AO Brotzu

Deliberazione 301

Adottata dal DIRETTORE GENERALE in data 07 FEB. 2019

Oggetto: Approvazione del "Regolamento aziendale sull'uso degli strumenti informatici dell'Azienda Ospedaliera Brotzu"

Pubblicata all'Albo Pretorio dell'Azienda a partire dal 08 FEB. 2019 per 15 giorni consecutivi e posta a disposizione per la consultazione.

Il Direttore Amministrativo

Il Direttore Generale Dott.ssa Graziella Pintus

coadiuvato da

Direttore Amministrativo Dott.ssa Laura Balata
Direttore Sanitario Dott. *Vinicio Atzeni*

Su proposta della S.C. "Tecnologie Informatiche e Servizi Informativi"

VISTO

- il Regolamento UE N. 2016/679 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);

- il D.Lgs n. 101 del 10 agosto 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/C£E (regolamento generale sulla protezione dei dati);

PREMESSO

- che la principale novità introdotta da Regolamento UE N. 2016/679 consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio in luogo del precedente approccio basato su adempimenti, consegnando quindi la protezione dei dati al Titolare del trattamento che, grazie al principio di responsabilizzazione *("accountability")* adotterà, secondo quanto previsto dal Regolamento, le misure che riterrà più opportune per garantire il trattamento dei dati personali;

- altresì che implementare il sistema privacy secondo quanto previsto dal GDPR significa generare nell'organizzazione la piena consapevolezza dei rischi relativi ai trattamenti dei dati e le responsabilità connesse, nonché la cultura della protezione dei dati quale parte integrante dell'intera struttura informativa dell'organizzazione, con particolare attenzione ai dati sanitari e ai dati sensibili (ora denominati "categorie particolari di dati") sotto il profilo dei diritti e delle libertà fondamentali dell'individuo;

CONSIDERATO

- che l'art.37 del GDPR prevede che venga nominato il *Data Protection* Officer (DPO) ovvero del Responsabile per la Protezione dei Dati;

- che l'art.24 del GDPR prevede che, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento effettuato è conforme a quanto stabilito nel GDPR;

RITENUTO di dover procedere alla predisposizione e alla divulgazione delle policy aziendali sulla protezione dei dati al fine di fornire ai professionisti le indicazioni operative necessarie a garantire una maggiore sicurezza sulle modalità di trattamento dei dati personali anche attraverso l'utilizzo degli strumenti informatici;

VISTO il "Regolamento aziendale sull'uso degli strumenti informatici dell'Azienda Ospedaliera Brotzu", allegato alla presente deliberazione per farne parte integrante e sostanziale, a tal fine predisposto;

CON il parere favorevole del Direttore Amministrativo nonché del Direttore Sanitario e sentito il Data Protection Officer

DELIBERA

Per i motivi esposti in premessa:

1) di approvare il "Regolamento aziendale sull'uso degli strumenti informatici dell'Azienda Ospedaliera Brotzu", allegato alla presente deliberazione per farne parte integrante e sostanziale;

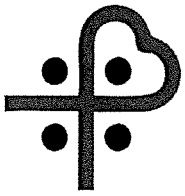
2) di demandare alla S.S.D. Affari Generali la pubblicazione della presente deliberazione sul sito Aziendale, nella sezione Amministrazione Trasparente.

Il Direttore Amministrativo
Dott.ssa Laura Balata

Il Direttore Sanitario
Dott. Vinicio Atzeni

Il Direttore Generale
Dott.ssa Graziella Pintus

Resp. S.C. "Tecnologie Informatiche e Servizi Informativi" A. Alimonda



Azienda Ospedaliera G. Brotzu

REGOLAMENTO AZIENDALE SULL'USO DEGLI STRUMENTI INFORMATICI DELL'AZIENDA OSPEDALIERA BROTZU

SOMMARIO

GLOSSARIO:

designato: la persona fisica autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, e a cui il titolare o il responsabile attribuisce specifici compiti e funzioni connessi al trattamento di dati personali.

dominio Windows Server: servizio di rete aziendale che contiene gli account degli utenti e le informazioni di protezione e condivisione delle risorse (postazioni di lavoro, stampanti, etc.).

responsabile o responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

titolare o titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

1. Oggetto e ambito di applicazione.

Il presente regolamento disciplina le modalità di accesso e di utilizzo della rete informatica dell'Azienda e dei servizi che - tramite la stessa rete - è possibile ricevere o offrire all'interno o all'esterno dell'Azienda Ospedaliera Brotzu.
È interessato dal presente regolamento tutto il personale dipendente ed il personale non dipendente fornito delle necessarie autorizzazioni per l'accesso alla rete aziendale.
L'utente si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi svolti attraverso la rete, e a non commettere abusi e violazioni dei diritti degli altri utenti e dei terzi.

2. Criteri generali relativi alle modalità di accesso alla rete aziendale, ai servizi (posta elettronica, applicativi) e all'utilizzo di dispositivi aziendali e personali

2.1. L'utilizzo della rete aziendale è ammesso per l'espletamento dei compiti e delle finalità istituzionali dell'Azienda Ospedaliera Brotzu.

2.2. L'accesso alla rete aziendale e ai servizi (posta elettronica, applicativi) è associato ad una persona fisica cui imputare le attività svolte, e che se ne assume la totale responsabilità.

2.3. L'accesso alla rete aziendale è protetto da password. Per l'accesso deve essere utilizzato il proprio profilo personale.

2.4. È vietato lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti atti ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità di sicurezza dei sistemi, decriptare file crittografati o compromettere la sicurezza della rete aziendale in qualsiasi modo.

2.5. È vietato lo svolgimento di attività che violino la riservatezza di altri utenti o di terzi, che influenzino negativamente la regolare operatività di rete e dei sistemi, nonché attività di monitoraggio del traffico della rete aziendale.

2.6. È vietato effettuare attività che provochino trasferimenti non autorizzati di informazioni. In particolare è vietato duplicare, portare all'esterno dell'ambito aziendale o dall'ufficio qualsiasi dispositivo di memorizzazione (di qualsiasi natura) contenente dati nella disponibilità dell'Azienda, o relativi alle attività da quest'ultima poste in essere in assenza di preventiva ed espressa autorizzazione.

2.7. È vietato l'utilizzo dell'anonimato o servirsi di risorse che consentano di restare anonimi.

2.8. È vietato l'utilizzo di dispositivi non autorizzati dalla SC "Tecnologie Informatiche e Servizi Informativi". L'Azienda Ospedaliera si riserva il diritto di eliminare qualsiasi dispositivo la cui installazione non sia stata appositamente prevista o autorizzata. In particolare, è vietata l'installazione e l'utilizzo di apparati di rete (hub, switch, access point, modem, router o altri dispositivi di accesso locale o remoto), la connessione alla rete aziendale di postazioni di lavoro, e l'utilizzo di dispositivi personali anche al fine di memorizzare o di esportare all'esterno immagini, registrazioni audio/video o altre informazioni relativi a luoghi, macchinari, documenti. L'Azienda Ospedaliera si riserva il diritto di eliminare qualsiasi dispositivo la cui installazione non sia stata appositamente prevista o autorizzata.

2.9. L'utente è responsabile della custodia dei dispositivi di memorizzazione aziendali e dei supporti informatici removibili (chiavi USB, Hard Disk esterni, SD Memory card, CD, DVD, etc.), nonché dei dati aziendali in essi contenuti. È fatto obbligo di conservare, custodire e controllare i dispositivi di memorizzazione aziendali e i supporti informatici removibili - in misura particolare se contenenti dati personali, categorie particolari di dati personali (quali, ad esempio dati sanitari) o dati relativi a condanne penali e reati - affinché nessun soggetto terzo ne prenda visione o possesso, valutando anche l'opportunità di cifrarne il contenuto. In particolare, i

supporti di memorizzazione removibili contenenti dati particolari (sensibili) o giudiziari, se non più utilizzati, devono essere distrutti o resi inutilizzabili, ovvero riutilizzabili da altri utenti solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

2.10. È vietato utilizzare i dispositivi di memorizzazione e i supporti informatici removibili per la memorizzazione, anche temporanea, di file estranei all'attività aziendale.

2.11. Non utilizzare dispositivi di memorizzazione e supporti informatici removibili di ignota provenienza (quali, ad esempio, chiavi USB trovate all'interno o all'esterno del luogo di lavoro), in quanto potenziale veicolo di infezione di software malevolo (virus, malware, etc.) nella rete aziendale. Nel caso contattare immediatamente la SC "Tecnologie Informatiche e Servizi Informativi".

2.12. Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax o nelle stampanti ubicate in luoghi accessibili al pubblico all'atto dell'invio. Qualora il dipendente sia prossimo a ricevere atti contenenti dati o informazioni riservate via fax o le mandi in stampa nelle stampante non ubicata nella stanza, avrà cura di monitorare la postazione fax e la stampante e preservare – limitatamente alle oggettive possibilità – la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

2.13. Nel caso in cui si constati o sospetti un incidente di sicurezza o di violazione dei dati personali, è fatto obbligo di darne immediata comunicazione al designato al trattamento dei dati includendo, ove possibile, una breve descrizione dell'evento. Sarà cura del designato informare tempestivamente il responsabile della SC "Tecnologie Informatiche e Servizi Informativi".

2.14. L'Azienda Ospedaliera Brotzu è legittimata a tracciare e registrare tutti gli accessi sui propri sistemi informativi, al fine di prevenire o correggere malfunzionamenti del sistema, garantire l'efficienza dello stesso, di mettere i file a disposizione dell'autorità giudiziaria qualora vengano richiesti, nonché di effettuare periodici controlli. La registrazione degli accessi comprenderà informazioni relative ai riferimenti temporali e alla descrizione degli eventi associati a tali accessi, comprensive delle autenticazioni nei confronti delle basi di dati. Tali informazioni potranno essere conservate per un periodo di tempo pari a sei mesi.

2.15. I servizi che risultano non utilizzati per oltre 6 mesi saranno disattivati, salvo eccezioni debitamente motivate.

3. Criteri generali per la gestione delle credenziali di accesso alla rete aziendale e ai servizi (posta elettronica, applicativi)

3.1. Le credenziali di accesso consistono in un codice per l'identificazione dell'utente (userid) associato ad una parola chiave riservata (password), e consentono l'accesso alla rete aziendale, alla posta elettronica e agli applicativi aziendali.

3.2. Le credenziali di accesso alla rete aziendale, alla posta elettronica e agli applicativi sono attribuite dalla SC "Tecnologie Informatiche e Servizi Informativi". Al riguardo nella intranet aziendale sono disponibili i moduli di richiesta di abilitazione ai servizi.

3.3. Ad ogni utente viene fornito il codice di identificazione (userid) e una parola chiave (password) provvisoria. Al primo accesso al sistema informatico, l'utente dovrà sostituire la password provvisoria assegnata con una di sua scelta.

3.4. Deve essere assicurato l'uso esclusivo e personale delle credenziali rilasciate. Le credenziali non possono in alcun modo essere comunicate a terzi.

3.5. Ogni password deve rispettare i seguenti requisiti di complessità:

- lunghezza minima: otto caratteri alfanumerici;

- non contenere riferimenti agevolmente riconducibili all'autorizzato e all'Azienda (cognome, nome, codice fiscale, data di nascita, struttura di appartenenza, parole quali "ospedale", "Brotzu");
- almeno un carattere minuscolo;
- almeno un carattere maiuscolo;
- almeno un numero;
- almeno un carattere speciale (ad esempio: !,-,#,_,?,%,=).

3.6. Ogni password avrà durata massima pari a 90 giorni e le ultime tre password non dovranno essere riutilizzate.

3.7. Le credenziali di accesso saranno bloccate a fronte di reiterati tentativi falliti di autenticazione.

3.8. Sostituire immediatamente la password nel caso si sospetti che la password abbia perso segretezza.

3.9. Qualora l'utente venisse a conoscenza di credenziali di accesso di un altro utente, questo è tenuto a darne immediata comunicazione al designato al trattamento dei dati e all'interessato.

3.10. Deve essere assicurata la custodia e la segretezza delle credenziali rilasciate e di qualsiasi altra informazione legata al processo di autenticazione. La documentazione relativa alle credenziali di accesso e l'eventuale documentazione inerente deve essere protetta in luogo custodito, non deve essere lasciata sulle scrivanie, in spazi comuni o agevolmente accessibili, alla libera visione di terzi, o utilizzando altre modalità che siano in grado, anche solo potenzialmente, di mettere a rischio l'integrità e la disponibilità degli strumenti informatici o telematici dell'Azienda (quali, ad esempio, l'uso di agende e post-it). Deve infine essere assicurata la custodia delle chiavi di locali, armadi e cassettiere in cui è conservata la documentazione contenente le credenziali di accesso ed eventuale documentazione inerente; in caso di furto o smarrimento, deve essere fatta pronta denuncia designato al trattamento dei dati.

4. Accesso alla rete aziendale (dominio Windows Server)

4.1. L'accesso alla rete aziendale (dominio) è fornito a seguito di richiesta da inoltrare alla SC "Tecnologie Informatiche e Servizi Informativi" utilizzando il modulo disponibile nella intranet aziendale.

4.2. Non è ammesso l'accesso simultaneo con le stesse credenziali su postazioni di lavoro differenti. Pertanto, prima di collegarsi su una seconda postazione di lavoro, occorre sempre eseguire la disconnessione del proprio utente sulla prima.

5. Accesso alla rete Wi-Fi

5.1. L'accesso alla rete Wi-Fi è consentito esclusivamente ai dispositivi ed agli utenti autorizzati.

5.2. L'accesso alla rete Wi-Fi è fornito a seguito di richiesta da inoltrare alla SC "Tecnologie Informatiche e Servizi Informativi" utilizzando il modulo disponibile nella intranet aziendale firmato dal responsabile della struttura di appartenenza, esplicitando le motivazioni della richiesta.

6. Servizio di posta elettronica aziendale

6.1. Il servizio di posta elettronica è concesso esclusivamente agli utenti abilitati, come supporto per il

raggiungimento dei fini lavorativi e istituzionali dell'Azienda Ospedaliera Brotzu.

6.2. La casella di posta assegnata dall'Azienda all'utente è uno strumento di lavoro individuale. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.3. La casella di posta elettronica aziendale è fornita a seguito di richiesta da inoltrare alla SC "Tecnologie Informatiche e Servizi Informativi" utilizzando il modulo disponibile nella intranet aziendale.

6.4. Non è ammesso l'utilizzo della casella di posta elettronica aziendale per attività di natura personale e non legate all'attività lavorativa.

6.5. Il servizio è soggetto ad un controllo preventivo su ogni casella tramite strumenti di filtro di protezione antispam e antivirus.

6.6. La dimensione della casella di posta non è elevabile. Prevenire la saturazione dello spazio disponibile provvedendo al trasferimento periodico dei messaggi su un archivio locale, e mantenere in ordine la casella di posta, cancellando documenti inutili e allegati di grosse dimensioni non necessari.

6.7. Nel caso di invio di allegati di grandi dimensioni, utilizzare formati compressi. Il servizio di posta elettronica impedisce l'invio di allegati di dimensioni superiori ai 10 MB.

6.8. Cancellare i messaggi insoliti, di richiesta di credenziali di accesso, o contenenti allegati sospetti. Eventuali richieste di comunicare le proprie credenziali di accesso ai sistemi (posta elettronica, dominio, applicativi) devono essere ignorate. La SC "Tecnologie Informatiche e Servizi Informativi" non richiederà mai le credenziali di accesso (incluse le password) ai sistemi aziendali.

6.9. Evitare la diffusione incontrollata di sistemi per propagare messaggi che inducono il destinatario a produrne molteplici copie da spedire, a propria volta, a nuovi destinatari, quali, ad esempio, messaggi aventi un numero considerevole di destinatari.

6.10. L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Verificare l'affidabilità del sito prima dell'eventuale iscrizione.

6.11. In caso di necessità urgenti di sicurezza, gli amministratori di sistema possono accedere ai dati contenuti nella casella di posta elettronica dell'utente. L'accesso avverrà tramite credenziali privilegiate.

6.12. Trascorsi 30 giorni dalla data di termine del rapporto di lavoro, la casella di posta elettronica dell'utente viene cancellata.

7. Servizio di posta elettronica certificata (PEC)

7.1. Il servizio di posta elettronica certificata (PEC) è concesso per il raggiungimento dei fini lavorativi e istituzionali dell'Azienda Ospedaliera Brotzu.

7.2. Ogni casella di posta elettronica certificata ha un responsabile individuato nominativamente, che ne risponde legalmente ed ha la responsabilità del corretto utilizzo.

7.3. La casella di posta elettronica certificata è fornita di norma alle Strutture Complesse o Semplici Dipartimentali che ne fanno richiesta alla SC "Tecnologie Informatiche e Servizi Informativi" utilizzando il modulo disponibile nella intranet aziendale firmato dal responsabile della struttura di appartenenza, esplicitando le motivazioni della richiesta.

7.4. Non è ammesso l'utilizzo della casella di posta elettronica certificata per attività di natura personale e non

legate all'attività lavorativa.

7.5. La dimensione della casella PEC non è elevabile. Prevenire la saturazione dello spazio disponibile provvedendo al trasferimento periodico dei messaggi su un archivio locale.

7.6. Per quanto non espressamente indicato per il servizio di PEC si applicano le regole di utilizzo previste per il servizio di posta elettronica aziendale.

8. Applicativi aziendali

8.1. Le credenziali di accesso agli applicativi aziendali sono associate ad una persona fisica.

8.2. L'accesso agli applicativi è consentito esclusivamente ai dispositivi ed agli utenti autorizzati.

8.3. L'accesso agli applicativi aziendali è fornito a seguito di richiesta da inoltrare alla SC "Tecnologie Informatiche e Servizi Informativi" utilizzando il modulo disponibile nella intranet aziendale firmato dal responsabile della struttura di appartenenza.

9. Postazioni di lavoro

9.1. La postazione di lavoro affidata al dipendente è uno strumento di lavoro. Ogni utente è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.

9.2. Non è consentito modificare le caratteristiche hardware della postazione di lavoro senza autorizzazione della SC "Tecnologie Informatiche e Servizi Informativi".

9.3. Non è consentito modificare le configurazioni impostate nella postazione di lavoro senza autorizzazione della SC "Tecnologie Informatiche e Servizi Informativi".

9.4. Non è permessa l'installazione autonoma di software senza autorizzazione e l'utilizzo di programmi diversi da quelli distribuiti ed installati ufficialmente dalla SC "Tecnologie Informatiche e Servizi Informativi". L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili e/o penali in caso di violazione della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software con regolare licenza.

9.5. Non è consentita la riproduzione o la duplicazione di programmi informatici.

9.6. Salvo diverse disposizioni, la postazione di lavoro deve essere spenta ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

9.7. L'utente è tenuto a scollegarsi dal sistema o bloccare la sessione ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima, anche temporaneamente. Lasciare una postazione di lavoro incustodita connessa alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

9.8. Le informazioni archiviate sulle postazioni di lavoro devono essere esclusivamente quelle previste o

necessarie all'attività lavorativa.

9.9. Gli operatori della SC "Tecnologie Informatiche e Servizi Informativi" possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sulle postazioni di lavoro.

9.10. Al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio in caso di prolungata assenza od impedimento dell'incaricato) gli amministratori di sistema possono accedere ai dati contenuti nella postazione di lavoro dell'utente, il quale verrà tempestivamente informato dell'intervento di accesso realizzato.

10. Dispositivi mobili (PC portatili, tablet, smartphone)

10.1. L'utente è responsabile del dispositivo mobile assegnatogli dall'Azienda, e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

10.2. Il dispositivo mobile, soprattutto se utilizzato all'esterno (convegni, visite) non deve essere mai lasciato incustodito. In caso di allontanamento deve essere custodito in un luogo protetto.

10.3. Il dispositivo mobile deve contenere solo i documenti strettamente necessari, con particolare attenzione alla rimozione di eventuali file elaborati sul dispositivo che non fossero più necessari. L'incaricato è tenuto comunque alla rimozione di eventuali file elaborati sui dispositivi mobili prima della riconsegna del bene.

10.4. Nel caso il dispositivo si provvisto di antivirus è necessario collegarsi periodicamente alla rete aziendale per consentire il caricamento degli aggiornamento.

10.5. Al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio in caso di prolungata assenza od impedimento dell'incaricato) gli amministratori di sistema possono accedere ai dati contenuti nel dispositivo mobile dell'utente, il quale verrà tempestivamente informato dell'intervento di accesso realizzato.

10.6. L'accesso al dispositivo dovrà essere protetto da PIN o password d'accesso.

10.7. Per quanto non espressamente indicato, ai dispositivi mobili si applicano le regole di utilizzo previste per le postazioni di lavoro.

11. Servizio di accesso alle cartelle di rete condivise

11.1. Il servizio di accesso alle cartelle condivise ha l'obiettivo primario di favorire la comunicazione interna.

11.2. Il servizio costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

11.3. È vietato l'utilizzo del servizio per motivi diversi da quelli strettamente legati all'attività lavorativa. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, nelle cartelle condivise.

11.4. Costituisce buona regola la periodica pulizia degli archivi (almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente

da evitare un'archiviazione ridondante.

11.5. Sulle cartelle condivise vengono svolte regolari attività di controllo, amministrazione e backup.

11.6. Al solo fine di garantire l'operatività, la sicurezza del servizio ed il normale svolgimento dell'attività aziendale, gli amministratori di sistema possono accedere ai dati contenuti nelle cartelle condivise e procedere alla rimozione di file o applicazioni ritenute pericolose per la sicurezza della rete aziendale.

12. Servizio Internet

12.1. Il servizio Internet ha l'obiettivo primario di favorire la comunicazione verso l'esterno, oltre che favorire il reperimento e la divulgazione di informazioni utili per lo svolgimento della propria professione.

12.2. Il dispositivo abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

12.3. È vietato il download di software, file musicali e altri tipi di file audio/video non legati all'attività lavorativa.

12.4. È vietato l'accesso ai siti contenenti contenuti audio/video in streaming (stazioni radio, televisione on line, youtube, pandora, spotify, deezer, apple music, google play music, etc.) non legati all'attività lavorativa.

12.5. È vietato l'utilizzo di reti di file sharing per motivi diversi da quelli strettamente legati all'attività lavorativa.

12.6. Si rende noto che l' Azienda ha attivato sistemi di monitoraggio della navigazione aziendale secondo la vigente normativa.

13. Accesso remoto alla risorse aziendali dall'esterno

13.1. L'accesso remoto alle risorse aziendali dall'esterno ha carattere straordinario ed è espressamente autorizzato dalla SC "Tecnologie Informatiche e Servizi Informativi" a seguito di adeguate motivazioni da fornire utilizzando il modulo disponibile nella intranet aziendale firmato dal responsabile della struttura di appartenenza.

13.2. L'accesso alle risorse aziendali dall'esterno è attuato tramite VPN (Virtual Private Network), le cui credenziali di accesso vengono assegnate all'utilizzatore che se ne assume la responsabilità in merito alla protezione e alla sicurezza dei dati trattati.

14. Osservanza delle disposizioni in materia di privacy e dei regolamenti aziendali

14.1. È obbligatorio attenersi alle disposizioni in materia di privacy e di misure di sicurezza, come indicate nelle lettere di incarico per i designati e gli autorizzati al trattamento, ai sensi della vigente normativa.

14.2. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è sanzionabile con

provvedimenti disciplinari.

15. Aggiornamento e revisione

15.1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente regolamento. Le proposte verranno esaminate dalla Direzione e dalla SC "Tecnologie Informatiche e Servizi Informativi".

15.2. Il presente Regolamento è soggetto a revisione con frequenza annuale.