REGIONE AUTONOMA FRIULI VENEZIA GIULIA
azienda per l'assistenza sanitaria
5 Friuli Occidentale

Regolamento sull'utilizzo e la gestione delle risorse informatiche aziendali.

Sommario

Indicazioni generali ... 1
Finalità della Policy ... 1
Campo di applicazione ... 1
Destinatari ... 1
Entrata in vigore del regolamento e diffusione ... 1
Verifiche ... 2
Sanzioni ... 2
Politiche ed utilizzo delle risorse informatiche aziendali ... 3
Indicazioni generali ... 3
Configurazioni dei dispositivi aziendali e collegamento alla rete aziendale ... 4
Installazione di hardware e software ... 4
Supporti di memorizzazione ... 4
Stampa su stampanti di rete ... 5
Scansione su multifunzione ... 5
Credenziali per l'accesso ai dispositivi e alla rete aziendale ... 5
Credenziali per l'accesso ai servizi e applicativi aziendali ... 7
Unità di rete e cartelle condivise ... 8
Diritti di accesso e controllo remoto ... 8
Utilizzo della rete Internet e dei relativi servizi ... 9
Regole di utilizzo di internet nelle sedi aziendali ... 9
Posta elettronica ... 10
Casella di posta elettronica aziendale ... 10
Credenziali per l'accesso alla casella di posta elettronica ... 10
Utilizzi consentiti della posta elettronica ... 12
Contenuto dei messaggi ... 12
Altre istruzioni riguardanti la posta elettronica ... 13
Terminologie e abbreviazioni ... 14

La crescente diffusione di tecnologie informatiche ed il loro utilizzo in ambito lavorativo espone l'*Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* e gli utenti fruitori a una serie di rischi e di conseguenti responsabilità.

Sebbene principi di diligenza e correttezza siano alla base dell'utilizzo di risorse informatiche, *l'Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* ha realizzato questo documento con l'obiettivo di diffondere nozioni fondamentali sulla sicurezza informatica ed evitare che comportamenti non idonei arrechino gravi danni al sistema informativo.

Il regolamento risponde quindi all'esigenza di disciplinare l'utilizzo degli strumenti informatici e contiene indicazioni su quali siano le migliori pratiche da adottare.

Indicazioni generali

Finalità della Policy

Le finalità di questo documento sono:
1. garantire e salvaguardare la sicurezza e la privacy degli utenti abilitati *dall'Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* (in seguito *Azienda*);
2. stabilire una policy per la sicurezza e il rispetto della privacy nell'utilizzo delle risorse informatiche aziendali con riferimento in particolare alle misure di sicurezza imposte dalle normative per il trattamento di dati personali;
3. fornire idonee indicazioni ed istruzioni agli utenti interessati dalle predette misure di sicurezza;
4. regolamentare l'utilizzo delle risorse informatiche aziendali in modo che siano utilizzate in maniera efficace, produttiva e orientata al raggiungimento degli obiettivi aziendali;
5. garantire la sicurezza e prevenire il danneggiamento delle risorse informatiche aziendali.

Campo di applicazione

Questa policy si applica:
1. a tutte le risorse informatiche di proprietà dell'*Azienda* e/o messe a disposizione nell'ambito del *Sistema Informativo Socio-Sanitario Regionale* (in seguito *SISSR*);
2. a tutte le operazioni di accesso a informazioni registrate ed archiviate elettronicamente tramite risorse informatiche aziendali;
3. a tutte le forme di comunicazione operate attraverso la rete aziendale e la posta elettronica.

Destinatari

Il regolamento si applica a tutti i dipendenti a tempo pieno o parziale (senza alcuna distinzione di ruolo e/o livello), collaboratori, consulenti, convenzionati, dipendenti di aziende esterne legate da contratti di fornitura e/o di servizi o altri individui in possesso di specifiche credenziali di autenticazione alla quale è consentito l'utilizzo dell'accesso alle risorse aziendali (a prescindere dal tipo di rapporto contrattuale intrattenuto con l'*Azienda*).

Entrata in vigore del regolamento e diffusione

Il regolamento entra in vigore con decreto del Direttore Generale dell'*Azienda* su proposta del Direttore della *S.C. Ingegneria Biomedicale e Sistema Informatico.*
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presente.

Ai sensi dell'art. 7 Legge n. 300 del 1970 l'*Azienda*, ai fini dell'esercizio del regolamento, darà adeguata pubblicità mediante invio ai responsabili della trattamento e provvederà alla pubblicazione dello stesso sul sito internet aziendale così come indicato dal D.Lgs. n. 33 del 14 marzo 2013.

Verifiche

Le segnalazioni di eventuali violazioni devono essere repentinamente comunicate alla *S.C. Ingegneria Biomedicale e Sistema Informatico* che laddove necessario provvederà ad attivare le idonee procedure di verifica con gli *Amministratori di sistema* aziendale.
Non sono ammesse segnalazioni di violazioni in forma anonima.
Viene comunque tutelato dell'*Azienda* il diritto alla privacy degli utenti che comunicassero dette violazioni nei limiti previsti dalla normativa italiana.

Sanzioni

Poiché in caso di violazioni contrattuali e giuridiche, sia l'*Azienda* sia il singolo utente sono potenzialmente perseguibili con sanzioni anche di natura penale, l'*Azienda* verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del sistema informativo.
In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali.
Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle autorità competenti.

Politiche ed utilizzo delle risorse informatiche aziendali

Indicazioni generali

1. L'utilizzo delle risorse informatiche aziendali e di quelle messe a disposizione dal *SISSR* è riservato ai dipendenti dell'*Azienda* e ad altri soggetti espressamente autorizzati dal responsabile del trattamento.
   Il responsabile del trattamento richiede alla *S.C. Ingegneria Biomedicale e Sistema Informatico* l'abilitazione ai servizi informatici e l'accesso alle banche dati necessari a ciascun utente.
   Il responsabile del trattamento comunica immediatamente qualsiasi modifica relativa all'organico del servizio che richieda l'attivazione o la sospensione di servizi informatici o autorizzazioni all'accesso alle banche dati (es. cambio di mansioni e/o trasferimento altro reparto);
2. le risorse informatiche aziendali sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente lavorativi. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, ecc.), sia per quelle affidate al singolo dipendente (desktop, notebook, periferiche, stampanti, ecc.).
   Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.
   L'utilizzo di risorse informatiche aziendali non deve compromettere la sicurezza e la riservatezza del sistema informativo oltre a non pregiudicare ed ostacolare le attività dell'Amministrazione o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici;
3. le risorse informatiche aziendali affidate al singolo utente (es. dispositivi e relativi programmi e/o applicazioni) sono strumenti di lavoro appartenenti al patrimonio aziendale e pertanto vanno custoditi in modo appropriato.
   Il furto, il danneggiamento o lo smarrimento di tali strumenti devono essere prontamente segnalati all'*Azienda*. (e qualora necessario denunciato alle competenti autorità)
   Il dispositivo è assegnato ad una struttura aziendale. In caso di trasferimento dell'utente le risorse informatiche restano alla struttura di appartenenza salvo esplicita autorizzazione da parte della *S.C. Ingegneria Biomedicale e Sistema Informatico* su richiesta del responsabile;
4. le postazioni di lavoro devono essere spente ogni sera prima di lasciare gli uffici. Casi particolari, in cui ci sia la necessità di lasciare sempre attiva la postazione, devono essere esplicitamente autorizzati dalla S.C. Ingegneria Biomedicale e Sistema Informatico. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
   Qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad eseguire una delle seguenti operazioni: spegnimento, blocco (digitando per es. i tasti CRTL+ALT+CANC) o disconnessione della postazione di lavoro.
   In caso di inattività prolungata la connessione dell'utente potrà essere sospesa e disconnessa in automatico;
4. i dati sensibili non possono essere salvati nei supporti di memorizzazione locali dei computer a meno di adeguati sistemi di protezione.

Nel caso di computer portatili aziendali inoltre:

1) L'utente deve custodire con diligenza il dispositivo sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro;
2) se il dispositivo è utilizzato all'esterno (convegni, conferenze ecc.), in caso di allontanamento, deve essere custodito in un luogo protetto;
3) il dispositivo non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.

Configurazioni dei dispositivi aziendali e collegamento alla rete aziendale

1. Non è consentita la modifica delle configurazioni impostate di default sul dispositivo;
2. ogni computer aziendale deve obbligatoriamente essere collegato alla rete aziendale e non può per nessun motivo essere scollegato da tale rete. Casi particolari in cui il computer non debba essere connesso alla rete aziendale devono essere esplicitamente autorizzati dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*.
   I computer portatili devono essere collegati alla rete aziendale con frequenza almeno mensile al fine di garantisce l'aggiornamento di: sistema operativo, antivirus e degli applicativi installati;
3. per ragioni di sicurezza non è concesso connettere alla rete aziendale stazioni di lavoro private e sistemi di connessione (es. modem, switch, hub ecc.) se non su esplicita e formale autorizzazione della *S.C. Ingegneria Biomedicale e Sistema Informatico*.

Installazione di hardware e software

1. Non è consentita l'installazione di programmi provenienti dall'esterno dell'*Azienda*, salvo previa autorizzazione esplicita della *S.C. Ingegneria Biomedicale e Sistema Informatico*. L'installazione autonoma di software non autorizzato comporta un grave pericolo di introduzione di virus informatici e/o di alterazione della stabilità delle applicazioni presenti nell'elaboratore;
2. non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'*Azienda* su indicazione della *S.C. Ingegneria Biomedicale e Sistema Informatico* o resi disponibili in ambito *SISSR* (dlgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore);
3. non è consentita l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro (es. masterizzatori, modem, ecc.), se non con l'autorizzazione esplicita della *S.C. Ingegneria Biomedicale e Sistema Informatico*;
4. non sono consentiti l'installazione autonoma e/o l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare, criptare o sopprimere il contenuto di comunicazioni e/o di documenti informatici con finalità omissive e fraudolente.

Supporti di memorizzazione

1. Non è consentito l'utilizzo di cd, dvd, nastri magnetici, chiavette USB, hard disk esterni, ecc. di provenienza ignota o dubbia;
2. ogni dispositivo di memorizzazione di provenienza esterna all'*Azienda* dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato alla *S.C. Ingegneria Biomedicale e Sistema Informatico* o a persone da lui delegate;
3. non è consentito scaricare file provenienti da Internet oppure contenuti in supporti di memorizzazione che non abbiano una chiara attinenza con la propria prestazione lavorativa;
4. i supporti di memorizzazione quali: dvd, nastri magnetici, chiavette USB, hard disk esterni, ecc. contenenti dati sensibili devono essere ridotti a casi di assoluta necessità e custoditi in archivi chiusi a chiave;
5. i supporti di memorizzazione contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato anche dopo la cancellazione mediante l'utilizzo di specifici strumenti di recupero dati;
6. non è consentita la memorizzazione e la diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Stampa su stampanti di rete

Si raccomanda agli utenti di prestare la massima attenzione nella stampa soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone. Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.

La stampa di documenti informatici dovrà essere limitata all'attività lavorativa e in ogni caso per documenti per cui esiste l'assoluta necessità di disporre della copia cartacea. In particolare per motivi di economicità per quanto riferito alle stampe a colori.

Scansione su multifunzione

Scansione da multifunzione con invio a casella di posta elettronica:

1. Le scansioni devono essere inoltrate alla propria mail aziendale per verificarne la corretta scansione. Solo dalla propria casella mail sarà possibile procedere all'inoltro a una persona terza.
2. È proibito l'invio di scansioni da multifunzione verso mail non aziendali

Scansione da multifunzione con salvataggio su cartella di rete:

1. Qualora il file derivante da scansione venga salvato su una cartella condivisa, l'utente si fa carico di spostare il file in una cartella non consultabile da utenti non autorizzati alla visione del documento.
2. La cartella condivisa nella quale vengono salvate le scansioni viene automaticamente cancellata periodicamente.
   La cancellazione periodica non dispensa tuttavia l'utente dall'obbligo di cancellare/spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile (al fine di non rendere accidentalmente noto a terzi il contenuto dei file scansione).

Si raccomanda di porre la massima attenzione nella scansione di documenti contenenti dati personali e sensibili.

Credenziali per l'accesso ai dispositivi e alla rete aziendale

Per accedere a dispositivi e alla rete dell'*Azienda*, l'utente dovrà attenersi al presente regolamento.

1. L'accesso ai dispositivi e alla rete aziendale avviene mediante un codice di identificazione personale e una parola chiave segreta (password). La coppia di informazioni prende il nome di credenziali di accesso;
2. dovranno essere adottate le necessarie cautele per garantire la segretezza delle credenziali e la diligente custodia dei dispositivi eventualmente in possesso ad uso esclusivo a scopo d'autenticazione (quali ad esempio: smart card, braccialetti, dispositivi RFID);
3. la password di accesso alla rete ha in genere un periodo di validità limitato. A intervalli regolari verrà quindi richiesto all'utente di modificare la password;
4. le credenziali di accesso ai dispositivi e alla rete aziendale vengono attribuite dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, all'assunzione del dipendente/inizio del rapporto di collaborazione (ove autorizzato) e devono essere obbligatoriamente modificate la primo accesso;
5. le credenziali vengono immediatamente revocate/annullate dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, alla cessazione del rapporto di dipendenza/collaborazione con l'*Azienda* non appena ne venga a conoscenza (tramite comunicazione da parte del responsabile al trattamento e/o uff. personale);
6. le credenziali di accesso ai dispositivi e alla rete attribuite dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, sono in genere modificabili in totale autonoma dall'utente;
7. l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dal amministratore di sistema;

8. l'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla rete, consapevole che la cessione delle stesse consente ad altri l'accesso e l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione / modifica di dati;
9. la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che dell'*Azienda*, di fatti e atti illeciti, con particolare riferimento all'immissione in rete di contenuti critici o contrari all'ordine pubblico o al buon costume così come definiti dalla giurisprudenza corrente;
10. non sono previsti accessi anonimi o di gruppo: laddove questi siano attualmente attivi saranno progressivamente dismessi;
11. è assolutamente proibito l'accesso alla rete locale e/o alle applicazione condivise con nomi utente diversi da quello assegnato;
12. l'utente si impegna a modificare tempestivamente la password d'accesso alla rete qualora tale dato sia stato rubato, smarrimento, perso o sia noto a terzi;
13. in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto alla *S.C. Ingegneria Biomedicale e Sistema Informatico*;
14. nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al *Amministratore di sistema* aziendale;
15. l'*Azienda* si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di *Autorità Giudiziaria*, *Autorità di Pubblica Sicurezza* e *Garante per la Protezione dei Dati Personali.*

Credenziali per l'accesso ai servizi e applicativi aziendali

1. Dovranno essere adottate le necessarie cautele per garantire la segretezza delle credenziali e la diligente custodia dei dispositivi eventualmente in possesso ad uso esclusivo a scopo d'autenticazione (quali ad esempio: smart card, braccialetti, dispositivi RFID);
2. la password di accesso agli applicativi ha in genere un periodo di validità limitato. A intervalli regolari verrà quindi richiesto all'utente di modificare la password;
3. le credenziali di accesso ai servizi e applicativi aziendali vengono attribuite/revocate/modificate dall'ufficio abilitazioni della *S.C. Ingegneria Biomedicale e Sistema Informatico* su apposita richiesta dei responsabili al trattamento di norma il Direttore della Struttura Complessa / Dipartimento / Distretto. La richiesta deve pervenire al servizio Abilitazioni della *S.C. Ingegneria Biomedicale e Sistema Informatico* secondo l'apposita procedura "richieste rilascio abilitazioni";
4. la compilazione della richiesta in modalità non conforme a quanto indicato nella procedura "richieste rilascio abilitazioni" ' potrà comportare una sospensione della pratica;
5. l'utente garantisce la veridicità dei dati personali forniti al momento dell'attivazione del servizio;
6. le credenziali vengono immediatamente revocate/annullate dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, alla cessazione del rapporto di dipendenza/collaborazione con l'*Azienda* non appena ne venga a conoscenza (tramite comunicazione da parte del responsabile al trattamento e/o uff. personale);
7. le credenziali di accesso a servizi e applicazioni attribuite dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, sono in genere modificabili in totale autonoma dall'utente;
8. l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dal amministratore di sistema;
9. l'utente si impegna a non cedere a terzi le proprie credenziali di accesso a servizi e applicazioni consapevole che la cessione delle stesse consente ad altri l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione / modifica dei dati;
10. la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione a servizi e applicazioni sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che dell' *Azienda*, di fatti e atti illeciti,
11. non sono previsti accessi anonimi o di gruppo;
12. qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad uscire dall'applicazione o dal servizio (quantomeno la postazione deve essere bloccata);
13. è assolutamente proibito l'accesso ad applicazioni e servizi con nomi utente diversi da quello assegnato;
14. l'utente si impegna a modificare tempestivamente la password d'accesso a servizi e applicazioni qualora tale dato sia stato rubato, smarrimento, perso o sia noto a terzi;
15. in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto alla *S.C. Ingegneria Biomedicale e Sistema Informatico*;
16. nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al *Amministratore di sistema* aziendale;
17. l'*Azienda* si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di *Autorità Giudiziaria*, *Autorità di Pubblica Sicurezza* e *Garante per la Protezione dei Dati Personali.*

Unità di rete e cartelle condivise

1. Per gli utenti del dominio aziendale è previsto, previa richiesta alla *S.C. Ingegneria Biomedicale e Sistema Informatico,* un sistema di salvataggio dei file su unità di rete.
   Le unità di rete si dividono in due categorie:
   a. Unità di rete per il salvataggio dei documenti aziendali
      I documenti salvati in queste unità (sever aziendali) sono tutelati da perdite mediante accurate procedure di salvataggio.
      Il salvataggio su unità di rete è obbligatorio per i dati che richiedono riservatezza (es. dati sensibili , amministrativi, giuridici, economici, ecc.).
      La memorizzazione avviene a seconda del grado di riservatezza dei documento su cartelle con adeguato livello di condivisione.
      I livelli di condivisione/privilegi di lettura e scrittura delle cartelle vengono definiti dal/dai responsabile/i della/e struttura/e proprietaria/e delle cartelle stesse e pertanto dei documenti ivi contenuti;

   b. Unità di rete per lo scambio dati
      Queste unità permettono lo scambio di file tra utenti di dominio ma non sono soggetti a procedure di copia di riserva.
      Poiché queste unità di rete sono di fatto punto di scambio dove i documenti transitano ma non possono rimanere per lungo periodo la *S.C. Ingegneria Biomedicale e Sistema Informatico* provvederà periodicamente alla cancellazione di tutti i file presenti in tali aree condivise;

2. entrambe le unità di rete sono aree di condivisione e salvataggio di informazioni inerenti l'attività istituzionale e non possono in alcun modo essere utilizzate per scopi diversi.
   Pertanto qualunque file non legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
3. la *S.C. Ingegneria Biomedicale e Sistema Informatico* si riserva la facoltà di procedere alla rimozione di qualsiasi file o applicazione memorizzata nelle unità di rete qualora ritenuto pericoloso per la sicurezza del sistema;
4. costituisce buona regola la periodica (almeno mensile) cancellazione dagli archivi/cartelle di file obsoleti e/o documenti non più necessari all'attività d'ufficio;
5. L'utente si impegna a non cedere a terzi le proprie credenziali di accesso alle proprie cartelle condivise consapevole che la cessione delle stesse consente ad altri l'utilizzo/accesso a contenuti riservati e la possibilità di cancellazione e modifica degli stessi.

Diritti di accesso e controllo remoto

1. Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, la *S.C. Ingegneria Biomedicale e Sistema Informatico* può avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale;
2. l'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire solo previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso;
3. in caso di malfunzionamenti straordinari e in situazioni di emergenza, la *S.C. Ingegneria Biomedicale e Sistema Informatico* ha facoltà in qualunque momento di accedere a qualunque sistema informativo aziendale per l'espletamento delle proprie funzioni.

La *S.C. Ingegneria Biomedicale e Sistema Informatico* può in qualunque momento procedere alla rimozione di qualsiasi file o applicazione che riterrà essere pericolosa per la sicurezza, sia sulle postazioni degli utenti che sulle unità di rete.

Utilizzo della rete Internet e dei relativi servizi

Regole di utilizzo di internet nelle sedi aziendali

1. L'abilitazione alla navigazione su internet deve essere accordata dal responsabile del trattamento che invia richiesta formale al servizio Abilitazioni della *S.C. Ingegneria Biomedicale e Sistema Informatico;*
2. qualora l'utente non fosse stato abilitato alla navigazione in internet è fatto divieto assoluto di connettersi autonomamente alla rete internet;
3. è tassativamente proibito l'utilizzo di sistemi di connessione quali modem dial-up, chiavette internet e condivisione di connessione con dispositivi mobili (hotspot e tethering), collegamento a reti wi-fi diversa da quella aziendale, ecc.;
4. è vietato modificare le impostazioni di connessione stabilite dalla *S.C. Ingegneria Biomedicale e Sistema Informatico* per le postazioni aziendali (firewall, IP, proxy ecc.);
5. il sistema di navigazione per mezzo di proxy aziendale effettua il monitoraggio dei siti visitati dai dipendenti. Tali dati vengono conservati al fine di rispondere ad eventuale legittima richiesta da parte di *Autorità Giudiziaria*, *Autorità di Pubblica Sicurezza* e *Garante per la Protezione dei Dati Personali*;
6. qualsiasi divulgazione di informazioni nella rete internet relative a strutture e/o attività aziendali dovrà rispettare specifici regolamenti aziendali in materia;
7. gli utenti sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web. L'utente è tenuto nel corso della navigazione a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online;
8. per ragioni di sicurezza non è concesso scaricare software dalla rete. Eventuali necessità dovranno essere appositamente concordate con la *S.C. Ingegneria Biomedicale e Sistema Informatico* che provvederà ad eseguire fisicamente lo scarico da una stazione protetta e ad applicare le misure antivirus relative. Il software scaricato sarà poi installato dal personale autorizzato al richiedente;
9. è vietato lo scarico di file audio e video, l'utilizzo di streaming (e in generale tutti gli utilizzi in grado di degradare le prestazioni offerte dal servizio di rete) a meno di utilizzi strettamente attinente l'attività istituzionale;
10. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
11. la *S.C. Ingegneria Biomedicale e Sistema Informatico*, su autorizzazione del Direzione Generale, ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazioni siti non attinenti agli scopi aziendali;
12. è vietato l'utilizzo di internet a scopi personali non attinenti l'attività istituzionale quali a titolo d'esempio: la partecipazione a forum, l'utilizzo di chat-line, bacheche elettroniche e servizi di rete sociale, la registrazione in guest-book anche utilizzando pseudonimi (nickname), l'adesione a servizi gratuiti di social networking e microblogging, remote banking, acquisti online e simili.

Posta elettronica

Casella di posta elettronica aziendale

1. All'atto dell'assunzione/inizio di collaborazione viene assegnato una casella di posta elettronica aziendale nominativa al dipendente/collaboratore (ove autorizzato);
2. all'atto della cessazione del rapporto di dipendenza/collaborazione con l'*Azienda* la casella mail viene bloccata e/o cancellata;
3. l'amministratore di sistema per comprovati motivi può revocare/cancellare la casella di posta elettronica aziendale nominativa di un dipendente / collaboratore;
4. l'*Azienda* favorisce l'utilizzo di indirizzi istituzionali condivisi accessibili a più utenti (es. urp@aas5.sanita.fvg.it, dg@aas5.sanita.fvg.it) per la consultazione di corrispondenza d'interesse comune a più utenti operanti in aree omogenee.
   Le persone che condividono una casella di posta istituzionale devono essere nominate dal responsabile del trattamento della struttura afferente;
5. per l'invio/ricezione di posta elettronica certificata per fini istituzionali avviene attraverso il protocollo aziendale che gestisce la casella PEC: aas5.protgen@certsanita.fvg.it
   Di norma non vengono concesse caselle di posta certificata personalizzate a meno di disposizioni normative diverse.

Credenziali per l'accesso alla casella di posta elettronica

1. L'accesso alla casella di posta elettronica aziendale avviene mediante un codice di identificazione personale e una parola chiave segreta. La coppia di informazioni prende il nome di credenziali di accesso;
2. le credenziali di accesso alla casella di posta elettronica vengono attribuite dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, all'assunzione del dipendente/inizio del rapporto di collaborazione (ove autorizzato) e devono essere obbligatoriamente modificate la primo accesso;
3. le credenziali vengono immediatamente revocate/annullate dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, alla cessazione del rapporto di dipendenza/collaborazione con l'*Azienda* non appena ne venga a conoscenza (tramite comunicazione da parte del responsabile al trattamento e/o uff. personale);
4. le credenziali di accesso attribuite dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*, sono in genere modificabili in totale autonoma dall'utente;
5. l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dall'amministratore di sistema;
6. l'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla casella di posta elettronica consapevole che la cessione delle stesse consente ad altri l'accesso ai servizi di posta con possibilità di inviare e ricevere mail a nome dell'utente abilitato;
7. la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione alla casella di posta elettronica sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che dell' *Azienda*, di fatti e atti illeciti. Quanto sopra vale per le caselle di posta elettronica istituzionali condivise alle quali si accede per tramite del proprio account;
8. qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad uscire dalla casella di posta elettronica;
9. è assolutamente proibito l'accesso a caselle di posta aziendali diverse da quella/e assegnate;
10. l'utente si impegna a modificare tempestivamente la password d'accesso alla casella di posta qualora tale dato sia stato rubato, smarrito o sia noto a terzi;
11. in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto alla *S.C. Ingegneria Biomedicale e Sistema Informatico*;

12. nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla *S.C. Ingegneria Biomedicale e Sistema Informatico*;
13. i dati e la corrispondenza intercorsa sono mantenuti riservati e possono essere resi disponibili a fronte di legittima richiesta da parte di *Autorità Giudiziaria*, *Autorità di Pubblica Sicurezza* e *Garante per la Protezione dei Dati Personali.*

Utilizzi consentiti della posta elettronica

La casella di posta è uno strumento di lavoro assegnato all'atto dell'assunzione dalla *S.C. Ingegneria Biomedicale e Sistema Informatico*.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

1. È fatto divieto di inviare/ricevere posta elettronica su caselle diverse da quelle assegnate dall'*Azienda* all'utente;
2. non è consentito l'utilizzo della posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate. In particolare è fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali;
3. è fatto divieto di utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;
4. la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati";
5. l'utente è tenuto a seguire attentamente le disposizioni date dalla *S.C. Ingegneria Biomedicale e Sistema Informatico* riguardanti la protezione da virus e da altri software che possano diffondersi via mail;
6. è vietato l'utilizzo di tecniche di "mail spamming" cioè l'invio massivo di comunicazioni a liste di comunicazioni extra aziendali e/o di azioni equivalenti;
7. nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
    1. sospendere ogni elaborazione in corso senza spegnere il computer;
    2. segnalare l'accaduto alla *S.C. Ingegneria Biomedicale e Sistema Informatico*.
8. l'*Azienda* mette a disposizione degli utenti sistemi di avviso automatico che in caso di assenza prolungata permettono d'informare i mittenti dell'assenza e forniscono coordinate e riferimenti all'interno dell'*Azienda* tali da garantire il corretto funzionamento dei servizi.
   L'attivazione è a cura dell'utente utilizzatore della casella di posta elettronica.

Contenuto dei messaggi

1. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
2. gli utenti devono prestare attenzione nell'invio di messaggi elettronici affinché non siano inserite inconsapevolmente delle informazioni su credenziali utilizzate in altre applicazioni;
3. gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi;
4. è esplicitamente vietato l'invio di messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte;
5. Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "*Rispondi*" e "*Rispondi a tutti*" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

Altre istruzioni riguardanti la posta elettronica

1. Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute.
2. Gli utenti sono invitati ad inviare allegati in formati comuni (MSOffice, Libre Office, OpenOffice ecc.) possibilmente senza funzioni macro. L'incapacità per il destinatario di aprire file con estensioni poco comuni potrebbe comportare la cancellazione del messaggio (scambiato per un allegato dannoso).
3. Gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo devono prestare molta attenzione nella selezione dei destinatari.
4. Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta. Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo può compromettere sensibilmente la stabilità del programma di posta.
5. Gli utenti devono sempre indicare con chiarezza nel campo oggetto, l'argomento del proprio messaggio.
6. E' possibile richiedere una ricevuta di lettura / ricevimento della propria mail. A tale ricevuta va tuttavia assegnata un'importanza relativa.
7. La conferma della ricezione avviene per opera del mail server centrale e non del destinatario ultimo del messaggio. Non sempre il destinatario conferma la lettura di un messaggio o utilizza sistemi di posta elettronica compatibili, pertanto non vi è certezza sullo stato di ricezione del messaggio.
8. Gli utenti sono invitati a porre attenzione a mail provenienti da mittenti sospetti, mail il cui messaggio riporti errori di ortografia o lessicali e/o contenenti allegati inconsueti non accompagnati da alcun messaggio di testo.
9. Si raccomanda di prevedere, con la funzione di inserimento automatico della firma in calce all'e-mail, la seguente avvertenza sulla privacy e sulla confidenzialità dei messaggi inviati: *"Questo messaggio è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo e-mail."*

Terminologie e abbreviazioni

Nel presente testo verranno utilizzati i seguenti termini:
Sistema Informativo:

amministratore di sistema: persona che a qualunque titolo (dipendenti dell'*AAS5*, dipendenti dell'*INSIEL s.p.a.*, dipendenti di *Ditte appaltatrici*..) ricopre uno dei ruoli sotto indicati relativamente a sistemi informatici dell'*Azienda* per l'Assistenza Sanitaria 5 "Friuli Occidentale":

- System Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, salvataggi, protezioni, ecc...) su sistemi operativi e software di base e d'ambiente;
- Network Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, ecc...) sulle componenti di una rete telematica (cablaggi, apparati di rete di varia natura);
- Database Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, ecc...) sui sistemi di gestione di basi di dati;
- Software Administrator: il ruolo contempla lo svolgimento di attività di amministrazione (configurazione, manutenzione, attribuzione di privilegi, ecc...) specifiche nel contesto di un'applicazione adibita al trattamento dei dati personali e/o sensibili.

La designazione degli amministratori di sistema è individuale e deve indicare l'ambito di operatività.
La designazione è effettuata dal Direttore della *S.C. Ingegneria Biomedicale e Sistema Informatico*;

comunicazione elettronica: qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica;
e-mail: posta elettronica per lo scambio di messaggi e di documenti;
incaricato al trattamento: ciascun utente delle risorse informatiche che effettui trattamenti di dati personali;
INSIEL: la società concessionaria che si occupa della realizzazione degli sviluppi e della conduzione del *SISSR*.
policy o regolamento: documento che ha come oggetto la regolamentazione di una determinata funzione aziendale. Può inoltre contenere delle linee guida e dei suggerimenti per una migliore fruizione dei servizi aziendali;
postazione di lavoro: calcolatore/computer collegato alla rete aziendale tramite il quale l'utente può accede ai servizi di rete;
remote banking: servizi automatizzati che consentono al cliente di collegarsi da remoto, utilizzando un computer, all'elaboratore della banca presso la quale intrattengono il rapporto di conto corrente.
risorse informatiche aziendali: qualsiasi combinazione di apparati tecnologici *dell'Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* e del *SISSR*, hardware o software utilizzati per le comunicazioni elettroniche ed elaborazione dei dati;
S.C. Ingegneria Biomedicale e Sistema Informatico: la struttura organizzativa che all'interno dell'*Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* si occupa della gestione operativa delle risorse informatiche aziendali;
server: designa il/i computer utilizzati dall' *Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* per fornire i servizi ed archiviare dati;
sito internet/intranet: è l'insieme dei file realizzati secondo lo standard HTML destinati ad essere installati su un server web e visibili dagli utenti;
situazione d'emergenza: circostanza nella quale il venir meno di un'azione può provocare un serio pregiudizio a persone o cose, comportare il danneggiamento o la scomparsa di dati o impedire la

verifica di una grave responsabilità dell' *Azienda per l'Assistenza Sanitaria 5 "Friuli Occidentale"* o di qualche dipendente dell'*Azienda*;
spam: è l'invio di grandi quantità di messaggi. Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail;
supporti di memorizzazione: dischetti, cd, dvd, chiavette USB, hard disk esterni, ecc.
SISSR: sistema informativo socio-sanitario regionale coordinato dalla *Direzione Centrale Salute*, inteso come il complesso dell'infrastruttura telematica, delle procedure applicative e condivise con tutte le aziende sanitarie della *Regione Friuli Venezia Giulia*;
utente: dipendenti a tempo pieno o parziale, collaboratori, consulenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri individui in possesso di specifiche credenziali di autenticazione alla quale è consentito l'utilizzo dell'accesso alle risorse aziendali.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: TECLA DEL DO'
CODICE FISCALE: DLDTCL62T45H816U
DATA FIRMA: 09/06/2016 13:57:07
IMPRONTA: 655462BC11E863EFD9F9E3484585BF7D10F14110C252C3F3D830896563D17F55
10F14110C252C3F3D830896563D17F55D3A48664926EB674E70AE0D2514E7B1A
D3A48664926EB674E70AE0D2514E7B1A410C3538C86CAF2A71463FD5F00A2E39
410C3538C86CAF2A71463FD5F00A2E39EAA257A15E58CE752BFB7E8E6A9B7E38

NOME: ROBERTO ORLICH
CODICE FISCALE: RLCRRT59H24L424T
DATA FIRMA: 09/06/2016 14:46:40
IMPRONTA: 5D448143EBA774B61768F151FDA2BB0E5064994CC8622F906B38518E098DAB78
5064994CC8622F906B38518E098DAB78236402E38E993E6546A6624C5732EA2E
236402E38E993E6546A6624C5732EA2E4C33B523C63CF587C034C1C5E8A25E40
4C33B523C63CF587C034C1C5E8A25E40BC0805923C13D5F308E26FB7B54A6F23

NOME: GIUSEPPE SCLIPPA
CODICE FISCALE: SCLGPP52T31I403U
DATA FIRMA: 09/06/2016 14:49:39
IMPRONTA: 0741E27A87C5CD7C1290AA5E86C681F47F3B93451FC721805B0731FA130673B5
7F3B93451FC721805B0731FA130673B5389D5330DAC0F7BF9E4083DA3A7E5638
389D5330DAC0F7BF9E4083DA3A7E5638A14CD2AFA0605CADD7ED53D83DBD1E3D
A14CD2AFA0605CADD7ED53D83DBD1E3D54AF077D4E1C8790E47077CD227D91A6

NOME: GIORGIO SIMON
CODICE FISCALE: SMNGRG55D25I403Y
DATA FIRMA: 09/06/2016 14:52:51
IMPRONTA: 88993F4E029E89635DFD76E590E2AF899BBE1B413899509831269D1BF9413DEC
9BBE1B413899509831269D1BF9413DECAF96E1F9A60971831B3E6EFDB95FE4DF
AF96E1F9A60971831B3E6EFDB95FE4DFF55A56DCED43063F00AC4209679CB1D5
F55A56DCED43063F00AC4209679CB1D50F6B1E6243EC6BC5F07F80F6834DDD4C