Sistema Socio Sanitario Regione Lombardia ATS Brianza	**DIPARTIMENTO AMMINISTRATIVO, DI CONTROLLO e degli AFFARI GENERALI e LEGALI** **Servizi Informativi Aziendali**

REGOLAMENTO

REGOLAMENTO AZIENDALE SULL'UTILIZZO DELLE RISORSE INFORMATICHE

ID 02371

rev	data di verifica	Descrizione delle modifiche	FIRMA DI REDAZIONE NOMINATIVO (FUNZIONE)	FIRMA DI VERIFICA NOMINATIVO (FUNZIONE)
0	25.11.2016	Prima emissione	Roberto Furlani	Rosaria di Fiore
1	01.10.2019	Aggiornamento terminologia e regole utilizzo spazi sindacali; aggiornamento sul tema sicurezza dati recependo le indicazioni del Team aziendale	Marco F. Romanelli Rosaria Di Fiore	Raffaella Clelia Borra

Approvato con deliberazione nr. 676 del .. 7 OTT. 2019

Sommario

Premessa 3
Art. 1: Definizioni 4
Art. 2: Scopo e campo di applicazione 8
Art. 3: Entrata in vigore del regolamento 8
Art. 4: Uso della postazione di lavoro 8
Art. 5: Credenziali di autenticazione 10
Art. 6: Utilizzo della rete locale 11
Art. 7: Utilizzo dei servizi informatici 12
Art. 8: Utilizzo e conservazione dei supporti rimovibili 12
Art. 9: Utilizzo di personal computer portatili, tablet, dotazioni mobili 13
Art. 10: Uso della posta elettronica 13
Art. 11: Accesso ad Internet 14
Art. 12: Protezione antivirus 15
Art. 13. risorse intranet e mail per organizzazioni sindacali 15

Premessa

La progressiva diffusione di nuove tecnologie informatiche, l'accesso alla rete Internet tramite postazioni di lavoro aziendali, la diffusione di esigenze sempre più marcate dell'utilizzo di strumenti di comunicazione, scambio dati e documenti sia all'interno che verso soggetti esterni, aumentano i pericoli legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia esponendo l'Agenzia ai rischi di un coinvolgimento sia patrimoniale che penale.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza che caratterizza il rapporto lavorativo fra l'Agenzia di Tutela della Salute (ATS) della Brianza e i propri dipendenti/collaboratori e adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, l'Agenzia di Tutela della Salute (ATS) della Brianza adotta il presente regolamento, promosso dall'U.O.C. Servizi Informativi Aziendali, per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare minacce alla sicurezza nel trattamento dei dati e/o alla continuità operativa.

Il regolamento oltre a dettare una disciplina per l'utilizzo degli strumenti informatici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei Servizi informativi aziendali, quali ad es. il rispetto della normativa sulla tutela legale del software.

Il presente regolamento è redatto tenendo in considerazione le Linee Guida del Garante Privacy G.U. n. 58 del 10.03.2007 e le raccomandazioni del Consiglio d'Europa CM_REC (2015) 5 adottate il 01.04.2015. Essa ha lo scopo di definire i criteri di utilizzo dei servizi informatici aziendali disciplinando le modalità di accesso e di utilizzo della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire all'interno e all'esterno dell'Amministrazione.

Art. 1: Definizioni

Si forniscono di seguito le definizioni delle componenti dell'infrastruttura informatica aziendale.

ATS	Agenzia di Tutela della Salute (ATS) della Brianza
Responsabile di struttura	Direttore di Dipartimento o Responsabile di struttura semplice o complessa
SIA	Servizi Informativi Aziendali
Utente	Ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione con diritto di accesso ai servizi informatici e di rete, in accordo con il proprio profilo di appartenenza e il presente Regolamento.
Rete interna o privata	Insieme delle risorse di rete che consentono il collegamento informatico e telematico tra le diverse sedi dell'ATS. La rete interna si dice anche 'Privata' in quanto non visibile, né accessibile da postazioni non aziendali.
Internet	Rete di accesso pubblico alla quale la rete interna accede e si presenta con i propri servizi.
Sistema Informativo	Un sistema informativo è l'insieme delle infrastrutture informatiche hardware e software che consente di collezionare, processare, gestire, memorizzare, distribuire i dati aziendali. Le componenti di un sistema informativo consistono in postazioni server, banche dati, postazioni di lavoro, periferiche accessorie di stampa e di memorizzazione dati, reti ed apparati di interconnessione interne ed esterne, software di base e software applicativi. L'insieme dei software e delle periferiche a corredo di una postazione di lavoro o server può variare a seconda delle funzionalità e dei servizi informatici da garantire e/o da attivare.

Postazione di lavoro (PdL)	La postazione di lavoro è un PC corredato dal software di base per lo svolgimento delle attività di ufficio. Essa può essere collegata ad una stampante propria oppure ad una stampante condivisa in rete (a disposizione cioè di più postazioni). Il PC può essere fisso, portatile oppure essere rappresentato da un dispositivo mobile (es. tablet). Ogni operatore dell'Agenzia può accedere al dominio della rete aziendale mediante delle credenziali (utente e password) fornite dalla UO Servizi Informativi Aziendali a seguito del ricevimento di una richiesta effettuata secondo le indicazioni riportate nella Procedura per la gestione degli account e delle risorse di rete.
Postazione Server	La postazione server è un computer con le principali funzionalità di seguito elencate: • gestione di uno o più applicativi aziendali; • gestione del dominio di rete aziendale; • memorizzazione degli archivi dei dati e dei documenti prodotti dal sistema informativo; • gestione della posta elettronica interna ed esterna; • gestione di aree comuni di disco a disposizione degli utenti di un servizio per la memorizzazione di dati e documenti da condividere; • gestione backup dei dati; • gestione software antivirus; • gestione basi di dati a supporto degli applicativi aziendali.
Periferiche	A titolo non esaustivo si elencano di seguito alcune tipologie di periferiche: • stampanti collegate direttamente alla postazione di lavoro oppure in rete per un utilizzo comune e condiviso da parte di più postazioni; • stampanti portatili; • telefoni cellulari collegati al pc ed usati come dispositivi di massa per memorizzazione dati; • lettori interni/esterni di CD/DVD;

	• dischi rigidi interni/esterni; • chiavetta usb; • scanner collegati alle postazioni di lavoro; • lettori DVD/CD-RW; • masterizzatori di DVD/CD; • sistemi interni/esterni di back-up dati su cartucce e/o nastri; • eventuali altri dispositivi interni od esterni alle postazioni di lavoro o server che svolgono funzioni di memorizzazione dati o connessioni telematiche (es. modem, chiavette per la navigazione Internet).
Rete Telematica Aziendale	La rete telematica aziendale è costituita dall'infrastruttura di telecomunicazioni e di tutti i servizi Intranet/Internet ai quali gli operatori dell'Agenzia, mediante le postazioni di lavoro collegate alla rete, possono accedere in base alle autorizzazioni concesse dai Responsabili di struttura.
Account Istituzionale	Account fornito dall'ATS a ciascun Utente per accedere ai servizi informatici e di rete in accordo con il relativo Profilo Utente. Può consistere nella coppia utente e password o in una smart card (es. carta operatore SISS) + PIN.
Profilo Utente	Tipologia di Utente con accesso ad un numero predefinito di servizi informatici e di rete.
Programmi Applicativi	Programmi che si basano su banche dati e svolgono funzioni specifiche tipicamente a supporto di processi aziendali.
Programmi di base	A titolo non esaustivo si elencano di seguito alcune tipologie di software a corredo delle postazioni di lavoro: • Sistema Operativo Microsoft Windows • Pacchetto di produttività d'ufficio MS-

	Office (Microsoft) • Pacchetto di produttività d'ufficio Libreoffice • Software per la creazione lettura e la modifica dei file pdf Acrobat Reader (Adobe) • Software di compressione dei file (es. 7zip) • Software antivirus • Software di Navigazione Internet • Software di consultazione della posta elettronica Software a corredo delle postazioni server: • Sistema Operativo Microsoft Windows • Sistema di virtualizzazione • Antivirus Server • Software di backup • Database (es. Oracle, Sql)
LOG	File di registrazione cronologica delle operazioni informatiche svolte sui sistemi server e sulle postazioni.
Dati Informatici	I Dati Informatici sono sia tutti quelli prodotti ed elaborati per tramite della postazione di lavoro nell'ambito del lavoro d'ufficio che quelli generati dal sistema informativo aziendale come esito delle operazioni attivate dall'utente.
VPN	Virtual Private Network
Credenziali di autenticazione	L' Allegato B. **Disciplinare tecnico in materia di misure minime di sicurezza** *(Artt. da 33 a 36 del Codice in materia di protezione dei dati personali) riporta che* 'Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo'. Un esempio di codice per l'identificazione dell'incaricato è il nome utente o username.

	Un esempio di parola chiave è la password, un esempio di dispositivo di autenticazione è la smart card operatore SISS, un esempio di codice identificativo associato al dispositivo di autenticazione è il PIN.
Cloud	Il Cloud, consolidata tecnologia di condivisione di dati e servizi, mette a disposizione tra l'altro **uno spazio di archiviazione** che risulta essere accessibile in qualsiasi momento ed in ogni luogo cliccando su un link Internet.

Art. 2: Scopo e campo di applicazione

Il presente regolamento ha lo scopo di definire i criteri di utilizzo delle risorse e dei servizi informatici aziendali.
Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'ATS, a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Art. 3: Entrata in vigore del regolamento

Il nuovo regolamento entra in vigore a partire dalla data di deliberazione.

Art. 4: Uso della postazione di lavoro

4.1 Il Personal Computer o altro dispositivo informatico affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ogni dispositivo informatico deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

4.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'ATS solo attraverso specifiche credenziali di autenticazione.

4.3 Il personale incaricato, che opera presso i SIA, è autorizzato a compiere interventi sia hardware che software sul sistema informatico aziendale e sulle postazioni di lavoro, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.). Detti Interventi potranno anche comportare l'accesso in

qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti Internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Agenzia, si applica anche in caso di assenza prolungata o manutenzione straordinaria.

4.4 L'eventuale sostituzione della postazione di lavoro dell'utente e/o la formattazione del PC avviene ad insindacabile giudizio del SIA secondo le modalità e le urgenze definite da questi ultimi a tutela della sicurezza aziendale. Il personale incaricato dei Servizi Informativi ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione all'utente della necessità dell'intervento stesso.

4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale dei SIA per conto dell'ATS, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa ATS a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

4.6 Salvo preventiva espressa autorizzazione del personale dei SIA, non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc...).

4.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale dei Servizi Informativi Aziendali nel caso in cui siano rilevati virus o comunque si ha anche solo il dubbio che vi possano essere state possibili infezioni.

4.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo non autorizzato da parte di terzi.

4.9 Sul personal computer e su ogni altra area di memorizzazione dati messa a disposizione degli utenti non devono essere presenti file personali.

4.10 Dati e documenti aziendali e/o sensibili, quando necessario, devono essere trasferiti solo previa criptazione, ossia protetti da password. E' inoltre necessario che la complessità delle password utilizzate sia sufficientemente elevata.

4.11 La postazione di lavoro è assegnata all'utente che si impegna a non cederne l'uso a persone non autorizzate;

4.12 Qualora l'utente rilevi l'avvenuto utilizzo da parte di terzi non autorizzati della propria postazione, è tenuto ad informare tempestivamente i Servizi Informativi.

4.13 Il personale dei SIA è autorizzato a procedere al ritiro di postazioni inutilizzate.

Art. 5: Credenziali di autenticazione

5.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del SIA, previa formale richiesta scritta del responsabile del personale o di struttura nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori, la preventiva richiesta verrà inoltrata direttamente dal responsabile del personale o di struttura con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

5.2 Nel caso di rapporti di lavoro a tempo determinato la richiesta di attivazione delle credenziali di autenticazione dovrà contenere la durata del relativo periodo di validità.

5.3 In caso di cessazione o modifica del rapporto di lavoro/collaborazione dell'utente o delle mansioni ad egli assegnate o in caso di dipendenti dislocati presso altri Enti, il Responsabile di struttura competente inoltra ai SIA richiesta tempestiva di disattivazione delle relative abilitazioni e credenziali. Contestualmente i SIA provvederanno al ritiro della postazione di lavoro aziendale assegnata all'utente.

5.4 I SIA provvedono alla disabilitazione delle utenze mensilmente a fronte delle cessazioni e sospensioni del servizio che figurano mensilmente nel sistema di gestione del personale.

5.5 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dai SIA, associato ad una parola chiave (password) riservata che dovrà venire custodita dall' utente con la massima diligenza e non divulgata. Le password sono infatti personali e segrete. L'utente non deve divulgare le proprie password di accesso alla postazione di lavoro, di accesso agli applicativi aziendali e ad ogni altra funzionalità del sistema aziendale e/o regionale per la quale viene fornita una password nominalmente ad ogni singolo operatore. **E' vietato usare password e utenze diverse dalle proprie.** Un uso scorretto delle password può innescare seri problemi di sicurezza; pertanto, in caso di utilizzo illecito della password, il responsabile di struttura che ne viene a conoscenza avrà cura di segnalarlo ai SIA allo scopo di richiedere la generazione di nuove password con conseguente inibizione di quella usata scorrettamente.

5.6 Non utilizzare mai le password aziendali (sia di applicativi che di accesso al pc) come proprie password di accesso per registrazioni a siti internet, social, newsletter, etc..in questo modo si agevola l'azione malevola da parte di hacker che più facilmente possono entrare in possesso delle credenziali di accesso ai dati aziendali.

5.7 Non fornire mai utenza e password di accesso a soggetti che non sono i diretti destinatari.

5.8 Evitare di comunicare via email utenze e password e comunque non comunicarli mai entrambi nel corpo dello stesso messaggio, in questo modo si facilita l'associazione della password all'utenza e dunque la conoscenza immediata e completa delle credenziali di accesso ai servizi e ai dati.

5.9 L'utente deve procedere alla modifica della parola chiave al primo utilizzo e, successivamente, almeno ogni tre mesi e comunque nel rispetto della vigente normativa in tema di privacy.

5.10 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri e/o simboli, anche in combinazione fra loro, deve essere composta da almeno dieci caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

5.11 In caso di violazione delle credenziali procedere immediatamente a cambiare la password e a comunicare la violazione ai Servizi Informativi Aziendali.

Art. 6: Utilizzo della rete locale

6.1 L'accesso alla rete locale dell'ATS avviene da parte di ciascun utente le credenziali di autenticazione ad egli assegnate e consegnate. E' proibito entrare nella rete o nei programmi con credenziali di autenticazione diverse da quelle assegnate.

6.2 Le credenziali vengono revocate alla chiusura del rapporto di lavoro o collaborazione tra l'utente e l'ATS. In ogni caso, al termine del rapporto di lavoro è fatto divieto all'utente di utilizzare le credenziali fornitegli per l'accesso ai servizi informatici ATS.

6.3 Le cartelle utenti presenti nei server dell'ATS sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio. Tutti i documenti per cui si renda necessaria la garanzia della conservazione devono essere posizionati sui server.

6.4 Il personale dei SIA può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete.

6.5 Con riferimento al principio di esattezza previsto al comma d), art. 5 del Nuovo Regolamento EU 2016/679, risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.6 E' fatto divieto di collegare alla rete aziendale computer personali e/o altri dispositivi informatici e computer non assegnati dal competente SIA, salvo motivata richiesta da parte del dirigente responsabile del richiedente ed autorizzazione da parte dei SIA. Inoltre, in questi casi, i SIA procederanno alla preliminare verifica del computer e/o dispositivo e sono autorizzati ad installare e configurare su di esso ogni strumento aziendale per la protezione della sicurezza.

6.7 L'Utente, preso atto che la conoscenza della password da parte di terzi può consentire agli stessi l'accesso ai servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della posta elettronica, uso indebito di servizi, ecc.), si impegna a:

- non cedere l'uso della propria Postazione di Lavoro (PdL) a persone non autorizzate;
- non lasciare incustodita ed accessibile la propria PdL soprattutto se connessa alla rete o a programmi applicativi con le proprie credenziali di autenticazione;
- custodire con diligenza le proprie credenziali e non comunicarle ad altre persone (es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare, nè condividere con altri la propria password;
- avvisare tempestivamente il proprio responsabile e i Servizi Informativi nell'ipotesi di smarrimento o uso improprio delle credenziali personali;
- non utilizzare credenziali di altri utenti nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.

Art. 7: Utilizzo dei servizi informatici

L'Utente è autorizzato all'utilizzo dei servizi unicamente nell'ambito delle proprie funzioni istituzionali dell'ATS.
A ciascun Utente, in fase di utilizzo dei servizi, è vietato:

- violare la privacy di altri utenti o dell'integrità di dati personali;
- compromettere l'integrità dei sistemi o dei servizi;
- compiere atti di criminalità informatica;
- accedere alla rete interna per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'ATS;
- consentire l'uso della connettività di rete a soggetti non autorizzati all'accesso alla Rete Interna;
- usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi;
- violare la sicurezza di archivi e banche tt, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete Interna, dei quali non si è destinatari specifici;
- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi;
- creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno;
- utilizzare la Rete dell'ATS e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale.

Art. 8: Utilizzo e conservazione dei supporti rimovibili

8.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, dischi esterni, memorie a stato solido, ecc.), contenenti dati sensibili nonché dati e/o informazioni aziendali, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

8.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili nonché dati e/o informazioni aziendali, ciascun utente dovrà contattare il personale dei Servizi Informativi e seguire le istruzioni da questo impartite.

8.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
8.4 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
8.5 E' vietato l'utilizzo di supporti removibili personali.

Art. 9: Utilizzo di personal computer portatili, tablet, dotazioni mobili

9.1 L'utente è responsabile del Personal Computer portatile o tablet o altra dotazione mobile assegnatogli dai SIA e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
9.2 I Personal Computer portatili o tablet o altra dotazione mobile utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
9.3 A garanzia della sicurezza, i Personal Computer portatili o tablet, per garantire il corretto aggiornamento degli applicativi installati e del sistema operativo Windows, devono essere connessi alla rete aziendale almeno mensilmente.
9.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni cui è stato assegnato un personal computer portatile o tablet o altra dotazione mobile aziendale.
9.5 Il personal portatile o tablet o altra dotazione mobile aziendale deve essere restituito ai SIA al termine del rapporto di lavoro o collaborazione con l'ATS.
9.6 Proteggere sempre con il pin lo sblocco del salvaschermo per poter utilizzare il cellulare. Evitare di memorizzare sul cellulare dati e/o informazioni aziendali.

Art. 10: Uso della posta elettronica

10.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
10.2 È fatto divieto di utilizzare le caselle di posta elettronica @ats-brianza.it per motivi diversi da quelli strettamente legati all'attività lavorativa e/o istituzionale. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzarle per:
- l'invio e/o il ricevimento di allegati contenenti fotografie, filmati o brani musicali (es.mp3) non legati all'attività lavorativa e/o istituzionale;
- l'invio e/o l'attivazione del ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, catene telematiche, ecc. Non si dovrà

in alcun caso procedere all'apertura degli allegati a tali messaggi, questo per evitare l'infezione da virus informatici.
- la registrazione a siti internet. Infatti una tale esposizione favorisce la cattura fraudolenta di informazioni relative ad indirizzi email e password aziendali consentendo più facilmente attacchi informatici ai dati e alle infrastrutture.

10.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensioni rilevanti.

10.4 Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile cancellare tutto, messaggio ed allegato, onde evitare infezioni da virus, ecc. non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

10.5 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) può inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto del Servizio di appartenenza. Tale funzionalità deve essere attivata dall'utente.

Art. 11: Accesso ad Internet

11.1 L'accesso alla Rete Interna da parte dell'Utente da Internet è consentito unicamente mediante i servizi di accesso remoto erogati dai SIA.

11.2 L'accesso ad Internet è consentito da tutte le postazioni di lavoro aziendali.

11.3 L'Utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine Internet ai quali abbia stabilito collegamento tramite link.

11.4 Le credenziali assegnate al singolo utente ed abilitato alla navigazione in Internet costituiscono uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso l'utente non potrà utilizzare Internet per:

- l'upload o il download di software, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale dei SIA);
- ogni forma di registrazione e accesso a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum e social network non professionali, l'utilizzo di chat line, di bacheche elettroniche (è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare firme e commenti) anche utilizzando pseudonimi (o nicknames) .

11.5 Il personale dei SIA è autorizzato al trattamento in forma anonima, tale da precludere l'immediata identificazione degli utenti, dei dati relativi al traffico Internet. I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive, di sicurezza e continuità operativa. Il controllo anonimo potrebbe concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali. L'avviso sarà circoscritto al Servizio a cui è riconducibile l'anomalia.
Verifiche su base individuale potranno essere legittimate solo in caso di individuazioni di specifiche anomalie come la rilevata presenta di virus o altre circostanze che necessitano di ulteriori controllo approfonditi.
11.6 Data la natura 'pubblica' dei Cloud disponibili su Internet (Dropbox, Google Drive, Wetransfer e molti altri), che sono ospitati su piattaforme distribuite su server di provider esterni e utilizzati da parte di tutti gli utenti di Internet, tali Cloud NON sono indicati per lo scambio di documenti e dati aziendali, specie se di tipo personale. In caso di necessità di scambio di informazioni/documenti con enti esterni, chiedere l'abilitazione ai servizi forniti dai SIA.

Art. 12: Protezione antivirus

12.1 Il sistema informatico dell'ATS è protetto da software antivirus, aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale attenendosi al rispetto del presente regolamento.
12.2 Nel caso il software antivirus rilevi la presenza di un virus evidenziando un messaggio di pop up sulla postazione, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, spegnere il computer, staccare il cavo, aprire un ticket all'assistenza tecnica e segnalare l'accaduto al personale dei SIA.

Art. 13. risorse intranet e mail per organizzazioni sindacali

ATS mette a disposizione delle organizzazioni sindacali sia dell'area dirigenza che dell'area comparto rispettivamente la casella di posta elettronica "oossdirigenza@ats-brianza.it" oosscomparto@ats-brianza.it abilitate ad inviare comunicazioni alla lista utenti.posta@ats-brianza.it che contiene tutti gli indirizzi personali (comparto e dirigenza) e un apposito spazio sull'intranet "bacheca sindacale" da utilizzarsi per le comunicazioni sindacali di competenza.
La disponibilità di tale spazio equivale alla messa a disposizione delle bacheche fisicamente disponibili all'interno della struttura istituzionale.

Le Organizzazioni Sindacali dovranno designare uno o più referenti delegati alla gestione della casella e della bacheca, i cui nominativi andranno comunicati alla Direzione tramite la casella istituzionale uo.rium@ats-brianza.it.

Le Organizzazioni Sindacali sono direttamente responsabili del contenuto sia delle comunicazioni inviate dalle caselle di cui sopra che di quelle affisse in bacheca.