TITOLO	REGOLAMENTO PER L'UTILIZZO DEI DISPOSITIVI E SERVIZI INFORMATICI
Tipologia Documento	Regolamento
Area di appartenenza	Sistemi Informativi aziendali
Numero Codice	QD_ENT_20212_1274
Raccolta	Sistemi Informativi

Redatto da	Verificato da	Approvato da
Coordinatore del Gruppo di Lavoro Dirigente Informatico U.O.C. Sistemi Informativi aziendali Dott. Paolo Colombo	RSGQ Dott. Roberto Agosti	Direttore U.O.C. Sistemi Informativi aziendali Dott. Giovanni Delgrossi

Storia delle modifiche al documento

Data	Numero revisione	Descrizione delle modifiche
31/01/2020	00	Nuova emissione
29/01/2021	01	Adeguamento per costituzione ASST della Brianza

Gruppo di lavoro

Nome	Ruolo	Struttura
Dott. Giovanni Delgrossi	Direttore	U.O.C. Sistemi Informativi aziendali
Rag. Giuseppe Noschese	Responsabile	U.O.S. Architetture Informatiche
Dott. Paolo Colombo	Dirigente Informatico	U.O.C. Sistemi Informativi aziendali

Indice

Art. 1 - Introduzione

L'Azienda Socio Sanitaria Territoriale della Brianza dispone di una architettura informatica complessa ed articolata attraverso la quale vengono resi disponibili sistemi, tecnologie e servizi che supportano il corretto ed efficace svolgimento delle attività dei professionisti di ambito sociosanitario ed amministrativo.

Il personale che opera a diverso titolo presso l'ASST della Brianza usufruisce di strumenti e servizi informatici messi a disposizione dall'Azienda per lo svolgimento delle rispettive attività professionali.

Il corretto utilizzo delle attrezzature informatiche, postazioni di lavoro, dispositivi, servizi applicativi ed informativi da parte degli utenti aziendali è un requisito fondamentale per assicurare il corretto funzionamento dell'intera architettura informatica, la valorizzazione del patrimonio informativo e la protezione dei dati che vengono trattati per lo svolgimento delle attività istituzionali.

1.1 Scopo

Il documento "*Regolamento per l'utilizzo dei dispositivi e dei servizi informatici*" descrive le modalità tecniche ed operative con le quali devono essere utilizzate le attrezzature informatiche, i dispositivi digitali, i servizi applicativi e informativi da parte degli utilizzatori autorizzati.

Il documento intende rappresentare un riferimento generale rivolto a tutto il personale che opera presso l'ASST della Brianza, sin dal momento dell'assunzione, e descrivere in modo chiaro e comprensibile le modalità tecniche, operative e comportamentali a cui gli utilizzatori si devono attenere.

1.2 Campo di applicazione

Il regolamento si applica alle attrezzature ed ai servizi informatici di utilizzo generale resi disponibili dall'ASST della Brianza al personale che opera a diverso titolo nei reparti, servizi ed uffici dell'amministrazione. Nel caso il personale faccia uso di sistemi applicativi e servizi particolari in uso presso il proprio reparto di assegnazione, dovrà eventualmente, fare riferimento a regolamenti specifici.

Il presente documento ha decorrenza dalla data di emissione ed ha validità a tempo indeterminato, salvo incorra la necessità di apportare variazioni e/o integrazioni o di emettere procedure sostitutive.

1.3 Riferimenti esterni

- Regolamento Europeo 679/2016 per la Protezione dei Dati - GDPR
- Normative integrative garante privacy
- Misure minime per la Sicurezza Informatica delle Pubbliche Amministrazioni – Agenzia per l'Italia Digitale

- Direttiva NIS (Network Information Security) 2016/1148
- Garante Privacy - Linee Guida per la gestione del Dossier Sanitario

1.4 Riferimenti interni

Il presente Regolamento è uno degli elementi di un corpus normativo interno, composto da una politica, regolamenti e direttive interne, che disciplinano aspetti generali o specifici della sicurezza informatica e della protezione dei dati, afferenti al presente Regolamento. In particolare, si faccia riferimento ai seguenti documenti pubblicati sulla Intranet aziendale (sezione "Documentale" area Direzione Generale/Sistemi Informativi) e disponibili a tutto il personale:

- Politica per la protezione dei dati e della sicurezza delle informazioni
- Piano di sviluppo triennale dei Sistemi Informativi
- Piano di Continuità Operativa e Disaster Recovery
- Gestione dei dati sanitari
- Conservazione Digitale

1.5 Termini, definizioni, abbreviazioni

GDPR – General Data Protection Regulation

AgID – Agenzia per l'Italia Digitale

NIS – Network Information Security

SIEM – Security Information and Event Management

BC – Business Continuity

DR – Disaster Recovery

1.6 Obiettivi

Gli obiettivi che la ASST della Brianza si propone di perseguire per assicurare il più alto livello possibile di protezione dei dati gestiti vengono descritti nel documento "*Politica per la protezione dei dati e della sicurezza delle informazioni* ". Il presente regolamento definisce le modalità tecniche ed operative che contribuiscono in modo significativo al raggiungimento degli obiettivi posti con particolare riferimento ai seguenti obiettivi generali:

- Riservatezza delle informazioni attraverso la prevenzione di divulgazione ed uso improprio dei dati.
- Disponibilità delle informazioni a supporto dei processi sociosanitari e disponibilità delle risorse tecnologiche e delle capacità elaborative necessarie al loro trattamento.

- Integrità delle informazioni attraverso processi che assicurino la consistenza, completezza e validità delle informazioni ai fini dei processi sociosanitari.

1.7 Deroghe ed eccezioni

Le prescrizioni contenute nel presente Regolamento, nelle direttive e nelle istruzioni tecniche per la sicurezza devono essere osservate obbligatoriamente.

Tuttavia, non è possibile escludere a priori che si presenti, in casi eccezionali, la necessità di derogare le direttive vigenti o di stabilirne delle eccezioni, purché siano effettivamente tali e l'Azienda sia disposta ad accettare il rischio che ne deriva.

In ogni caso, qualunque deroga o eccezione alle prescrizioni delle direttive e delle linee guida, per essere ammessa, deve essere espressamente giustificata, richiesta ed autorizzata da funzioni aziendali che ne abbiano la responsabilità. Ogni deroga deve essere approvata dal Direttore dell'U.O.C. Sistemi Informativi previa verifica documentata da parte del Responsabile della Sicurezza delle Informazioni.

1.8 Risorse informatiche

Ai fini della sicurezza, si identificano come risorse:

- ***Apparati fisici e dispositivi***, direttamente coinvolti nel processo di elaborazione, archiviazione e trasmissione delle informazioni. Essi sono definiti sensibili quando il loro danneggiamento, alienazione o distruzione può provocare l'interruzione di funzionamento e la conseguente sospensione di servizio, ovvero la diffusione di informazioni.
- ***Sistemi operativi o prodotti software***. Essi sono definiti sensibili quando la loro modifica, cancellazione o indisponibilità può comportare l'interruzione di funzionamento e la conseguente sospensione del servizio, ovvero la possibilità di accesso o alterazione di dati da parte di personale non autorizzato.
- ***Software applicativo***. Esso è definito sensibile quando la sua manomissione, cancellazione o indisponibilità può produrre la sospensione di alcune funzioni o l'alterazione delle corrette caratteristiche di funzionamento del sistema informativo.
- ***Informazioni (dati).*** Essi sono definiti sensibili quando la loro indisponibilità, manomissione o divulgazione può provocare la sospensione di funzioni del sistema informativo o compromettere il suo corretto funzionamento o procurare danno diretto o indiretto all'Azienda.

1.9 Responsabilità e principio di non-ricusazione

Chiunque usi risorse informatiche della ASST della Brianza deve operare nei limiti delle proprie competenze e secondo le norme definite.

L'operato dell'utente su risorse classificate sensibili (vedi Classificazione delle Risorse) in quanto a riservatezza, disponibilità ed integrità deve essere riconducibile ad una non negabile responsabilità personale, attraverso opportuni meccanismi di autenticazione (non-ricusazione).

Chiunque operi in violazione delle norme aziendali o al di fuori delle proprie competenze è sottoposto ai provvedimenti indicati nel paragrafo Provvedimenti sanzionatori, in relazione alla gravità dell'operato.

Art. 2 - Regolamento per l'utilizzo delle-risorse informatiche dell'ASST della Brianza

All'inizio del rapporto lavorativo o di consulenza, l'U.O.C Risorse Umane con il supporto dell'U.O.C. Sistemi Informativi dell'ASST della Brianza autorizza il personale all'uso delle attrezzature informatiche aziendali di base (Personal computer e periferiche), al servizio di navigazione Internet, al servizio di posta elettronica e ad altri applicativi e servizi informatici specifici, qualora necessari.

Gli utilizzatori vengono forniti immediatamente di "Userid" e "Password" univoche ed individuali necessarie per accedere alle postazioni di lavoro presenti presso il servizio di assegnazione e per accedere ai servizi di comunicazione Internet/Intranet e posta elettronica con casella personale.

L'accesso a sistemi applicativi specifici viene autorizzato a seguito di verifica dell'esistenza dei presupposti necessari, viene abilitato con configurazione del corretto profilo e ruolo applicativo richiesto e può essere modificato o revocato a seguito di variazioni delle necessità del servizio cui è assegnato il dipendente.

L'ASST della Brianza autorizza normalmente tutto il personale con un rapporto lavorativo continuativo all'utilizzo delle seguenti attrezzature e servizi di comunicazione di base:

- Personal Computer e periferiche associate;
- Servizio di posta elettronica con casella personale;
- Servizio di navigazione Internet/Intranet con accesso individuale.
- Servizi di comunicazione (telefonia e messaggistica)

Il presente Regolamento descrive le modalità con le quali devono essere utilizzate da parte degli utenti autorizzati le attrezzature informatiche aziendali, i dispositivi e le soluzioni applicative che compongono l'architettura informatica dell'ASST della Brianza.

2.1. Titolarità delle attrezzature informatiche e dei dati trattati

L'ASST della Brianza è esclusiva titolare e proprietaria delle attrezzature informatiche, delle periferiche associate e dei dispositivi mobili messi a disposizione degli utilizzatori ai soli fini dell'attività lavorativa.

L'ASST è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante le proprie attrezzature informatiche e dispositivi.

Il personale non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nelle attrezzature informatiche aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

2.2. Finalità dell'utilizzo delle attrezzature informatiche e dei dispositivi

Le attrezzature ed i dispositivi informatici assegnati sono uno strumento lavorativo nelle disponibilità degli utilizzatori esclusivamente per un fine di carattere lavorativo. *I dispositivi informatici, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali*, se non eccezionalmente e nei limiti evidenziati dal presente Regolamento.

Qualsiasi eventuale tolleranza da parte dell'ASST della Brianza, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Regolamento.

2.3. Restituzione delle attrezzature e dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza del personale con l'Azienda o, comunque, al venir meno, ad insindacabile giudizio dell'ASST, della permanenza dei presupposti per l'utilizzo delle attrezzature informatiche e dei dispositivi aziendali assegnati, gli utilizzatori hanno i seguenti obblighi:

- Procedere immediatamente alla restituzione delle attrezzature e dispositivi assegnati.
- Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.
- Sospendere l'utilizzo dei servizi di comunicazione e dei servizi applicativi assegnati durante lo svolgimento della propria attività professionale.

2.4. Credenziali personali e gestione delle Password

L'utilizzo di credenziali individuali con password riservate e adeguatamente protette rappresenta il principale metodo di autenticazione utilizzato dall'ASST della Brianza per garantire l'accesso protetto ad un sistema informatico oppure ad un applicativo software.

Per l'accesso ad alcuni sistemi informatici e sistemi applicativi di particolare criticità e riservatezza, l'ASST può utilizzare sistemi di autenticazione più complessi che, oltre alle credenziali individuali, prevedono l'utilizzo di un secondo meccanismo di autenticazione denominato "autenticazione forte".

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'ASST nel suo complesso. La sicurezza della password personale diminuisce nel tempo e, pertanto, è necessario che ciascun utente provveda alla sua sostituzione con una nuova password periodicamente. L'ASST della Brianza chiede obbligatoriamente a tutti gli utilizzatori la sostituzione della password individuale almeno ogni 3 mesi.

L'ASST ha implementato alcuni meccanismi che permettono di aiutare e supportare gli utenti in una corretta gestione delle password con particolare riferimento per le password di accesso al Dominio; l'ASST ha attuato un sistema automatico di richiesta di aggiornamento della password sulla base del livello di minimo di sicurezza ritenuto necessario e, comunque, in linea con quanto richiesto dalla normativa privacy.

L'ASST della Brianza per consentire agli utenti di accedere al Domino informatico aziendale, ai servizi di Posta Elettronica ed agli altri sistemi applicativi con le stesse credenziali personali e relative password. Tale modalità, seppur estremamente comoda per gli utenti che non devono in tal modo avere password specifiche per i diversi sistemi utilizzati, necessità di molta attenzione e riservatezza nella gestione delle proprie credenziali individuali.

Le credenziali e relative password NON devono essere memorizzate su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Le credenziali di accesso che non vengono utilizzate da parte degli incaricati per un periodo superiore ai sei mesi verranno disattivate dall'ASST.

In qualsiasi momento l'organizzazione si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, disabilitando le credenziali di accesso e/o modificando la password ad esse associate.

L'ASST della Brianza attua periodicamente, normalmente su base annuale, una procedura di verifica e ricertificazione delle utenze registrate e verifica l'adeguatezza dei profili di autorizzazione che, a causa di cambio di reparto e/o di mansione, potrebbero avere subito modifiche.

2.4.1. Regole per la corretta gestione delle Password

L'utente, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

1. le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. occorre cambiare immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura";
3. le password devono essere lunghe almeno 8 caratteri e devono contenere lettere maiuscole, minuscole, caratteri speciali e numeri;

4. le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
6. evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ente.

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti.

2.4.2. Password non ammesse

Al fine di una corretta gestione delle password, l'ASST stabilisce il divieto di utilizzare come propria password:

1. nome, cognome e loro parti;
2. lo username assegnato;
3. una password già impiegata in precedenza.

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio;
3. la propria data di nascita, quella del coniuge, ecc.;
4. targa della propria auto;
5. numero di telefono proprio, del coniuge, ecc.;
6. parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);
7. qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

2.4.3. La Password nei sistemi

Ogni utente può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione una funzionalità di questo tipo (Change password), oppure facendone richiesta. La password non può essere recuperata in alcun modo ma solamente sostituita con una nuova dall'ASST anche qualora l'Utente l'abbia dimenticata.

2.4.4. Audit delle Password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'ASST potrebbe effettuare analisi periodiche sulle password degli utenti al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli interessati.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato richiesto di cambiarla.

2.5. Protezione delle postazioni di lavoro

In questa sezione vengono trattate le operazioni a carico dell'utente e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

2.5.1. Operazioni di Login e Logout

Il "Login" è l'operazione con la quale l'utente si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password ed aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

Ogni utente è autorizzato all'utilizzo unicamente del proprio specifico username e password per accedere a tutti i sistemi ai quali è stato autorizzato. L'ASST, solo in casi eccezionali e specifici, potrà assegnare un univoco username e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

2.5.2. Obblighi del dipendente

L'utilizzo dei dispositivi fisici e la gestione dei dati contenuti deve avvenire nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'utente deve quindi eseguire le operazioni seguenti:

- se si allontana dalla propria postazione dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti;
- bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
- chiudere la sessione (Logout) a fine giornata;
- controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

2.6. Utilizzo e gestione del Personal Computer aziendale

Il sistema informativo aziendale è composto da un insieme di sistemi informatici centrali e molteplici personal computer e dispositivi connessi alla rete aziendale che utilizzano diversi sistemi operativi e applicativi.

L'Ente non effettua il backup dei dati memorizzati in locale. Non sarà quindi possibile recuperare i files creati, elaborati o modificati sul computer assegnato e salvati localmente in caso di guasto o malfunzionamento del sistema.

2.6.1. Corretto utilizzo del Personal Computer aziendale

Il computer assegnato all'area di lavoro dove opera l'utente è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività necessarie ed affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso a ciascun Personal Computer è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata. Il Personal Computer contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare l'utente deve adottare le seguenti misure:

1. uilizzare solo ed esclusivamente le aree di memoria della rete resa disponibile dall'ASST per creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;

3. utilizzare sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;
4. non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Personal Computer o a meno di necessità stringenti e sotto il proprio costante controllo.

2.6.2. Divieti espressi sul Personal Computer aziendale

All'utente è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'ASST.
4. Installare alcun software di cui l'ASST non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. Non è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

2.7. Internet

La connessione alla rete internet dal dispositivo informatico assegnato è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati.

2.7.1. Misure preventive per ridurre navigazioni illecite

L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

2.7.2. Divieti espressi per la navigazione Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.
2. È fatto divieto di accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'utente lo scarico di software (anche gratuito) prelevato da siti Internet;
4. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
5. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
6. È vietato all'utente promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
7. E' vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'ASST stessa.
8. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'utente inadempiente

2.7.3. Divieto di sabotaggio

È vietato accedere ad alcuni siti Internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'ente per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

2.7.4. Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. Legge 22 aprile 1941, n. 633 e successive modificazioni, D. Lgs. 6 maggio 1999, n. 169 e Legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ecc.) se non espressamente autorizzato dall'organizzazione.

2.8. Posta Elettronica

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.

Gli utenti possono utilizzare unicamente indirizzi di posta elettronica nominativi.

Alcune caselle di posta elettronica possono essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, …) per evitare che il destinatario delle e mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2.8.1. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli utenti e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'organizzazione tramite email all'indirizzo *security@asst-brianza.it* quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

2.8.2. Divieti espressi

3. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.
4. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.

5. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.
6. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
7. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

2.8.3. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'utente riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione tramite l'email *security@asst-brianza.it*

2.9. Utilizzo di altri dispositivi

2.9.1 L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'organizzazione agli utenti che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.

L'Incaricato è responsabile dei device mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping). Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'ente. I device mobili utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'ente che provvederà – se del caso – ad occuparsi delle procedure connesse

alla privacy. Anche di giorno, durante l'orario di lavoro, all'utente non è consentito lasciare incustoditi i device mobili.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'ente.

In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'esterno devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

2.9.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

2.9.3. Device personali

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'ente per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato, salvo esplicita autorizzazione, l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell'ente solo se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali device dovranno essere preventivamente valutati dall'ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

2.9.4. Utilizzo di cellulare personale

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di pazienti, clienti o fornitori.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell'ente solo se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dall'ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

2.9.5. Distribuzione dei device

Ogni Device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'ente che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare l'ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati

Art. 3 - Sistemi in Cloud

3.1. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un insieme di risorse o servizi informatici, come l'archiviazione, l'elaborazione o la gestione di dati tramite sistemi esterni alla rete aziendale, solitamente erogati attraverso Internet.

Utilizzare un servizio di cloud computing per l'invio o la memorizzazione di dati personali o sensibili, espone l'ente a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati su sistemi di aziende che spesso risiedono in uno stato diverso da quello dell'ente con soluzione di protezione, gestione e backup dei dati non conforme con le normative del nostro paese.

Esempi di servizi Cloud sono: Whatsapp, Dropbox, One Drive (Microsoft), Google Drive, iCloud, WeTransfert, Telegram, ecc.

3.2. Utilizzo di sistemi Cloud

E' vietato agli incaricati l'utilizzo di sistemi cloud non espressamente approvati dall'ente. Per essere approvati i sistemi cloud devono rispondere ai seguenti requisiti minimi:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia o all'interno di uno degli stati membri dell'Unione Europea
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'ente;
- L'azienda che fornisce il sistema in cloud deve comunicare all'ente, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

Art. 4 - Note finali

Il presente documento, le procedure in esso contenute e gli allegati, sono documenti aziendali dinamici, vale a dire che sono soggetti a revisione e aggiornamento periodico in rapporto a nuove disposizioni e raccomandazioni internazionali / nazionali nonché a suggerimenti degli operatori sanitari dell'azienda. Referente aziendale per il presente documento organizzativo e per gli eventuali aggiornamenti è l'U.O.C. Qualità e Risk Management.

Art. 5 - Feedback aziendale

Tutti gli operatori interessati direttamente o indirettamente a quanto contenuto nel presente documento, possono inviare richieste di chiarimento, suggerimenti e osservazioni all'U.O.C. Sistemi Informativi aziendali utilizzando il servizio di posta elettronica aziendale, al seguente indirizzo:

sia@asst-brianza.it