medesimi accorgimenti di sicurezza obbligatori per analoghi dispositivi aziendali a lui assegnati*

- *il dipendente, in conformità al Regolamento UE 679/2016 in materia di protezione dei dati personale, qualora abbia accesso alle proprie caselle di posta elettronica aziendali mediante uno strumento mobile (smartphone, tablet, notebook, etc),* ***sia aziendale che personale****, dovrà prestare particolare cautela nella conservazione dei dispositivi a lui assegnati.* ***L'eventuale perdita o sottrazione di uno di detti dispositivi costituisce una forma di "data breach"****, ovvero di violazione dei dati personali o, potrebbe costituire, comunque, un serio rischio per la conoscibilità a terzi non autorizzati dei dati personali in esso contenuti*

- *si consiglia altresì a ciascun dipendente assegnatario di un indirizzo di posta elettronica aziendale di inserire in calce alle email inviate un messaggio in cui si avverte il destinatario della natura personale e riservata delle informazioni inviate (c.d. disclaimer).*
  Segue un esempio di tale messaggio:
  "Qualora abbia ricevuto questa e-mail per errore, La invito cortesemente ad avvertire immediatamente il mittente e a distruggere il presente messaggio e i suoi eventuali allegati. Tenga presente che qualsiasi uso, riproduzione o divulgazione di questo messaggio è vietata."

- ***il sistema di posta elettronica in uso e concesso in utilizzo, non è un sistema di posta certificata*** *(a meno di situazioni espressamente indicate), non vi è pertanto la garanzia della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di privatezza relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni.*
  È pertanto fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio

- *l'Azienda favorisce la condivisione di indirizzi di posta elettronica fra più utilizzatori mediante l'adozione di cosiddette "mailing list", cioè di gruppi di indirizzi*

- *l'Azienda non fornirà indirizzi di posta elettronica aziendali per usi di tipo personale, ma non vieta la consultazione del contenuto di indirizzi di tipo personale, anche dall'interno dell'Azienda, qualora la modalità di consultazione di tali informazioni sia compatibile con i vincoli di sicurezza del sistema aziendale e ciò avvenga in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda*

- *l'Azienda mette a disposizione funzionalità di avviso in caso di assenza prolungata dell'operatore, che sfruttano le peculiarità del sistema di posta elettronica, e possono fornire coordinate di altri riferimenti all'interno dell'Azienda tali da garantire il corretto funzionamento dei servizi; l'attivazione di tali misure sarà a cura dell'operatore che dovrà avvisare l'UOSITRP di attuare la misura o attuarla in autonomia se tecnicamente in grado. Qualora l'operatore non abbia adottato tale misura e l'assenza si protragga per più di una settimana, il suo Direttore responsabile dell'U.O. o articolazione organizzativa potrà richiedere all'UOSITRP l'adozione di una tale provvedimento*

- *ogni assegnatario di indirizzo di posta elettronica aziendale potrà, in caso di necessità, dirottare la propria posta elettronica su un indirizzo di posta elettronica aziendale di un fiduciario interno all'Azienda; nel caso non sia in grado di attuare detta misura in autonomia, potrà chiedere all'UOSITRP la messa in atto della misura. Della attuazione di tale misura verrà tenuta traccia e verrà data notizia all'intestatario dell'indirizzo di destinazione alla prima occasione utile*

- *qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'Azienda, occorrerà rendere edotto di ciò il destinatario*

- *fatte salve le limitazioni di cui ai punti precedenti, l'Azienda favorisce l'utilizzo della posta elettronica come strumento per la rapida comunicazione fra i dipendenti, fra dipendenti e cittadini, fra Pubbliche Amministrazioni, purché queste comunicazioni siano parte delle attività istituzionalmente previste e compatibili con le mansioni proprie di ogni operatore.*

Alla trasmissione telematica di atti e documenti all'interno dell'Azienda per posta elettronica è riconosciuta la stessa validità della trasmissione per via cartacea; in particolare potranno essere trasmessi atti deliberativi, disposizioni dirigenziali e documenti in genere che non contengano dati sensibili e il cui mancato recapito non ingeneri danni per l'Azienda, per i dipendenti o per altri.
L'utilizzo della posta elettronica, in questi casi, potrà sostituire completamente l'invio di carta; atti o documenti aventi valenza generale possono essere comunicati a tutti o a grande parte dei dipendenti dell'Azienda. Ciò può avvenire tramite l'utilizzo di apposite liste di distribuzione che sono messe a disposizione in posta elettronica

- *esigenze particolari od occasionali di comunicazione ad un numero di utenti il cui volume o la cui qualità non sia già stata prevista dovranno essere inoltrate all'UOSITRP*

- *a titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:*
  - *utilizzare tecniche di "mail spamming", ovvero invio massiccio di comunicazioni non istituzionali o azioni equivalenti (es. auguri in occasione di festività)*
  - *utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, giochi, scherzi, barzellette e altre e-mail avulse dal contesto lavorativo*
  - *inviare messaggi lesivi dell'immagine aziendale oppure recanti un linguaggio non appropriato, nonché con contenuto di materiale in violazione della legge sul diritto d'autore o di altri diritti di proprietà intellettuale ed industriale*
  - *usare la rete in modo difforme da quanto previsto da questo documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete*

- *in relazione a quanto riportato nel secondo punto del presente capitolo, ovvero "In particolare è vietato un uso di tale strumento dal quale possa derivare la possibilità, anche indiretta o preterintenzionale, di rilevare le opinioni politiche, religiose o sindacali dell'operatore….., l'Azienda non ritiene che la posta elettronica possa essere utilizzata quale strumento di propaganda informativa politica o sindacale. La posta elettronica non si configura tra l'altro quale mezzo adeguato per trasmettere informazioni o documenti idonei a rivelare categorie particolari di dati (c.d. sensibili) che la normativa privacy prevede oggetto di maggiore protezione*

- *si promuovono invece, e si possono quindi rendere disponibili a seguito di specifica richiesta scritta, strumenti di divulgazione quali particolari sezioni della Intranet aziendale, le c.d. Bacheche elettroniche onLine, oppure il collegamento da queste a precisi indirizzi web esterni, finalizzati al medesimo risultato (p.e. bacheche onLine di sigle sindacali). Nelle succitate Bacheche elettroniche onLine potranno essere rese disponibili in consultazione, a titolo di esempio, pubblicazioni, testi e comunicati. Tutti i dipendenti potranno quindi liberamente accedere, in qualsiasi momento della giornata lavorativa e in modo veramente semplice, alle comunicazioni sindacali depositate sull'Intranet aziendale*

Utilizzo sistemi mobile (tablet, smartphone, notebook, etc.)

L'Azienda si riserva di assegnare ai dipendenti la dotazione di dispositivi "mobile", quali smartphone, tablet, notebook che consentono di usufruire della navigazione in internet tramite rete dati.

L'assegnazione di tali apparati è a completa ed insindacabile discrezione dell'AUSL di Piacenza.

L'utilizzo dei dispositivi qui disciplinati risponde alle regole che di seguito si riportano:

- *ogni dipendente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione*
- ***i dispositivi devono essere dotati di password di sicurezza** (es. codice pin, segno di sblocco, touch id, etc) che ne impedisca l'utilizzo da parte di soggetti non autorizzati.*
  Ogni dipendente deve inoltre 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'UOSITRP

- *in caso di furto o smarrimento possono sussistere due possibilità:*
  - *<u>il dispositivo e/o la linea sono di proprietà dell'Azienda</u>. Il furto o smarrimento dovrà essere denunciato alle autorità di pubblica sicurezza e la denuncia dovrà pervenire nel più breve tempo possibile all'UOSITRP, che provvederà al reset della password dell'account corrispondente nel più breve tempo possibile*
  - *<u>il dispositivo e/o la linea sono di proprietà del dipendente</u> (nel caso in cui il dipendente decidesse di rendere accessibili le proprie le caselle di posta elettronica aziendali mediante dispositivi personali). Il furto o smarrimento dovrà essere comunicato il prima possibile con ogni mezzo ritenuto idoneo al personale UOSITRP, che provvederà al reset della password dell'account corrispondente nel più breve tempo possibile*
- *in ogni altro caso in cui si abbia fondato sospetto di un accesso non autorizzato al dispositivo mobile in uso e che le proprie credenziali aziendali siano venute ad indebita conoscenza di terzi non autorizzati, è fatto obbligo al dipendente di provvedere all'immediato cambio password e di darne comunicazione all'UOSITRP*

Utilizzo dei sistemi di comunicazione in fonia – telefoni fissi, telefoni mobili, ecc…

L'Azienda si riserva di assegnare ai dipendenti apparati e linee di telefonia mobile e fissa; la loro assegnazione è a completa ed insindacabile discrezione dell'AUSL di Piacenza.

*Per le modalità di assegnazione degli apparati di telefonia mobile aziendale e le modalità di utilizzo da parte del personale assegnatario, sia esso dipendente o non dipendente ma titolare di specifico incarico commissionato dall'AUSL di Piacenza si faccia riferimento allo specifico "**Regolamento aziendale per l'assegnazione di apparati di telefonia mobile ed utilizzo dei servizi di telefonia fissa e mobile",** strettamente correlato e a cui si rimanda.*

Ulteriori istruzioni per la tutela delle informazioni gestite dagli operatori

Nelle sezioni seguenti vengono identificate alcune casistiche generali che implicano il trattamento di dati sensibili e non. Si intende pertanto normare il comportamento dei dipendenti aziendali relativamente alle citate situazioni.

Utilizzo dei supporti di memorizzazione

È vietato l'utilizzo di supporti rimovibili, come ad esempio CD-ROM, HDD esterni o pen drive per lo scambio di dati sensibili.

Qualora vi fosse assoluta necessità di utilizzarli, è indispensabile assicurarsi che essi non vengano riutilizzati e siano distrutti dopo il loro utilizzo; qualora, viceversa, vengano riutilizzati, occorre verificare che il precedente contenuto sia stato reso assolutamente irrecuperabile, in quanto le normali procedure di cancellazione di un dato informatico non sono normalmente sufficienti a garantire ciò, potendosi in molti casi recuperare anche dati cancellati con procedure e strumenti particolari.

In relazione al trattamento di supporti di natura informatica specifici quali CD-ROM e DVD vergini:

- *l'uso dei supporti vergini è consentito limitatamente allo svolgimento di attività inerenti all'archiviazione, funzionale alla attività imprenditoriale dell'Azienda, di dati, documenti digitali, o registrazioni. È rigorosamente vietato l'utilizzo dei supporti a scopo personale o comunque non inerente alle attività di archiviazione o conservazione di informazioni che esulano dal contesto aziendale*
- *i supporti vergini devono essere utilizzati solo per scopi aziendali legittimi e non per attività di carattere commerciale e/o estranee all'Azienda. Tutto il personale che viene a contatto con tali strumenti deve adottare le misure necessarie per scongiurare furti, danni o abusi. Qualsiasi sospetto di incidente o furto dovrà essere denunciato immediatamente. L'utilizzo o la distribuzione non autorizzati di questi strumenti costituisce una violazione del codice e potrebbe anche costituire un reato, con le conseguenze civili e penali del caso*
- *tutto il materiale deve essere mantenuto in maniera adeguata e con le dovute attenzioni, oltre a ottemperare alle normali disposizioni del codice di condotta aziendale. Tutti i beni dell'Azienda devono essere attentamente e accuratamente archiviati, salvo diversa disposizione.*

Utilizzo di servizi di Cloud Storage

Le nuove tecnologie permettono una distribuzione delle informazioni molto più veloce rispetto al passato. Documenti confidenziali e dati sensibili degli utenti potrebbero essere trasferiti dall'Azienda ad un account personale online del dipendente. Un crescente numero di hacker predilige colpire i repository sui cloud, molto spesso proprio per reperire informazioni relative l'ambito lavorativo delle vittime.

*Ciò premesso, si sancisce il divieto all'utilizzo **di soluzioni pubbliche di cloud storage**, come Dropbox, Google Drive, ICloud, SkyDrive, etc., **di soluzioni di file sharing basate su SaaS** (Software as a Service**) e comunque di qualsiasi account personale online**.*

Si stabilisce di conseguenza che sulle postazioni di lavoro aziendali non sarà installato nessun componente client che consenta l'accesso ai servizi forniti da soluzioni pubbliche di cloud storage e/o a soluzioni di file sharing.

Eventuali eccezioni dovranno essere autorizzate specificamente da UOSITRP e non possono comunque riguardare la condivisione di documenti contenenti dati personali e/o lo spostamento di file confidenziali e/o dati sensibili di utenti/pazienti/dipendenti aziendali.

Garanzie fornite dall'Azienda

L'Azienda definisce quali sono gli uffici e le strutture preposte ai controlli previsti dal presente Disciplinare; sarà possibile in qualsiasi momento per l'operatore avere accesso a tali informazioni rivolgendosi all'U.O. Sistemi Informativi, Telecomunicazioni e R.P.
Inizialmente gli uffici e strutture preposte ai controlli saranno:

- *l'U.O. Sistemi Informativi, Telecomunicazioni e R.P.*
- *l'U.O. Risorse Umane*
- *il Referente Aziendale Privacy unitamente al Gruppo Aziendale per la protezione dei dati personali.*

L'Azienda garantisce che per nessuna ragione i dati contenuti e gestiti nel sistema informativo aziendale saranno utilizzati per il controllo a distanza dei lavoratori (art.113-114 e 184 comma 3) del Codice; artt.4 e 8 L.20 maggio 1970 n.300).

Facoltà dell'Azienda

Qualora l'Azienda:

- *abbia ad accertare manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso*
- *riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema informatico, telematico, telefonico aziendale o il suo buon funzionamento e/o a garantire ad altri accessi o altri privilegi non dovuti*
- *abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata*

si riserva il diritto di:

- *effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature aziendali;*
- *disabilitare le autorizzazioni all'accesso e all'uso delle attrezzature aziendali;*
- *segnalare al Responsabile organizzativo situazioni e comportamenti anomali degli operatori.*

In caso di problemi inerenti la sicurezza della infrastruttura tecnologica l'Azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni software e/o hardware, ecc… Tutte le azioni messe in atto dovranno essere valutate in una logica di costo/beneficio e dovranno essere improntate ad un criterio di minimizzazione del disservizio.

L'Azienda si riserva la facoltà di sospendere l'accesso ai servizi qualora, anche a seguito di segnalazioni rappresentate dal Responsabile organizzativo, sussistano nel tempo reiterate evidenze delle inadempienze da parte dell'operatore.

L'Azienda si riserva la possibilità di interrompere i servizi informatici e telefonici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni.

LA PRESENTE COPIA E' CONFORME ALL'ORIGINALE DEPOSITATO.
Elenco firme associate al file con impronta SHA1 (hex):

A8-C9-DA-AA-46-2D-16-27-35-3E-0A-2C-31-CD-93-BE-F9-4A-BC-B4

CAdES 1 di 2 del 14/06/2019 13:59:43

Soggetto: BISOTTI FLAVIO BSTFLV65A22G535V

Validità certificato dal 06/02/2017 02:00:00 al 07/02/2020 01:59:59

Rilasciato da ArubaPEC S.p.A. NG CA 3, ArubaPEC S.p.A., IT con S.N. 518F BB8E 1835 6A91 FFA7 46

CAdES 2 di 2 del 17/06/2019 13:10:14

Soggetto: GAMBERINI MARIA GMBMRA69T48H294I

Validità certificato dal 09/10/2017 02:00:00 al 09/10/2020 01:59:59

Rilasciato da ArubaPEC S.p.A. NG CA 3, ArubaPEC S.p.A., IT con S.N. 49F9 404F D39F 9B65 A4EB 1B
