REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE

REDAZIONE	Coordinatore del gruppo: **Pierfrancesco Ghedini** - Direttore UO Tecnologie Informatiche e di Comunicazione Gruppo di redazione: **Flavio Fabbri** - Referente Qualità e Accreditamento UO Tecnologie Informatiche e di Comunicazione **Massimo Cavazza** - Referente Sicurezza Informatica UO Tecnologie Informatiche e di Comunicazione
APPROVAZIONE	**Pierfrancesco Ghedini** Direttore UO Tecnologie Informatiche e di Comunicazione

INDICE GENERALE

Indice generale

1. Normativa di riferimento

1.1. Principali riferimenti normativi

- Regolamento Generale sulla Protezione dei Dati 2016/679 (GDPR);
- Decreto Legislativo 30 giugno 2003, n.196, “Codice in materia di protezione dei dati personali”, aggiornato dal D.L. 10 agosto 2018 n.101 e successive modificazioni e integrazioni.
- Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 “Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali”
- 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".
- 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"
- Deliberazione 1 Marzo 2007 “Lavoro: le linee guida del Garante per posta elettronica e internet”
- Circolare AgID n° 1/2017.

1.2. Violazioni della normativa

La normativa di riferimento prevede in caso di violazione sanzioni penali e amministrative.

A titolo di esempio, si elencano di seguito alcune figure di reato previste dal Codice Penale:

- Attentato a impianti informatici di pubblica utilità (art. 420);
- Falsificazione di documenti informatici (art. 491bis);
- Accesso abusivo ad un sistema informativo o telematico (art. 615ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater);
- Diffusione di programmi diretti a danneggiare o interrompere un Sistema informativo (art. 615quinquies);
- Violazione di corrispondenza telematica (artt. 616-617sexies);
- Intercettazione di e-mail (art. 617quater);
- Danneggiamento di sistemi informatici e telematici (art. 635bis);
- Frode informatica (alterazione dell'integrità di dati allo scopo di procurarsi un ingiusto profitto) (art. 640ter).

Le seguenti figure di reato sono invece previste dal “Codice in materia di protezione dei dati personali” così come aggiornato dal D. Lgs. 10 agosto 2018 n.101:

- Trattamento illecito di dati (art. 167)
- Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)
- Inosservanza di provvedimenti del Garante (art. 170)

2. Le principali definizioni

Risorse Informatiche

Qualsiasi mezzo di comunicazione e elaborazione elettronica, hardware, software, rete, servizio e informazione in formato elettronico di proprietà dell'Azienda o in disponibilità o a essa concesso in licenza d'uso.

Le risorse informatiche includono a titolo di esempio:

- sistemi informatici a uso sanitario, amministrativo o tecnico (es. posta elettronica, accesso a Internet, applicativi aziendali quali Areas, P4c, Galileo, GRU, GAAC, ecc.);
- ogni sistema di elaborazione elettronica delle informazioni: server, personal computer fissi o portatili, tablet e similari;
- software di base e di ambiente: sistemi operativi, software di rete, sistemi per il controllo degli accessi, package, utility e similari;
- software di produttività individuale (Office, LibreOffice, OpenOffice, Project, Visio ecc.);
- ogni informazione elettronica registrata o conservata in file e banche dati;
- ogni periferica: stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati, supporti di memorizzazione, video terminali;
- ogni dispositivo di rete: concentratori, ripetitori, modem, switch, router, gateway, firewall, apparati VoIP e similari, access point, chiavette Internet;
- ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche: cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, patch e similari.

Utilizzatori

Persone fisiche dipendenti o collaboratori a vario titolo, frequentatori, universitari che hanno accesso a strumenti informatici o telematici e che sono nella potenzialità di utilizzarli.

Trattamento

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

L'interessato è la persona fisica cui si riferiscono i dati personali.

In merito al tipo di dati si distinguono:

- Dato personale:

  qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- Dati relativi alla salute:

  i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- Dati biometrici:

i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- Dati genetici:

  i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- Categorie particolari di dati personali (<<dati sensibili>>) (C10, Art.9):

  Ogni dato personale che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

- Dato pseudonimizzato:

  i dati personali che non possono più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- Dato anonimo:

  informazioni che non si riferiscono a una persona fisica identificata o identificabile o dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. (C26).

In merito ai soggetti che possono effettuare operazioni di trattamento si distinguono:

- Titolare:

  Nel nostro caso è l'Azienda USL di Bologna

- Responsabile:

  la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Di norma sono formalmente nominati e il trattamento avviene sulla base di istruzioni impartite per iscritto dal titolare stesso

- Referente privacy (del. n. 11 del 14/1/2019)

  coloro che ricoprono specificamente i seguenti incarichi: Direttori di Unità Operativa Complessa (SC), Dirigenti Responsabili di Unità Operativa Semplice Dipartimentale (UOSD), Direttori di Programmi Gestionali.

- Autorizzato:

  la persona fisica autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Banca di dati

Qualsiasi complesso di dati ripartito in una o più unità dislocate in uno o più siti.

Misure minime di sicurezza

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per la sicurezza dei dati (integrato anche dalla Circolare AgID n° 1/2017 che si riferisce alle misure di sicurezza della PA).

Credenziali di autenticazione

I dati e i dispositivi, in possesso di una persona, da questa conosciuti o a essa univocamente correlati, utilizzati per l'autenticazione informatica, ovvero il processo che garantisce l'accesso a un sistema informatico.

La parola chiave (password) è la componente di una credenziale di autenticazione associata a una persona e solo a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica, da mantenere riservata.

3. Premessa

Il presente documento, redatto a cura della UO Tecnologie Informatiche e di Comunicazione (di seguito UO ICT), regolamenta l'accesso e l'uso delle risorse informatiche dell'Azienda USL di Bologna (nel seguito AUSL), secondo i principi e le disposizioni della normativa citata in premessa e le indicazioni in materia di corretto uso delle risorse informatiche secondo le politiche e disposizioni aziendali definite in accordo con la direzione aziendale.

I I servizi informatici aziendali sono regolamentati, oltre che dal presente documento, dal Regolamento per l'utilizzo della Posta Elettronica e Internet. Per le misure in materia di protezione dei dati personali, ma non esclusivamente relative al trattamento di dati con supporto informatico, si rinvia ad altra documentazione aziendale specifica.

II La UO ICT si impegna ad adeguare questo regolamento in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità tecniche. L'ultima versione del regolamento sarà sempre consultabile sul sito intranet aziendale.

4. Oggetto e campo di applicazione

Le regole stabilite si riferiscono a tutte le risorse informatiche dell'Azienda, devono essere applicate da tutti i soggetti che le utilizzano e hanno valenza per tutte le tipologie di dati.

Gli utenti, dipendenti della AUSL e i collaboratori esterni autorizzati, devono essere nominati, ai sensi del GDPR 679/2016, “autorizzati del trattamento dei dati personali” a cui possono avere accesso mediante i servizi informatici aziendali.

Pertanto i dati possono essere trattati limitatamente alle operazioni indispensabili per l'esercizio delle funzioni degli autorizzati.

Gli utenti a vario titolo autorizzati devono attenersi alle disposizioni del presente regolamento.

Oltre a quanto definito in questo documento si precisa che:

- per le risorse informatiche messe a disposizione o date in uso all'azienda da altre organizzazioni valgono gli accordi e le condizioni contrattuali stipulate fra le parti;
- per l'utilizzo di dati, programmi e materiali valgono sempre le condizioni di copyright, ove previsto;
- l'utilizzo delle risorse informatiche dell'azienda deve essere comunque conforme a quanto previsto dalla normativa vigente.

5. I principali indirizzi

Le risorse informatiche:

- sono parte integrante del patrimonio dell'Azienda USL di Bologna;
- devono essere utilizzate per gestire le attività aziendali, secondo le finalità autorizzate e definite dalla direzione aziendale e inerenti alla propria mansione, nel rispetto dei principi di necessità, indispensabilità, non eccedenza;
- devono essere rese disponibili solo alle persone autorizzate;
- devono essere protette da danneggiamenti, furti e cause diverse che possano compromettere le attività aziendali.

6. I principali divieti

- Introdursi abusivamente nei sistemi informatici aziendali.
- Procurare a sé, o ad altri, profitto, o arrecare danni all'azienda, procurandosi, riproducendo, diffondendo, o consegnando codici, parole chiave o altri mezzi idonei all'accesso ai sistemi informatici.

- Riprodurre, duplicare e/o asportare, comunicare a terzi, diffondere i dati di cui l'azienda è titolare del trattamento.
- Riprodurre e asportare documentazione di qualsiasi tipo classificata riservata, compresi progetti, schede, prospetti se non dietro esplicita autorizzazione del titolare dei relativi diritti (o di persona delegata).
- Intercettare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici.
- Distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici ovvero i programmi e le informazioni o i dati esistenti nei sistemi.
- Riprodurre, duplicare e/o asportare programmi installati di cui l'azienda è licenziataria o proprietaria.
- Introdurre, installare, utilizzare programmi che non siano stati regolarmente acquistati, distribuiti e installati dalle preposte funzioni aziendali.
- Adottare comportamenti che mettano a rischio la sicurezza del sistema informatico/informativo, inclusi i dati contenuti, o che pregiudichino o ostacolino le attività della collettività degli utilizzatori.

7. Responsabilità

7.1. Procedure informatizzate autorizzate

Le procedure informatiche distribuite e gestite dalla UO ICT sono tutte e sole quelle individuate nell'allegato A - Elenco applicativi di base e specifici autorizzati.

Relativamente a tali procedure, sono a carico della UO ICT le misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, per quanto riguarda i server, i software di base, le procedure applicative, le infrastrutture tecnologiche, i dispositivi della rete aziendale.

Infine sono a carico degli utilizzatori (referenti privacy e autorizzati, ciascuno per i rispettivi ambiti di competenza e responsabilità) le misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, in particolare questo regolamento, per quanto riguarda le postazioni di lavoro (Personal Computer) e le attività svolte con esse.

7.2. Procedure informatizzate non gestite dalla UO ICT

Fermo restando il divieto di utilizzare programmi non autorizzati, se per qualsiasi ragione, in particolare la necessità di garantire la continuità operativa, dovessero essere in uso presso le Unità Operative procedure informatizzate NON distribuite dalla UO ICT, fintanto che esse rimangono operative l'organizzazione e la gestione delle misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, sono a carico del singolo referente privacy.

8. Sistemi di autenticazione e di autorizzazione

Il referente privacy, individuati gli autorizzati, dovrà richiedere l'attivazione della credenziale di autenticazione informatica, specificando a quali dati e tipi di operazioni può accedere in relazione ai compiti impartiti.

Il trattamento di dati personali, con strumenti elettronici, è consentito infatti ai soli autorizzati dotati di credenziali di autenticazione, in genere costituite da NomeUtente (username) e password.+

8.1. Credenziali di autenticazione (coppia username e password)

Le credenziali di autenticazione sono il presupposto necessario per l'utilizzo dei sistemi informatici messi a disposizione dall'Azienda USL di Bologna.

Le credenziali consentono il superamento di una procedura d'autenticazione che permette l'accesso a uno specifico trattamento o a un insieme di trattamenti.

8.2. Rilascio e rinnovo delle credenziali

Tutte le informazioni relative alle modalità di rilascio e di rinnovo delle credenziali sono riportante nell'Allegato B - Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente.

8.3. Gestione delle credenziali

Le credenziali possono consistere:

- in un codice per l'identificazione dell'autorizzato, associato ad una parola chiave riservata conosciuta solamente dal medesimo (**username e password**),

oppure

- in un dispositivo d'autenticazione (per es. una carta magnetica o smart card) in possesso e uso esclusivo dell'autorizzato, eventualmente associato a un codice identificativo o a una parola chiave,

oppure

- in una caratteristica biometrica dell'autorizzato (per es. impronta digitale), eventualmente associata a un codice identificativo o a una parola chiave.

Lo ***username****,* o nome utente, è di norma costituito dal nome e dal cognome dell'utilizzatore intervallati da un "**.**" (ad esempio: **mario.rossi**).

Lo stesso username non potrà, neppure in tempi diversi, essere assegnato a autorizzati diversi.

La ***password*** (o parola chiave) è una parola segreta, conosciuta solo dall'autorizzato che, in coppia con lo username, permette di accedere alla procedura informatizzata scelta dal dipendente e deve essere cambiata, per motivi di sicurezza, ogni novanta giorni (con altra diversa da quelle precedenti).

La password è strettamente personale e per nessun motivo deve essere resa nota a altri. La sua conoscenza da parte di estranei consentirebbe il trattamento dei dati per nome e per conto del possessore delle credenziali. Infatti, l'eventuale uso improprio di apparecchiature, strumenti o servizi sarà imputato al titolare della password con la quale è avvenuto l'accesso.

A ogni autorizzato sono assegnate individualmente una o più credenziali per l'autenticazione.

L'assegnatario dovrà farne un uso strettamente personale (quindi non condivisibile con altri), operare nell'ambito delle autorizzazioni ricevute e utilizzare le risorse solo per scopi aziendali.

Ogni autorizzato è tenuto ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (password), e la diligente custodia dei dispositivi in suo possesso o a suo uso esclusivo.

Le credenziali vengono disattivate nel caso di non utilizzo per oltre 6 mesi.

Le credenziali vengono disattivate anche in caso di perdita della qualità che consente all'autorizzato l'accesso ai dati personali.

Sono esplicitamente vietate credenziali di accesso anonime.

La scelta sicura della password si realizza attraverso le seguenti regole di buon senso:

- deve essere facilmente memorizzabile in modo tale che si possa evitare di scriverla (per es. sulla postazione di lavoro o in prossimità di essa), ma non banale e di facile individuazione (per es. priva di riferimenti chiari all'autorizzato).
- La sua lunghezza deve essere di almeno dieci caratteri
- deve contenere almeno un numero o un carattere speciale e almeno una lettera maiuscola e almeno una lettera maiuscola (il sistema non consentirà di agire diversamente)[1].
- Non deve contenere il codice identificativo assegnato alla persona.
- Deve essere modificata al primo utilizzo e successivamente ogni tre mesi.

1 Solo nel caso in cui, per es. per obsolescenza, lo strumento elettronico non consenta una password lunga 10 caratteri, questa deve avere lunghezza pari al numero di caratteri massimo consentito

- Deve essere modificata ogni volta che si abbia la sensazione che possa essere conosciuta, intenzionalmente o accidentalmente, da altri.
- In caso di modifica, la nuova password non deve essere uguale a una password già usata in precedenza.

Il cambio password può essere eseguito agevolmente collegandosi dalla Intranet nella sezione *Strumenti* al link *Cambio password*[2].

Per agevolare gli utenti sono inviati avvisi e-mail nel caso di imminente scadenza della password o disattivazione dell'account.

8.4. Sistema d'autorizzazione per le procedure informatizzate distribuite dalla UO ICT

L'assegnazione di credenziali di autenticazione del tipo “nome.cognome” abilita l'assegnatario a una serie di “servizi informatici di base” quali a esempio:

- accesso a una casella di posta elettronica;
- visualizzazione del portale del dipendente;
- accesso a Internet;
- accesso alla cartella di rete personale;
- accesso potenziale a gran parte degli applicatici aziendali (che richiede, però, separata autorizzazione).

Per l'abilitazione all'accesso a servizi informatici e procedure non comprese nei servizi di base, la relativa autorizzazione dovrà essere richiesta dal responsabile della struttura organizzativa di appartenenza.

È dovere del responsabile di una struttura organizzativa, firmatario della suddetta modulistica, dare immediata comunicazione alla UO ICT circa la modifica o revoca di funzioni che avevano giustificato in precedenza l'accesso da parte di un proprio collaboratore a procedure/banche dati/servizi.

La richiesta di una nuova attivazione deve pervenire con almeno 15 giorni d'anticipo rispetto alla data di attivazione del codice identificativo.

La richiesta di modifica o disattivazione di un profilo deve pervenire con almeno 10 giorni d'anticipo rispetto alla data di variazione.

La maggior parte dei servizi e procedure informatiche distribuite dalla UO ICT prevedono differenti profili di autorizzazione: tali profili, definibili per ciascun autorizzato o per classi omogenee di autorizzati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, il referente privacy deve verificare la sussistenza delle condizioni per la conservazione dei profili d'autorizzazione attribuiti ai singoli autorizzati.

Dopo un limitato numero di tentativi d'accesso falliti, alcuni sistemi di sicurezza disattivano lo username, che sarà riattivabile solo a seguito di richiesta del singolo autorizzato del trattamento.

Nel caso di prolungata assenza o impedimento di un autorizzato le cui credenziali consentano in modo esclusivo l'accesso ad alcuni dati o strumenti elettronici, tale da rendere indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'autorizzato potrà individuare per iscritto un altro lavoratore (fiduciario) a cui affidare il compito dell'accesso in sua vece, o, alternativamente, il Referente privacy potrà richiedere per iscritto alla UO ICT di autorizzare un altro autorizzato all'accesso ai dati o strumenti interessati. Tale attività dovrà essere riportata in apposito verbale dal Referente privacy che deve informare l'autorizzato del trattamento alla prima occasione utile.

2 https://web-ldap.internal.ausl.bologna.it/cimarosa/passwd.htm

9. Norme generali per l'utilizzo delle apparecchiature informatiche

L'utente deve utilizzare in modo corretto e lecito le risorse che gli sono state messe a disposizione.

Si riportano di seguito alcune tra le principali indicazioni a cui gli utilizzatori sono tenuti ad attenersi; il personale della UO ICT è a disposizione per fornire chiarimenti e ulteriori precisazioni in merito ad aspetti che possano risultare complessi o troppo tecnici.

9.1. Computer aziendali

Il personal computer aziendale in dotazione è uno strumento di lavoro. L'utilizzo personale o improprio dello stesso può comportare inefficienze, problemi di sicurezza e costi di manutenzione imprevedibili ed è pertanto non consentito, salvo casi particolari espliciti.

Il computer deve essere usato in condizioni di sicurezza e stabilità che lo preservino da pericoli di danneggiamento.

I personal computer aziendali sono di norma iscritti in una infrastruttura informatica aziendale di sicurezza, gestione e controllo chiamata Dominio AD (Microsoft Active Directory).

l'UO ICT potrà modificare la configurazione e le funzionalità delle postazioni di lavoro iscritte a dominio tramite la distribuzione centralizzata di policy opportune per assicurare l'uso appropriato delle stesse e la sicurezza della infrastruttura informatica

Possono essere utilizzati unicamente programmi/applicazioni installati o autorizzati dalla UO ICT e per i quali siano stati regolarmente assolti gli oneri relativi alla concessione delle licenze d'uso, ove richieste. In caso di necessità di ulteriori applicazioni il dipendente dovrà farne richiesta alla UO ICT.

È vietato disinstallare o disattivare i software presenti sul PC, in particolare i sistemi di protezione e sicurezza aziendali (tra cui l'antivirus), e i prodotti software di inventariazione e controllo remoto (OCS Inventory, MSRA, Bomgar ecc.). Eventuali eccezioni devono essere concordate con la UO ICT ed esplicitamente autorizzate.

Il personale tecnico potrà effettuare verifiche automatizzate o puntuali sui software presenti nelle postazioni, rimuovendo o bloccando l'esecuzione dei software non autorizzati, richiedendo eventualmente giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

L'utilizzatore è personalmente responsabile del computer assegnatogli; egli ha pertanto l'obbligo, per quanto nelle sue possibilità, di impedire ad altri indebiti utilizzi dell'apparecchiatura informatica.

Si sottolinea che il furto o l'indebito utilizzo di un computer hanno rilevanza, oltre che sotto il profilo patrimoniale, anche in relazione a un possibile improprio utilizzo dei dati in esso contenuti e/o alla perdita degli stessi.

È obbligatorio segnalare tempestivamente casi di furti o incidenti relativi alla sicurezza.

Per finalità di sicurezza e risparmio energetico, computer e monitor devono sempre essere spenti al termine del loro utilizzo. Le apparecchiature devono essere disattivate anche nel caso di prolungate assenze dal servizio, pur nell'ambito dell'orario di lavoro.

In caso di assenze brevi (es. pausa mensa, riunione ecc.) durante le quali l'apparecchiatura rimane incustodita è obbligatoria l'attivazione dello screen saver (salvaschermo) protetto da password.

Al computer possono essere connesse solamente periferiche o dispositivi forniti o autorizzati dall'Azienda, da utilizzarsi esclusivamente se necessari per le attività aziendali.

Nessuna periferica o dispositivo componente la stazione di lavoro può essere rimossa, salvo specifica autorizzazione.

Il personale tecnico potrà effettuare verifiche automatizzate o puntuali sulle periferiche presenti nelle postazioni, disabilitando o rimuovendo le periferiche non autorizzate, eventualmente richiedendo giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

9.2. Computer portatili aziendali

Oltre a quanto indicato nel paragrafo precedente, gli utilizzatori dei computer portatili aziendali (includendo anche tablet, mini PC ecc.) devono seguire le seguenti istruzioni.

Il computer portatile deve essere conservato con cura sia durante gli spostamenti sia sul luogo di utilizzo aziendale o extra-aziendale, adottando idonee precauzioni per preservarlo da furti e custodendolo in luogo sicuro in caso di allontanamento, anche temporaneo.

Inoltre, in luoghi pubblici non devono essere inserite o lette informazioni di carattere riservato o critico.

La UO ICT provvederà a dotare i portatili di ulteriori sistemi di sicurezza (es. crittografia dei contenuti, sistemi antifurto ecc.).

9.3. Utilizzo di attrezzature informatiche personali

Le attrezzature personali di qualsiasi tipologia (PC, tablet, smartphone ecc.) non possono essere collegate alla rete aziendale, salvo diversa esplicita autorizzazione in forma scritta rilasciata dalla UO ICT.

In alcuni casi i dispositivi personali potranno collegarsi, previa richiesta alla UO ICT, a sottoreti appositamente predisposte nel rispetto della sicurezza della rete aziendale e pertanto destinate a funzioni limitate.

9.4. Stampanti e scanner

Salvo eccezioni particolari e giustificate (es. ambulatori, guardiole, sportelli), saranno sempre installate stampanti di rete o fotocopiatrici multifunzione (con funzione stampante e scanner) in modo da consentirne l'uso condiviso tra più uffici, settori, strutture, anche al fine di un razionale utilizzo delle risorse assegnate.

Sono distribuite esclusivamente stampanti bianco/nero, generalmente laser. Nel caso si ritenga indispensabile, per uso clinico, l'acquisto di una stampante a colori, la richiesta dovrà essere motivata e autorizzata dal Responsabile dell'UO richiedente.

È consentita la stampa solo di documenti strettamente necessari, mentre dovrà essere privilegiato l'utilizzo di documenti informatici. In caso di stampa è importante ritirarla prontamente dai vassoi delle stampanti comuni per evitare accesso indesiderato a dati personali. Si raccomanda in particolare di indirizzare verso una stampante dedicata, collocata in un'area controllata, le stampe di dati sensibili.

È buona regola, inoltre, privilegiare la stampa di documenti in modalità fronte/retro e bianco/nero in *modalità risparmio*.

In caso di necessità di stampe di documenti particolarmente lunghi o di un numero significativo di copie, si consiglia di rivolgersi al Centro Stampa.

Nell'utilizzo dello scanner accertarsi di utilizzare sempre una bassa risoluzione di scansione, in particolare prima di inviare, per es. via mail, un documento scansionato.

Si ricorda che nel caso di utilizzo di scanner deve essere rispettata la normativa sul diritto d'autore, analogamente a quanto avviene per la riproduzione di documenti attraverso fotocopiatrici. Inoltre non possono essere scansionati documenti aventi contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

9.5. Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive

L'utilizzo di supporti di memorizzazione rimovibili quali hard disk esterni, CD , DVD, memory card, pen drive, non è consentito in quanto tali supporti non garantiscono le caratteristiche di sicurezza necessarie per memorizzare dati personali, e categorie particolari di dati personali (relativi alla salute, genetici, giudiziari, etc.).

Gli utenti sono incoraggiati ad utilizzare le cartelle di rete personali e condivise.

9.6. Norme generali per l'utilizzo del software distribuito dalla UO ICT

L'autorizzato al trattamento:

- deve utilizzare il software solo per attività aziendali;
- deve custodire il software ricevuto in dotazione;
- non deve cedere il software a colleghi o a terzi;
- deve utilizzare solo il software aziendale assegnato.

Inoltre si ribadisce che:

- è vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), traduzione, distribuzione di software di terzi, che non sia autorizzata in base alla licenza a esso applicabile,
- salvo specifiche autorizzazioni, non è consentito l'uso in azienda di software acquisito privatamente o disponibile gratuitamente, né l'uso all'esterno dell'azienda di software aziendale.

9.7. Software antivirus e di protezione dei dati

La UO ICT, mediante l'utilizzo di firewall, prodotti antivirus e altri apparati di sicurezza gestiti e aggiornati centralmente, assicura la protezione dell'infrastruttura, dei sistemi informatici e delle postazioni di cui effettua la manutenzione.

L'aggiornamento dell'antivirus avviene giornalmente, quello delle patch critiche e di sicurezza di Windows avviene ogni due mesi, previa verifica in ambienti di test.

È vietato il collegamento alla rete aziendale di qualsiasi personal computer non adeguatamente protetto mediante il software antivirus aziendale e le patch di sicurezza del sistema operativo.

9.8. Dischi di rete, cartelle personali e cartelle condivise

Oltre alla cartella di rete personale connessa alle credenziali di autenticazione, l'Azienda mette a disposizione degli utilizzatori che ne fanno richiesta, dischi di rete (cartelle che possono essere accedute da uno o più utilizzatori) per l'archiviazione di informazioni di carattere professionale. Non possono essere collocati sulle unità di rete - nemmeno per periodi brevi - file personali o comunque aventi contenuto diverso da quello strettamente connesso all'attività lavorativa.

La richiesta di attivazione di tale servizio va fatta tramite il Modulo per l'utilizzo dei Servizi Informatici Aziendali (vedi anche Allegato B).

La UO ICT può svolgere periodici controlli a campione sulle unità di rete e può procedere autonomamente alla rimozione di dati non connessi alle attività proprie dell'azienda. Nel caso in cui la natura o il contenuto di informazioni/dati da collocare in rete per un utilizzo professionale potesse risultare dubbia/ambigua il titolare degli stessi dovrà informare preventivamente la UO ICT affinché non proceda alla rimozione.

La UO ICT provvede al backup dei dati collocati su unità di rete. Nel caso di perdita di dati in rete, pertanto, sarà possibile richiedere il recupero del file così come salvato nell'ultima versione di backup. Per questi motivi è fortemente consigliato l'utilizzo delle unità di rete per il salvataggio di dati/file di particolare importanza e rilevanza.

Le unità di rete devono essere mantenute con diligenza a cura degli utilizzatori; agli stessi è richiesta la periodica - almeno semestrale - revisione dei dati salvati e l'eliminazione di quelli obsoleti o, comunque, non più utilizzati o necessari. È opportuno evitare la duplicazione di dati onde consentire uno sfruttamento razionale delle unità di rete.

I server aziendali centralizzati sono le uniche entità predisposte alla condivisione di risorse. È vietato condividere localmente e direttamente dischi, cartelle o risorse (es. cartelle di scambio) a eccezione delle stampanti comuni.

Solo in situazioni di particolari problematiche tecniche, su autorizzazione della UO ICT, potranno essere attivate condivisioni fra personal computer che dovranno inderogabilmente essere protette da password di accesso.

Per ogni cartella condivisa è individuato un referente, avente la responsabilità di definire l'elenco degli utilizzatori e dei profili di abilitazione, nonché di verificare il corretto utilizzo della cartella da parte degli utilizzatori stessi.

Al referente spetta verificare periodicamente e comunque almeno annualmente, le abilitazioni assegnate agli utilizzatori, segnalando tempestivamente alla UO ICT la necessità di assegnare, modificare o cancellare l'accesso alla cartella da parte degli utilizzatori.

Il referente della cartella può individuare fino a 2 collaboratori per affiancarlo nella gestione delle abilitazioni all'uso della cartella.

Lo spazio assegnato può essere concordato di volta in volta secondo le reali necessità.

9.9. Presentazioni

È fatto divieto di inserire dati personali nelle presentazioni (es. powerpoint): si devono utilizzare dati privi di qualsiasi riferimento ai soggetti interessati. Va precisato che anche codifiche, quali il codice fiscale o altro codice, non sono ammesse in quanto possono ricondurre indirettamente ai dati identificativi del soggetto interessato.

10. Collegamento di attrezzature alla rete dati

La rete dati aziendale su cavo o wireless (wi-fi) è gestita dalla UO ICT.

L'accesso di computer o altre attrezzature alla rete aziendale deve essere autorizzato dalla UO ICT, che definisce la connettività da assegnare in base alle caratteristiche dell'attrezzatura e alle esigenze dell'utilizzatore.

10.1. Rete AUSL

La rete interna permette l'accesso a tutti i principali applicativi aziendali e pertanto è destinata all'uso da parte dell'utente aziendale esclusivamente mediante dispositivi dell'azienda.

Il collegamento alla rete di attrezzature informatiche personali, se ammesso, è regolato mediante accesso a sottoreti predisposte ad-hoc.

Pertanto sono vietati:

- Il collegamento alla rete Aziendale di computer e server se non forniti o autorizzati dalla UO ICT.
- Il collegamento alla rete aziendale di personal computer non adeguatamente protetti mediante software antivirus e patch di sicurezza del sistema operativo.
- Il collegamento alla rete, non autorizzato dalla UO ICT, di apparati di rete quali switch, router (anche USB o wifi) e attrezzature per reti wireless (es. access point).
- Qualsivoglia forma di collegamento ad altre reti laddove la stazione di lavoro sia connessa alla rete dell'Azienda USL di Bologna; sono pertanto vietate, per le stazioni di lavoro connesse alla rete aziendale, le connessioni tramite modem o chiavette Internet e l'utilizzo di una doppia scheda di rete; per i PC portatili dotati sia di scheda di rete tradizionale che di scheda di rete wireless, entrambe le schede possono essere abilitate al collegamento alla rete aziendale purché non vengano utilizzate contemporaneamente.

Le regole valgono anche per le attrezzature collegate o ospitanti strumentazioni medicali e analitiche.

10.2. Altre reti wi-fi in Azienda

Oltre alla rete dati aziendale, sia cablata che wi-fi, sono disponibili anche le seguenti reti wi-fi:

- *AlmaWifi*: rete per gli utenti universitari, con credenziali Unibo, senza accesso alla rete aziendale
- WispER - rete regionale disponibile a chiunque sia dotato di credenziali di accesso "FedERa" *fornite da una PA regionale*[3].

3 Ulteriori informazioni al link http://federazione.lepida.it/documentazione/documentazione-utente/wisper

- *EmiliaRomagnaWiFi:* rete pubblica regionale con accesso internet senza registrazione, *esterna* alla rete aziendale, disponibile a chiunque.

11. Utilizzo in Azienda di dispositivi di telecomunicazione radiomobili o wireless

A causa della concreta possibilità che le attrezzature informatiche ed elettromedicali aziendali siano soggette a malfunzionamenti legati alla presenza di sorgenti di campi elettromagnetici (es. dispositivi mobili con connessione di tipo wireless), nell'allegato C “Raccomandazioni per l'utilizzo in Azienda di dispositivi di telecomunicazione radiomobili o wireless” sono fornite indicazioni di comportamento per tutti gli operatori aziendali.

12. Uso e salvataggio dei dati aziendali

La UO ICT provvede al salvataggio dei dati registrati tramite i sistemi informativi aziendali centralizzati.

La politica di backup (creazione di copie di sicurezza), che definisce la frequenza di salvataggio e il tempo di tenuta dei backup, viene adottata dalla UO ICT in linea con indicazioni normative, raccomandazioni e best practice.

Al fine di salvaguardare tutti gli altri dati aziendali ritenuti di interesse e utilità per l'Azienda (es. documenti doc, xls, pdf, ecc.), **è vietato memorizzarli sull'hard disk dei PC**: a tale scopo dovranno invece essere utilizzati i dischi di rete e i server gestiti dalla UO ICT (vedi capitolo “Dischi di rete, cartelle personali e cartelle condivise).

Nel caso in cui l’utente ritenga sia indispensabile memorizzare dati aziendali localmente sul hard disk del PC dovrà contattare l’UO ICT per l’analisi e la definizione della soluzione più idonea.

13. Norme generali per l'utilizzo dei servizi Internet

13.1. Posta elettronica e navigazione Internet

In conformità ai requisti imposti dalla circolare AgID n.° 1/2017 non è consentito l'utilizzo di qualsiasi client locale di posta. L'unico accesso alla posta consentito deve avvenire tramite il servizo webmail del sistema di posta aziendale Zimbra che rispetta tutti i requisiti imposti dalla circolare.

Relativamente al corretto utilizzo della posta elettronica e della rete Internet si rinvia al relativo regolamento.

13.2. Pubblicazione di contenuti e realizzazione di siti personali

L'utente non è autorizzato in alcun caso a produrre e a pubblicare siti web personali utilizzando risorse aziendali né a pubblicare autonomamente siti riferiti alla struttura di appartenenza.

Ogni eventuale necessità di realizzare siti web personali o di struttura utilizzando risorse aziendali dovrà essere espressamente autorizzata dalla UO Comunicazione.

È fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza autorizzazione della UO Comunicazione.

È fatto divieto agli utenti di inserire nei siti personali collegamenti (link) al sito aziendale senza autorizzazione della UO Comunicazione.

Si applicano in ogni caso le norme dei Codici deontologici professionali.

È fatto assoluto divieto di realizzare funzioni di Hosting utilizzando risorse aziendali.

13.3. Connessione a provider diversi da quello aziendale

È vietato l'utilizzo di accessi internet mediante Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti Provider, anche con abbonamenti privati.

Infatti tali connessioni rappresentano un rischio per la sicurezza dell'intero sistema informativo aziendale di cui l'utente è pertanto consapevole.

13.4. Utilizzo dell'ambiente di cloud aziendale per la condivisione temporanea di documenti

Nel caso risulti necessario, per esigenze aziendali, condividere o inviare documenti aziendali, anche di grosse dimensioni, con persone esterne all'AUSL, è possibile utilizzare il sistema di cloud aziendale chiamato “NextCloud” reperibile all'indirizzo https://nextcloud.ausl.bologna.it.

Per accedere occorre essere abilitatati previa richiesta come indicato in Allegato B.

Tale sistema è da ritenersi un deposito temporaneo in cui i documenti devono permanere per il tempo necessario per il loro recupero da parte della persona destinataria. Si consiglia di non superare il limite di due settimane.

L'accesso ai documenti deve essere sempre consentito mediante password.

Il sistema NextCloud permette altresì all'utente aziendale stesso di poter depositare occasionalmente documenti per potervi poi accedere dall'esterno della rete aziendale, ad esempio da casa, mediante l'uso delle proprie credenziali aziendali in associazione con un secondo fattore di autenticazione (tipicamente One Time Password - OTP)

In questo caso, si raccomanda che vengano caricati su NextCloud esclusivamente i documenti per i quali vi sia necessità di accesso dall'esterno, e che al termine dell'utilizzo vengano quanto prima rimossi da NextCloud.

Il sistema NextCloud aziendale è utilizzabile, per esigenze esclusivamente aziendali, da tutti gli utenti dotati di credenziali aziendali.

L'uso temporaneo è giustificato dal fatto che il sistema aziendale NextCloud, essendo raggiungibile da internet e protetto esclusivamente mediante password+secondo fattore, non offre le medesime garanzie di protezione e sicurezza presenti nei sistemi file server interni alla rete aziendale, e pertanto non è da considerarsi una alternativa a tali sistemi bensì una integrazione per le casistiche eccezionali qui descritte.

Il tempo di permanenza di file e documenti sul cloud è comunque lasciato alla valutazione e alla responsabilità dell'utilizzatore.

13.5. Utilizzo di server esterni per backup/gestione/condivisione documenti aziendali

È vietato caricare documenti aziendali riservati e dati sensibili su sistemi di memorizzazione esterni cloud quali Dropbox, Google Drive, SkyDrive ecc.

Ciò in quanto tali sistemi possono essere soggetti ad attacchi informatici e i dati possono essere sottratti o manipolati illegalmente. Inoltre molti di tali sistemi sono ospitati in paesi non soggetti a regolamentazioni sulla privacy analoghe a quella italiana.

Non verranno pertanto effettuate abilitazioni specifiche che permettano la connessione a tali sistemi, salvo casi particolarissimi da valutare e autorizzare singolarmente (per es. accessi temporanei per prelevare dati da gruppi di lavoro già esistenti).

Gli utenti universitari e gli utenti aziendali dotati di Office nella versione online possono accedere a OneDrive mediante credenziali universitarie o aziendali; infatti in tal caso si ha la garanzia che i dati siano conservati in Europa, secondo la relativa normativa privacy, tuttavia permane il divieto di collocare su tale cloud dati riservati o sensibili.

13.6. Assistenza da remoto (VPN e altre tipologie)

Sono ammessi collegamenti remoti dall'esterno per l'accesso alle risorse aziendali, sia per manutenzione di attrezzature da parte di ditte esterne, sia per lo svolgimento di specifiche attività da una sede esterna, ma devono essere autorizzati dalla UO ICT.

In particolare, per quanto riguarda lo smartworking, le modalità di richiesta, autorizzazione, formazione, accesso sono descritte sulla intranet aziendale.

14. Modalità di prestazione dei servizi

La UO ICT si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità di interromperli esclusivamente per le manutenzioni ordinarie e cercando di arrecare il minor disagio possibile agli utilizzatori. Salvo impedimenti le interruzioni saranno comunicate agli utenti.

Per poter fornire assistenza e supporto tempestivi nel caso di guasti e malfunzionamenti, su ciascun computer fisso o portatile è installata un'applicazione che consente ai tecnici della UO ICT di collegarsi remotamente, senza bisogno di intervenire sul luogo.

Pertanto la manutenzione alle stazioni di lavoro viene generalmente effettuata, in prima battuta, mediante tali sistemi software di manutenzione remota. Solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento in loco.

Si informa che i sistemi di controllo remoto suddetti sono configurati affinché gli operatori che intervengono per la manutenzione possano farlo esclusivamente previo consenso dell'utilizzatore della postazione (consenso che viene richiesto in tempo reale sullo schermo del pc); non sarà richiesta l'autorizzazione solo nei casi in cui si renda necessario effettuare installazioni o aggiornamenti software da remoto, che non prevedono la possibilità di accesso ai dati presenti.

Inoltre l'utente può verificare l'attività effettuata in remoto dal tecnico rimanendo presso la postazione.

In casi di emergenza/urgenza, in particolare nel caso in cui la sicurezza informatica possa essere pregiudicata ma non solo, il personale tecnico potrà comunque effettuare interventi sulle postazioni senza alcun preavviso, anche in assenza dell'utente utilizzatore della postazione.

Gli interventi sono eseguiti da personale identificato e autorizzato dalla UO ICT: tale personale afferisce alla UO ICT direttamente o tramite contratti di fornitura di servizi.

15. Acquisto su progetti finanziati (PO)

Tra i servizi erogati dalla UO ICT vi è anche l'acquisto di beni e servizi informatici per l'attività ordinaria aziendale e per la realizzazione di progetti obiettivo con finanziamenti dedicati. Utilizzando fondi derivanti da progetti finanziati si possono acquistare solo attrezzature analoghe a quanto viene acquistato con fondi "standard", ciò anche in ottica di ottimizzare l'assistenza tecnica ai sistemi e alle infrastrutture. Eventuali eccezioni devono essere giustificate e autorizzate.

16. Installazione di Microsoft Office sulle postazioni di lavoro

Sui PC di nuova fornitura vengono installati preventivamente sistemi open di automazione d'ufficio (es. Libre Office).

E' comunque prevista l'installazione di MS-Office, su richiesta, per esigenze specifiche, che devono essere adeguatamente motivate e autorizzate, quali:

- procedure aziendali che richiedano necessariamente l'utilizzo di MS Office
- necessità di compatibilità con vecchie procedure Access
- gestione di documenti che presentano evidenti incompatibilità con i sistemi open.

Si precisa che le licenze di MS Office installabili sui PC aziendali sono solo quelle acquistate dall'Azienda (non sono ammesse né licenze personali né licenze universitarie).

Sui PC universitari sono installabili solo le licenze fornite da UniBO.

17. Disposizioni finali

17.1. Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente regolamento, la disponibilità a un utente dei servizi informatici aziendali cesserà totalmente nel caso non sussista più la condizione di dipendente o di collaboratore esterno, ad eccezione della firma digitale remota e dell'accesso al portale del dipendente GRU RER, i cui utilizzi sono consentiti fino a scadenza validità, per la firma remota, e di norma fino a 18 mesi dopo la pubblicazione dell'ultimo documento pubblicato relativo al dipendente (cedolino

stipendiale, CU), per il Portale GRU, oltre la data di cessazione del rapporto di lavoro; inoltre può cessare o essere limitata nei privilegi assegnati in caso di:

- revoca dell'autorizzazione all'uso fornita dal Referente privacy (per es. per cambio di mansione, ruolo, CDR ecc.);
- accertato uso non corretto o comunque estraneo alla sua attività lavorativa dei servizi informatici aziendali;
- accertate manomissioni e/o interventi illeciti sul hardware e/o sul software;
- accertate diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. e altre informazioni tecniche riservate;
- accesso illecito e intenzionale dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili, in particolare se l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- violazione delle regole essenziali stabilite dal presente regolamento.

Si precisa che in caso di cessazione della condizione di dipendente o collaboratore a una certa data la casella di posta dell'utente sarà immediatamente bloccata. A partire da tale data non sono consentiti né l'accesso alla casella, né la ricezione tramite inoltro. Saranno inoltre cancellati tutti i dati e i documenti presenti nella cartella personale di rete associata alle credenziali di autenticazione.

Casi particolari in deroga alla precedente disposizione devono essere esplicitamente autorizzati dalla direzione aziendale.

Si ricorda inoltre che, una volta cessata la condizione di dipendente o collaboratore è vietato asportare dati aziendali prodotti nell'attività istituzionale. Non sarà dato seguito, pertanto, alla richiesta di scarico massivo (per es. su supporto esterno) delle mail dell'utente, né di altri file contenuti nei file server o nei personal computer.

17.2. Responsabilità dell'utilizzatore delle risorse informatiche

- L'utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di posta elettronica e di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
- All'utente è consentito di utilizzare il servizio solo per ragioni professionali connesse alla propria attività, in modo individuale, salvo eccezioni riportate del relativo regolamento.
- Con l'accettazione di questo regolamento l'utente è informato e consapevole del fatto che la conoscenza della password da parte di terzi consente a questi ultimi l'accesso alla rete aziendale e l'utilizzo dei relativi servizi in nome dell'utente e l'accesso ai dati cui il medesimo è abilitato, con le conseguenze che la cosa può comportare, quali ad esempio la visualizzazione di informazioni riservate, la distruzione o la modifica dei dati, la lettura della propria posta elettronica, l'uso indebito di servizi ecc.
- L'utente prende atto che è vietato servirsi o dar modo ad altri di servirsi della rete aziendale e dei servizi da essa messi a disposizione per utilizzi illeciti che violino o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica o privata, per recare offesa o danno diretto o indiretto all'Azienda o a terzi.
- E' vietato all'utente che disponga dei diritti per farlo, alterare le impostazioni del sistema operativo o degli applicativi in senso contrario a quanto indicato dalla circolare AgID n.° 1/2017 (es. attivazione dell'esecuzione automatica di macro nei file di office, visualizzazione automatica del contenuto dei file ecc).

17.3. Informativa sul trattamento dei dati da parte della UO ICT

Ai sensi del GDPR si informa che i dati relativi all'utilizzo dei servizi informatici da parte degli utenti sono trattati nel rispetto della legge e degli obblighi di riservatezza cui è ispirata l'attività dell'AUSL.

Il trattamento dei dati si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza e all'identità personale e al diritto di protezione dei dati personali.

Finalità e modalità del trattamento

L'AUSL si impegna a trattare i dati relativi all'utilizzo dei servizi informatici unicamente per motivi volti a garantire la sicurezza e il corretto funzionamento dei servizi informatici e per finalità direttamente pertinenti all'attività lavorativa del dipendente.

Le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate per finalità di sicurezza del sistema.

L'attività di registrazione avviene attraverso i file “log” di sistema a cura della UO ICT o dell'articolazione aziendale che detiene la responsabilità organizzativa dei sistemi o servizi.

Per quanto riguarda l'utilizzo dei sistemi informativi aziendali, le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate al fine di garantire la tracciabilità del trattamento dei singoli dati. Le informazioni relative alla tracciabilità del dato (visualizzazione, inserimento, modifica, cancellazione) vengono gestite con le stesse modalità del dato a cui si riferiscono.

Per quanto riguarda l'accesso ai servizi di posta elettronica e internet, la UO ICT garantisce la custodia dei file “log” per il tempo indicato da fonti normative o regolamentari (per es. di AgID).

Le registrazioni potranno essere utilizzate, su richiesta del Titolare o dei Referenti privacy, per finalità statistiche e di valutazione della qualità in riferimento a taluni servizi erogati, esclusivamente da parte di personale dell'Azienda appartenente alla UO ICT.

L'AUSL si riserva di effettuare dei controlli, anche a campione, concernenti l'utilizzo corretto degli strumenti di lavoro, fermo restando il divieto di controllo a distanza dei lavoratori stabilito dall'art. 4 della L. 20.5.1970, n. 300.

Comunicazione e diffusione

I dati relativi all'utilizzo degli strumenti informatici sono trattati, per le finalità indicate al punto precedente, dagli operatori della UO ICT e possono essere portati a conoscenza, esclusivamente nei casi consentiti dalla legge, del responsabile della U.O. di appartenenza dell'utente.

Infine i log potranno essere oggetto di provvedimenti dell'Autorità giudiziaria e amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo all'interno dell'Azienda.

Titolarità

Titolare del trattamento dei dati è l'Azienda USL di Bologna, legalmente rappresentata dal Direttore Generale pro-tempore, con sede legale in Bologna, Via Castiglione, 29.

Il Direttore Generale ha nominato Referenti privacy; Direttori di Unità Operativa Complessa (SC), Dirigenti Responsabili di Unità Operativa Semplice Dipartimentale (UOSD), Direttori di Programmi Gestionali (del. n. 11 del 14/1/2019).

Diritti dell'utente “interessato”

A seguito del trattamento dei dati, si possono esercitare i diritti previsti dal GDPR, e più precisamente l'utente, in qualità di “interessato”, può conoscere i dati trattati, nonché può richiedere l'aggiornamento, la rettifica e, ove abbia interesse, l'integrazione, nonché le altre prerogative previste dalla Legge.

È possibile in qualsiasi momento far valere i diritti sopra specificati di cui all'art. 7 del GDPR con richiesta avanzata al Titolare o al Direttore della UO ICT.

Allegato A - Elenco applicativi di base e specifici autorizzati

Applicativi di base (sono esclusi dall'elenco i sistemi operativi)

#	Applicativi di base	Note
AB1	Kaspersky antivirus	11.6.0.394
AB2	Oracle 8.1.7 ADS/9/10g/11g	Oracle 8.1.7/9/10g/11gR2/12
AB3	Java Runtime Environment 1.6 update 25 o 1.7 update 09	La versione dipende dal tipo di applicativi installati
AB4	.Net Framework 3.5 Sp3	Su Windows 10 .Net framework 4.0 4.5 o superiore
AB5	Oracle Jinitiator	1.3.1.22
AB6	Adobe Reader	7 – 8 – 9 – 10 – 11 - DC
AB7	PdfCreator	8.2.0
AB8	Peazip	7.8.0
AB9	CdburnerXp	4.5.8
AB10	Vlc	2.2.4 3.0.12
AB11	LibreOffice	4.4.2 7.1.2
AB12	Open VPN	2.4.3 2.4.5 installato solamente per comprovate esigenze
AB13	Mozilla Firefox 41 o superiore	41.0.2
AB14	Google Chrome	80
AB15	Bomgar	19.2.4

Applicativi specifici

#	Applicativi Amministrativi	Utilizzo	Note
AA1	ADIUVAT	Distretti, Front-office, Back office, RRF dei vari Ospedali	Webapp & RDP
AA2	AS400	UOC Amministrazione del Personale, UOC Economico Finanziario	RDP
AA3	AVELCO – AVELCO WEB	Dipartimento Sanità Pubblica	Webapp & RDP
AA4	BABEL	Tutti gli amministrativi	Webapp
AA5	BUSINESS OBJECT AND ODBC	UOC Flussi Informativi	Web & Locale
AA7	EUSIS PORTALE	Tutti	Web & Locale
AA8	FEP	UOC SUMAGP e SUMAEP	10 utenze
AA9	FIRMA DIGITALE	Tutti gli amministrativi	Web app
AA11	JOBTIME E MEDICI CONVENZIONATI	Amministrativi	RDP
AA12	MAP	Amministrativi	Webapp
AA13	MATRIX	Contabilità usato dal Dipartimento Tecnico	Client
AA14	ALISEO (NHR)	UOC SUMAGP e SUMAEP	RDP
AA15	ORDINATIVO INFORMATICO	Amministrativi	Webapp ex Mandato
AA16	PROTOCOLLO E DELIBERE	Amministrativi	Solo consultazione
AA17	RECUPERO CREDITI	Distretto	Client
AA18	REPORTMED	Controllo gestione, flussi amministrativi	
AA19	SCRIVANIA VIRTUALE	Tutti gli amministrativi	Solo consultazione

AA20	SINFO-F7	Amministrativi	10 utenze
AA21	SORIWEB	Reparti, Cucine	Webapp
AA22	SSI	Formazione, Amministrativi	Su Citrix
AA23	VCQL: Verifica e Controllo Qualità Lungodegenza	Attività con case di cura private e convenzionate	10 utenze
AA24	VITTO	Reparti, Cucine	Client
AA25	GRU RER (WHR-TIME)	Gestione risorse umane - amministrativi	Webapp
AA26	MAESTRO	Amministrativi	RDP
AA27	SAS ENTERPRISE	Amministrativi	Client

#	Applicativi Sanitari	Utilizzo	Note
AS1	ANMCO CARDIO G8	Cardiologia	
AS2	AREAS	Tutti i clinici	Webapp
AS3	ATHENA	Anatomia patologica	Webapp
AS4	ANAGRAFE CANINA	Veterinari	Client
AS5	CARDIOREF	Cardiologia	RDP
AS6	CARTELLE CLINICHE (CARCERE)	Ambulatori carcere	Terminal server DB Access Webapp
AS7	CEDAP	Clinici	Webapp
AS8	DIABETE	Clinici	Webapp
AS9	DIGISTAT	Sale Operatorie	Client
AS10	DNLAB	Laboratorio analisi, Clinici	Webapp
AS11	DNTERR	Clinici del Territorio	Webapp
AS12	DNWEB	Clinici	Webapp
AS13	ELEA	Neuropsichiatria infantile	Webapp
AS14	ELIOT	Servizio trasfusionale	Client & Webapp
AS15	EUROTOUCH	Diabetologia OM	20 utenze
AS16	GALILEO	Tutti i clinici	Webapp
AS17	GARSIA ADI E GEAC	Assistenza domiciliare	Rdp
AS18	GARSIA HANDYCAP E FORMAZIONE	Case riposo, Formazione	Webapp
AS19	GARSIA WE	Distretto	Webapp
AS20	GEDO	Clinici	Solo consultazione
AS21	GESIWEB	Clinici	Webapp
AS22	Onvac	Profilassi	Webapp
AS23	ISESWEB	Cup	Webapp
AS24	LOG 80	Clinici	Webapp
AS25	MILLEWIN	Medicina di base	Client
AS26	MY SANITA’	Clinici	Webapp
AS27	PARMA	Clinici	Client
AS28	PATHWIN ANATOMIA PATOLOGICA	Anatomia patologica	Solo consultazione
AS29	POLARIS	Tutti i clinici	Webapp
AS30	SIR	Clinici	Client
AS31	SISTER 2 / SISTER 4	SERT	Webapp
AS32	SIT	DSM	Webapp
AS33	SCREENING	Clinici	Web & RDP
AS34	SILOR	Sale operatorie sul territorio	Webapp
AS35	REGISTRO ANESTESIOLOGICO	Sale operatorie sul territorio	In via di sostituzione
AS36	WINSIMET	SERT	Client
AS37	SIO	Clinici	In consultazione, sostituito da Areas RDP

AS38	CARTELLE CLINICHE	Accoglienza e URP	Webapp
AS39	DEMETRA	Screening	Webapp
AS40	KODAK CARESTREAM	Radiologia	Client
AS41	ARA	Front Office - Cup	WebApp
AS42	CASA DELLA SALUTE	Tutti i clinici	Webapp
AS43	SCCE	Reparti clinici	Webapp
AS44	DIETE SANIGRAFIA	Dietiste	Client
AS45	JUNIORBIT	Pediatria	RDP
AS46	MARGHERITA 3	Rianimazione	Client
AS47	MEMO TRACK II	Trasfusionale	Client
AS48	OFFERTA AGENDA	Agende cup	Webapp - Client
AS49	SERENA	Clinici	Webapp
AS50	SISTEMA INFORMATIVO TRAPIANTI	Clinici	Webapp
AS51	REGISTRO MALATTIE RARE	Clinici	Webapp
AS52	UFFICIO PATENTI	Clinici	Webapp
AS53	WEBCALL	Ing. Clinica	Webapp
AS54	CARESTREAM VUEMOTION	Radiologia	Webapp
AS55	CUPWEBALP	CUP	Webapp

Allegato B - Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente

Per accedere ai servizi informatici aziendali qualsiasi nuovo utente dovrà fornire i propri dati personali, prendere visione del presente regolamento e compilare il modulo per l'utilizzo dei servizi informatici aziendali.

Il modulo dovrà essere consegnato alla struttura aziendale deputata alla creazione degli accessi ai sistemi o servizi di cui si richiede l'abilitazione (corrispondente alla UO ICT nella maggioranza dei casi), firmato dal Responsabile della struttura organizzativa a cui l'utente appartiene.

Nel caso dei sistemi informativi aziendali centralizzati (es. Anagrafe Sanitaria, GRU, Farmacia ecc.), va raccolta la firma per autorizzazione anche del Responsabile organizzativo dei sistemi o servizi di cui si richiede l'abilitazione.

Nella Intranet aziendale, seguendo il percorso “Articolazioni Organizzative”, “Dipartimento Tecnico Patrimoniale”, “UO Tecnologie Informatiche e di Comunicazione (SC)”, si ha accesso alla modulistica (https://intranet.internal.ausl.bologna.it/servizi/dip/dip_tecn_patr/serv_ced/mod_ced/ModUsoSistInf.pdf) per effettuare la richiesta di abilitazione all'utilizzo di servizi e procedure informatiche:

L'utilizzo dei servizi informatici aziendali richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) e una parola chiave segreta (password).

Nel caso di disattivazione del codice di identificazione personale, per riottenere l'accesso ai servizi l'utente dovrà compilare nuovamente il modulo per l'utilizzo dei servizi informatici aziendali, allegare la fotocopia di un documento di identità e consegnarlo alla UO ICT firmato dal Responsabile della struttura organizzativa a cui l'utente appartiene.

In caso di rinnovo la password può essere consegnata esclusivamente in due modalità:

1. Inviata con sms a un cellulare fornito dall'utente;
2. ritirata di persona.

In nessun caso può essere fornita al telefono o inviata con altri mezzi.

La password non potrà essere ceduta a terzi, neppure temporaneamente e dovrà essere mantenuta segreta.

Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.

Non sono previsti codici di accesso anonimi.

L'utente deve conservare la password con la massima riservatezza e con la massima diligenza. La password non deve essere banale né contenere riferimenti facilmente riconducibili all'utente.

È modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni tre mesi.

Il cambio password può essere eseguito agevolmente dall'utente autonomamente collegandosi dalla Intranet nella sezione *Strumenti* al link *Cambio password*. (https://web-ldap.internal.ausl.bologna.it/cimarosa/passwd.htm) o da interntet al link https://ldap.ausl.bologna.it

Dopo sei mesi di non utilizzo dei servizi, o nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali, la userid e la password vengono automaticamente disattivati. In quest'ultimo caso, i messaggi di posta elettronica in giacenza vengono eliminati.

L'utente si impegna a comunicare immediatamente alla UO ICT l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi della password.

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE

UO Tecnologie Informatiche e di Comunicazione (SC)

MODULO PER L'UTILIZZO DEI SERVIZI INFORMATICI AZIENDALI

da inviare al fax **0516478345** – breve **38345**

Richiedente	
Direzione /Gestione /Unità Operativa	
Data	
Numero Telefonico di Riferimento	

Servizi o sistemi informatici di cui si richiede l'attivazione,
disattivazione o riattivazione dell'utilizzo

Dati dell'incaricato

Cognome			
Nome			
Codice Fiscale			
Cellulare (per il reset della password)			
Indirizzo posta elettronica			
Servizio di appartenenza			
Indirizzo sede di lavoro			
Profilo (medico, infermiere, amministrativo,.)			
Data attivazione		Data disattivazione	

Il Responsabile del Servizio richiedente

Cognome e nome *(timbro e firma)*	

L'incaricato dichiara di aver preso visione del "Regolamento per l'utilizzo dei servizi informatici aziendali" e di accettare sotto la propria responsabilità tutte le condizioni ivi contenute.

In fede _____

Il Responsabile organizzativo

Cognome e nome *(timbro e firma)*	

Revisione N.3 del 28-10-2021

Allegato C - Raccomandazioni per l'utilizzo in azienda di dispositivi di telecomunicazione radiomobili o wireless

1. Definizioni

Campo elettromagnetico

Fenomeno fisico che consiste nell'esistenza contemporanea di un campo elettrico e di un campo magnetico mutuamente accoppiati al punto da costituire un'unica entità fisica. L'intensità del campo elettromagnetico diminuisce con la distanza dalla sorgente.

Le fonti di campo elettromagnetico sono le più svariate: apparecchi elettrici e elettronici, radio, televisione, radar, antenne per la telefonia cellulare, forni a microonde ecc.

Compatibilità elettromagnetica (EMC)

La capacità di un sistema o apparato elettrico e/o elettronico di funzionare correttamente nel suo ambiente elettromagnetico senza introdurre disturbi che possano interferire con il funzionamento di altre apparecchiature presenti nello stesso ambiente.

Interferenza elettromagnetica (EMI)

La sovrapposizione in un ambiente di segnali elettromagnetici riferibili a diversi dispositivi, tale da poter indurre disturbi al corretto funzionamento dei dispositivi stessi.

Dispositivo di telecomunicazione portatile

Apparecchiatura radiomobile aziendale o personale (es. smartphone, tablet, chiavette UMTS/LTE, router mobili, cordless, PC portatili ecc.)

Dispositivo elettromedicale (DM)

Qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche o terapeutiche e necessario al corretto funzionamento del dispositivo, destinato dal fabbricante ad essere impiegato sull'uomo a fini di diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia; di diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi (Art. 1 D. Lgs. 46/97 e s.m.i.)

Wireless

Comunicazione tra dispositivi elettronici che non fa uso di cavi. Per estensione sono detti wireless i rispettivi sistemi o dispositivi di comunicazione che implementano tale modalità di comunicazione. Sono wireless le tecnologie di comunicazione basate su onde radio come il Bluetooth, il Wi-fi, le reti cellulari (GSM, GPRS, EDGE, UMTS), le reti satellitari ecc.

Wi-fi

Standard (IEEE 802.11) per collegamenti wireless ad alta fedeltà attuati su bande a radiofrequenza specifiche.

Access point

Dispositivo elettronico di telecomunicazioni che, collegato ad una rete cablata, o anche, per esempio, ad un router, permette all'utente mobile di accedervi in modalità wireless direttamente tramite il suo terminale, se dotato di scheda wireless.

2. Premessa

La grande diffusione e l'incalzante sviluppo tecnologico dei sistemi di telecomunicazione portatili introducono un nuovo fattore di rischio nelle aree destinate a un uso sanitario, in quanto si presenta la concreta possibilità che tali sorgenti di campi elettromagnetici possano essere utilizzate in stretta prossimità di dispositivi elettromedicali (DM). Come è noto questa condizione è una fonte potenziale di malfunzionamento di tali dispositivi. Si tratta del fenomeno noto con il termine di interferenza elettromagnetica (EMI = ElectroMagnetic Interference), che solo recentemente ha ricevuto l'attenzione dovuta da parte sia della comunità scientifica sia degli enti tra i cui fini figurano la promozione e la tutela della salute.

3. Scopo del documento

Questo documento ha lo scopo di fornire alcune raccomandazioni per l'utilizzo dei dispositivi mobili con connessione di tipo wireless, ovvero dei dispositivi in grado di emettere in varia misura un significativo campo elettromagnetico, ai fini di una corretta prevenzione dei possibili effetti sulla salute dei pazienti e del personale che accede o opera presso le strutture aziendali, con particolare riferimento alla compatibilità elettromagnetica e alle potenziali interferenze con altri dispositivi elettromedicali e di telecomunicazione presenti nell'Azienda USL di Bologna.

I destinatari del presente regolamento sono pertanto:

- Il personale interno all'Azienda (medici, infermieri, dipendenti, convenzionati, collaboratori ecc.).
- I pazienti, i loro accompagnatori e i visitatori.
- Il personale esterno all'Azienda (fornitori, consulenti, addetti alla manutenzione ecc.).

4. Dispositivi oggetto di regolamentazione

Di seguito si riporta una lista, da ritenersi non esaustiva in quanto soggetta a continua evoluzione, dei dispositivi oggetto della presente regolamentazione, che è da intendersi estesa in via generale a tutti i dispositivi in grado di emettere un campo elettromagnetico:

- Dispositivi Radiomobili Privati dell'Azienda e in particolare del servizio 118 (analogici, a standard Tetra ecc.).
- Dispositivi Radiomobili Aziendali e Personali con connettività anche GSM/UMTS/LTE (telefoni cellulari GSM, smartphone UMTS/LTE/Wi-Fi, Tablet UMTS/LTE/Wi-Fi, chiavette USB UMTS/LTE, Router Mobile Wi-Fi/UMTS/LTE ecc.).
- Dispositivi cordless telefonici o con connettività fonia/dati solo wi-fi e/o bluetooth: cordless telefonici, telefoni wi-fi, tablet e PC portatili wi-fi, auricolari ecc.
- Cercapersone.
- Altri dispositivi assimilabili ai casi precedenti.

5 Classificazione

Per maggiore semplicità di trattazione, i dispositivi di cui al punto precedente possono essere raggruppati nelle seguenti macro categorie o tipologie:

- **Tipo A**: dispositivi radiomobili privati dell'Azienda e in particolare del servizio 118 (analogici, a standard Tetra, ecc.), ovvero dispositivi in grado di emettere un campo elettromagnetico non trascurabile fino a qualche metro di distanza.
- **Tibo B**: dispositivi radiomobili pubblici aziendali e personali (telefoni cellulari GSM, smartphone UMTS/LTE/Wi-Fi, Tablet UMTS/LTE/Wi-Fi, chiavette USB UMTS/LTE, Router Mobile Wi-Fi/UMTS/LTE ecc.), ovvero dispositivi in grado di emettere un campo elettromagnetico non trascurabile fino a diverse decine di centimetri di distanza.
- **Tipo C**: es. dispositivi cordless telefonici o con connettività fonia/dati solo wi-fi e/o bluetooth, quali cordless telefonici, telefoni wi-fi, tablet e PC portatili wi-fi, auricolari, ecc., ovvero dispositivi in grado di emettere un campo elettromagnetico non trascurabile anche fino a qualche centimetro di distanza. Rientrano in questa classe anche gli access point wi- fi

- **Tipo D**: es. dispositivi cercapersone in sola ricezione (dispositivi cercapersone bidirezionali, che possono trasmettere anche dati e/o fonia in continuità che potrebbero essere meglio raggruppati, a seconda della tecnologia utilizzata, in una delle categorie superiori).

6. Metodologia di lavoro e documentazione

In carenza di documentazione certificata e di supporto normativo, le informazioni e raccomandazioni del presente documento derivano dallo studio eseguito da un gruppo multidisciplinare costituito nel 2015 presso l'Azienda USL di Bologna che, con la collaborazione di un supporto professionale esterno[4], ha realizzato dettagliate misure dell'inquinamento elettromagnetico generato da una molteplicità di apparecchiature.

Tutti i dati riportati sono rilevati con i sistemi in funzione ovvero durante una conversazione o in trasmissione e ricezione dati.

In estrema sintesi si è rilevato che:

1. I sistemi tablet aziendali, i cordless e i cellulari smartphone aziendali di ultima generazione generano un campo elettromagnetico ridotto (il rischio si presenta in prossimità o quasi a contatto dei DM). Gruppi B, C e D
2. I sistemi radio in uso al 118 presentano un rischio da interferenza piuttosto elevato. Lo stesso grado di rischio potrebbe aversi con i telefoni cellulari di più vecchia generazione. Gruppo A.

Per approfondimenti sui test eseguiti dal gruppo di lavoro presso l'Azienda USL di Bologna è possibile visionare l'allegato 1, in cui sono riportati anche i riferimenti normativi disponibili e a cui si rinvia per ogni dettaglio.

7. Raccomandazioni

L'utilizzo dei telefoni cellulari per ragioni di lavoro in ambito sanitario, in particolare per arricchire il patrimonio informativo su casi clinici o per la sicurezza, porta un sicuro miglioramento ai percorsi di cura dei pazienti. Tuttavia, anche alla luce di recenti pubblicazioni, che riportano incidenti o eventi sentinella correlati all'utilizzo non controllato e disattento del cellulare come causa di una diminuzione dell'attenzione durante l'effettuazione di attività sanitarie articolate e complesse, si raccomanda di utilizzarli in modo limitato e solo in caso di necessità. A questo si aggiunga che in relazione alla possibile interferenza che tali apparati possono avere con il funzionamento di dispositivi elettromedicali è necessario che l'utilizzo avvenga secondo alcune semplici raccomandazioni di cautela e di prudenza qui di seguito elencate.

Ciò premesso, valgono le seguenti raccomandazioni:

Dispositivi di **tipo A**

Deve essere evitato l'utilizzo in prossimità di dispositivi elettromedicali. Se in conversazione la distanza di sicurezza raccomandata è di **almeno 3 metri**. In stand by o in solo ascolto sono assimilabili ai dispositivi di classe B.

Dispositivi di **tipo B, C e D**

Deve essere evitato l'utilizzo in estrema prossimità di dispositivi elettromedicali. Se in conversazione o in trasmissione dati la distanza di sicurezza raccomandata è di **almeno 30 centimetri**. Nella modalità stand by la distanza può scendere fino a un massimo di 10 cm.

Access point Wi-Fi e dispositivi Wi-Fi mobili

I dispositivi che emettono il segnale dati e che nel loro insieme costituiscono la rete Wi-Fi aziendale (access point), seguono le regole di cui al punto precedente (classe C). Poiché essi sono in genere posizionati sulle pareti o sul soffitto non sussiste il rischio di interferenze. Tuttavia particolare attenzione va posta nel caso di dispositivi elettromedicali posizionati su carrelli nel caso questi fossero disposti in estrema prossimità di un access point fisso. In particolare quest'ultimo potrebbe

4 Laboratori Guglielmo Marconi S.p.A.

essere accidentalmente o intenzionalmente rimosso dalla sua posizione fissa e quindi trovarsi in area a rischio interferenza.

Infine si assiste alla diffusione di dispositivi Wi-Fi mobili, peraltro di minuscole dimensioni, collegati alla rete dati pubblica mediante SIM dati. Questi oggetti potrebbero essere posizionati in prossimità di un dispositivo elettromedicale dallo stesso paziente o da parenti e visitatori o anche dalle ditte esterne in caso per es. di interventi per manutenzione. Anche per questi casi si raccomanda la massima attenzione e di seguire le indicazioni date.