Sistema Socio Sanitario
Regione Lombardia
ATS Val Padana

Cl.: 1.1.02

DECRETO n. 55 del 07/02/2020

OGGETTO: REGOLAMENTO DELL'AGENZIA DI TUTELA DELLA SALUTE DELLA VAL PADANA SULLA SICUREZZA INFORMATICA

IL DIRETTORE GENERALE – Dott. Salvatore Mannino

Acquisito il parere favorevole del
DIRETTORE AMMINISTRATIVO — Dott. Alessandro Cominelli

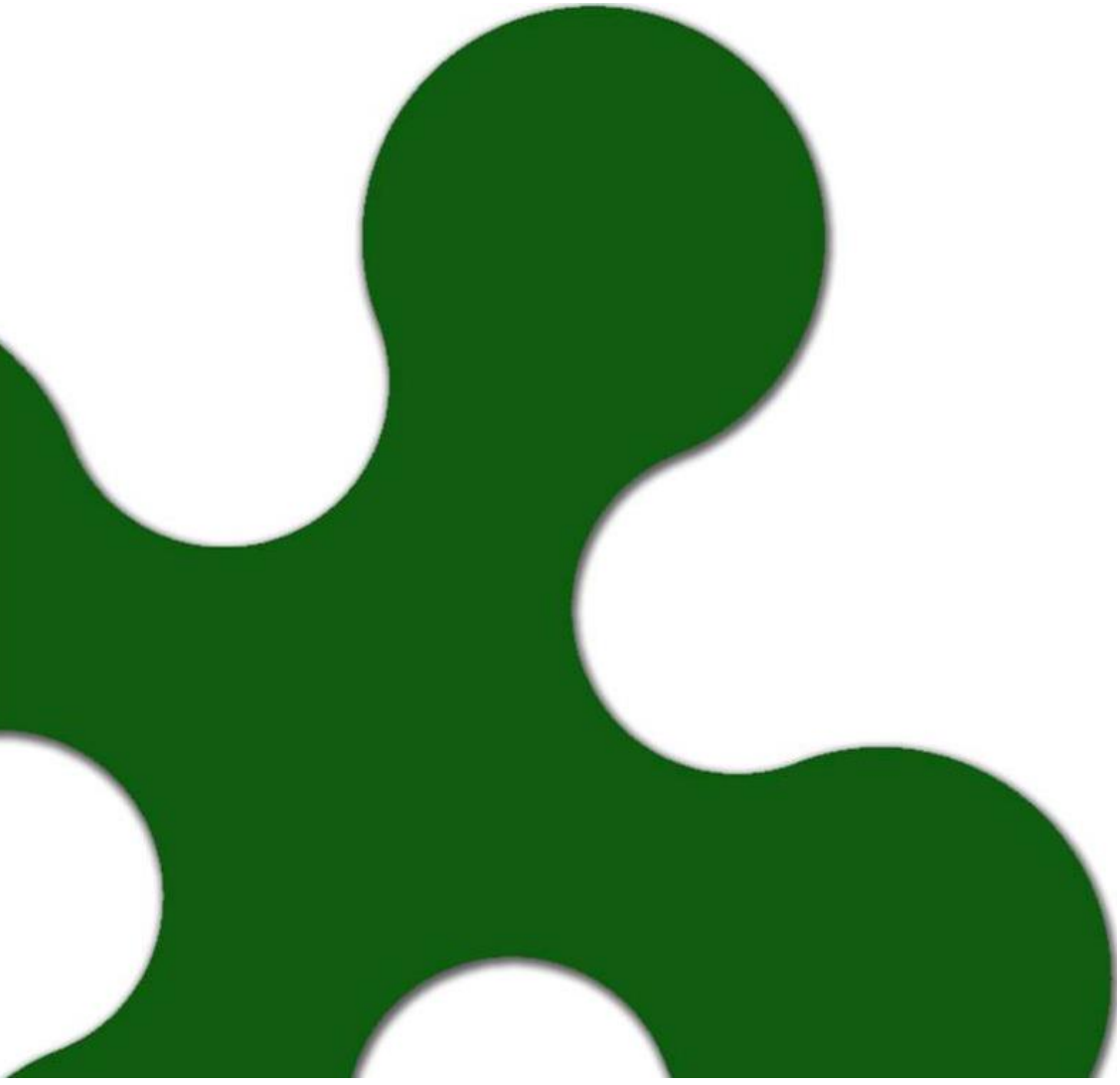
Acquisito il parere favorevole del
DIRETTORE SANITARIO — Dott.ssa Silvana Cirincione

Acquisito il parere favorevole del
DIRETTORE SOCIOSANITARIO — Dott.ssa Carolina Maffezzoni

Responsabile del procedimento: Dott. Ugo Boni

Manuale del Sistema di Gestione per la Qualità

Allegato
Regolamento sulla Sicurezza Informatica



Sistema Socio Sanitario
Regione Lombardia
ATS Val Padana

REGOLAMENTO DELL'AGENZIA DI TUTELA DELLA SALUTE DELLA VAL PADANA SULLA SICUREZZA INFORMATICA:

Norme per l'utilizzo della Posta Elettronica
Navigazione su Internet
Salvataggio dei dati

INDICE

Il presente allegato MQA0.12, redatto dal Responsabile dell'UOS Sistemi Informativi e DWH costituisce parte integrante del Manuale del Sistema di Gestione per la Qualità - MQ0 – dell'Agenzia di Tutela della Salute dell'ATS Val Padana.

Al Responsabile della Qualità dell'ATS Val Padana sono assegnate l'emissione, la conservazione e la distribuzione dello stesso.

LISTA DELLE APPROVAZIONI

data	Rev.	Approvazione (firma)
8/1/2020	02	Dott. Marco Villa

Capitolo 1. Utilizzo della dotazione informatica e sicurezza

Premessa

Il presente documento è redatto dalla "U.O.S. Sistemi Informativi e DWH" ed è periodicamente revisionato.

Il servizio ha il compito di assicurare il coordinamento tecnico della progettazione e della realizzazione dei sistemi informativi, telematici e di comunicazione interaziendale, sulla base di standard per i sistemi di hardware, software e reti conformi alle specifiche regionali e di sistema.

Il servizio esercita anche le funzioni di monitoraggio e controllo sull'utilizzo delle attrezzature informatiche aziendali rispetto alla sicurezza informatica, cui tutti i servizi aziendali sono comunque chiamati a collaborare.

Si ricorda che è in vigore il Regolamento Generale sulla protezione dei dati personali 679/2016 dell'Unione Europea (nel seguito GDPR) e che il Titolare del trattamento dati, nella persona del Direttore Generale pro tempore, è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza - limitazione della finalità - minimizzazione dei dati – esattezza- limitazione della conservazione - integrità - riservatezza e responsabilizzazione.

Dai principi del GDPR derivano una serie di obblighi in capo a chiunque utilizzi dati personali, non soltanto obblighi di riservatezza e segretezza ma anche di tutela, protezione e sicurezza dei dati.

I principi contenuti nel GDPR devono essere conosciuti e rispettati da chiunque tratti, nell'esercizio delle proprie funzioni, dati e informazioni personali e sensibili.

La dotazione informatica della ATS della Val Padana rappresenta un valore importante per il servizio da noi erogato e di conseguenza va utilizzata con cura.

Inoltre in essa sono custoditi dati personali (anche appartenenti a categorie particolari) che sono tutelati dalla legge.

La diffusione non autorizzata di tali dati costituisce PREMESSA per un'azione penale nei confronti della ATS della Val Padana e del dipendente che abbia eventualmente commesso il fatto.

Da questo consegue che un utilizzo che violi le presenti norme può causare, oltre ad un danno ai sistemi stessi, un'azione legale verso la ATS della Val Padana.

Si raccomanda quindi di attenersi scrupolosamente alle presenti norme e di segnalare ogni violazione o incidente al responsabile della sicurezza delle informazioni (sempre via email a sistemi.informativi@ats-valpadana.it).

Ruoli e Responsabilità	Per la conduzione del Sistema Informativo della ATS della Val Padana è stato identificato il Responsabile della Sicurezza delle Informazioni nella figura nel Responsabile dell'U.O.S. Sistemi Informativi e DWH. Egli si occupa di implementare le politiche aziendali relative alla fruizione e sviluppo della rete informatica aziendale, della manutenzione preventiva, degli interventi informatici e del supporto agli utenti e di tutte le problematiche attinenti al buon funzionamento del sistema. Tutti i dipendenti/collaboratori che utilizzano il Sistema Informatico dell'ATS della Val Padana sono tenuti ad osservare le norme contenute nel presente regolamento.
Accesso alla rete	1. Ogni utente del sistema ha un proprio account (nome utente a cui è associata una password) che lo identifica univocamente. 2. Ogni accesso ai PC dell'ATS deve essere fatto con il proprio account e non con account di altri. E' consentito l'utilizzo di accessi non nominali esclusivamente a computer determinati (es. sale riunioni). 3. Il Personal Computer connesso alla rete non deve essere lasciato incustodito (vedi anche punto 5). 4. Al termine del turno di lavoro è necessario disconnettersi (o spegnere il computer) salvo specifiche disposizioni della UOS Sistemi Informativi e DWH. Se un nuovo utente vi sostituirà alla postazione di lavoro dovrà identificarsi con il proprio nome utente e non continuare ad utilizzare il vostro. 5. Su ogni PC deve essere utilizzato il salvaschermo protetto da password (che sarà automaticamente la vostra password personale) ed impostato un tempo di attivazione di non più di 10 minuti. 6. Nel caso dei computer SISS l'accesso a determinati software/ambienti/portali è subordinato all'utilizzo della smart card operatore SISS e relativo PIN: l'uso di tali dispositivi di accesso è strettamente personale, le smart card SISS sono sempre nominali e non devono essere cedute ad altri.

Password	7. La password di accesso al computer è strettamente personale, scelta dall'utente, modificata trimestralmente alla scadenza e tenuta segreta in ogni situazione. 8. La password deve essere composta da almeno 8 caratteri, non essere uguale al nome, al cognome, a parole di uso comune sul luogo di lavoro e comunque non deve essere facilmente individuabile (nomi di figli, coniugi, città di residenza ecc. ecc.). 9. Le regole di composizione delle password prevedono che ciascuna password abbia almeno 3 delle seguenti caratteristiche: almeno una lettera maiuscola, almeno una lettera minuscola, almeno un numero, almeno un carattere speciale. 10. Non comunicare mai per nessuna ragione ad altri la propria password. Nel caso i tecnici dell'help desk accedano per verifiche tecniche o altro motivo di manutenzione, l'utente è invitato a cambiare la propria password al termine dell'intervento. 11. Le password relative agli account aziendali NON devono essere usate anche in riferimento a propri account non aziendali (esempio non usare la password dell'ATS anche per la posta elettronica di libero.it).
Antivirus	12. Il software antivirus deve essere sempre attivo su ogni Personal Computer (fisso o portatile) e deve essere aggiornato almeno settimanalmente per impedire contaminazioni e perdita di informazioni (in particolare i PC Portatili devono essere periodicamente collegati alla rete aziendale per consentire l'aggiornamento dell'antivirus). 13. L'utente non deve mai disattivare l'antivirus. 14. In caso di segnalazione della presenza di un virus in un file o messaggio di posta elettronica, o anche in caso di dubbio, il file ed il messaggio oggetto della segnalazione (e soprattutto gli eventuali allegati) non devono essere aperti o inviati ad altri utenti. Le segnalazioni a questo riguardo devono essere effettuate tempestivamente al Responsabile per la Sicurezza delle Informazioni (utilizzare sempre e comunque i canali previsti dal servizio di Fleet Management) e, solo in caso di pericolo immediato, anche ad eventuali colleghi che si apprestino a lavorare con lo stesso file o che potrebbero avere ricevuto la stessa email. Queste segnalazioni NON devono a loro volta contenere l'allegato o il link sospetto.

in Installazione di software	15. Sul Personal Computer fisso o portatile non devono essere installati dall'utente software diversi da quelli in dotazione alla ATS Val Padana (ed espressamente autorizzati in forma scritta via email dal Responsabile U.O.S. Sistemi Informativi e DWH). 16. In caso di particolari necessità contattare il Responsabile U.O.S. Sistemi Informativi e DWH che verificherà la fattibilità dell'installazione, l'integrazione con le applicazioni esistenti e la situazione delle licenze del software richiesto (l'acquisto delle eventuali licenze mancanti va comunque effettuato facendo richiesta secondo le procedure dell'agenzia in essere). 17. Qualora un programma installato dall'utente senza autorizzazione causasse danni al personal computer o alla rete aziendale i costi e le operazioni di sistemazione del danno verranno imputati all'utente stesso e potranno essere decise sanzioni disciplinari.
Installazione PC	18. I Personal Computer dovranno essere installati e configurati esclusivamente da personale della U.O.S. Sistemi Informativi e DWH o da un suo incaricato (ad esempio, personale del servizio Fleet Management). 19. Non è consentito modificare le configurazioni base impostate sul pc dall' U.O.S. Sistemi Informativi e DWH. 20. Non è possibile spostare in altro ufficio o scrivania un Personal Computer (esclusi ovviamente i PC portatili) senza autorizzazione. *Le richieste devono essere effettuate al servizio di Fleet Management secondo le modalità previste dallo stesso.*

Salvataggio dei dati	21. I dati e i documenti di lavoro importanti devono essere salvati esclusivamente nella cartella Documenti del computer o cartelle di rete dei server (cartelle condivise). 22. I dati salvati sul personal computer in cartelle diverse da Documenti (ad esempio sul desktop del computer) NON sono oggetto di operazioni di backup e sono quindi perduti in caso di guasto irrimediabile del disco fisso del PC. 23. In caso di guasto o rottura del proprio personal computer i dati dell'utente potrebbero andare persi causando danni al lavoro dello stesso o anche rischi penali e amministrativi per l'azienda (ad esempio nel caso di dati sensibili protetti dalla legge sulla privacy). 24. In caso di dubbi sulle operazioni di salvataggio o sui dischi da utilizzare per i propri documenti di lavoro effettuare una richiesta tramite le modalità previste dal servizio di Fleet Management (numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche). 25. Nessun file personale o non attinente alle attività della ATS dovrà essere salvato sui dischi di rete o sulla propria cartella Documenti (gli spazi e i meccanismi di backup non devono essere appesantiti da questa casistica). 26. In nessun caso si devono attivare condivisioni del disco del proprio personal computer con altri utenti per condividere documenti e informazioni in rete senza autorizzazione specifica del Responsabile U.O.S. Sistemi Informativi e DWH. 27. Per quanto concerne i documenti delle cosiddette Aree Comuni (cartelle condivise su server) si veda il paragrafo specifico.
Segnalazione di guasti o anomalie	28. Ogni guasto o anomalia deve essere comunicato tempestivamente tramite le modalità previste dal servizio di Fleet Management (numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche). 29. Ogni segnalazione deve essere il più possibile dettagliata e non generica. E' bene allegare ove possibile la schermata (screenshot) che mostra l'anomalia che si intende segnalare. 30. Quando i tecnici effettueranno gli interventi dovrà essere cura dell'utente fornire al personale tecnico tutte le informazioni per verificare la completa sistemazione del guasto segnalato. L'utente è tenuto a collaborare a queste operazioni fornendo la propria disponibilità e reperibilità in orari concordati

Pirateria Informatica e accessi non autorizzati	31. Ogni tentativo di connessione fraudolento al personal computer, al sistema di posta o ai dischi di lavoro di un altro utente (ove non espressamente autorizzati) cercando di ottenere la password dello stesso o anche utilizzando il Personal Computer incustodito è considerato attività illegale e punito dalla legge. 32. Nello stesso modo è vietato tentare di introdursi in sistemi di società o enti esterni alla ATS Val Padana se non espressamente autorizzati. 33. Queste operazioni di cui ai punti 31 e 32 precedenti, considerate attacchi informatici, sono punite dalla legge. Il dipendente verrà ritenuto responsabile e dovrà rispondere delle conseguenze.

Personal Computer Portatili	34. I Personal Computer portatili affidati ad un dipendente o collaboratore della ATS Val Padana sono sotto la diretta responsabilità dell'utente stesso che deve porre nell'uso tutta la cura atta a non causare danni al Personal Computer ed alle informazioni contenute in esso. 35. I Personal Computer portatili non devono essere lasciati incustoditi in auto o altrove per nessun motivo. 36. L'utilizzo delle connessioni ad internet dall'esterno della ATS Val Padana (ad esempio tramite WiFi domestico o smartphone aziendale usato come modem) deve essere fatto nel rispetto di tutte le norme di sicurezza qui esposte per evitare contaminazione da virus o altro software in grado di causare danni al sistema. 37. Il software antivirus deve sempre essere attivo ed aggiornato ad ogni connessione ad internet o alla rete della ATS Val Padana. 38. Il Personal Computer non può essere utilizzato da utenti diversi da quello/i a cui lo stesso è affidato salvo specifica autorizzazione da parte del Responsabile U.O.S. Sistemi Informativi e DWH. 39. È severamente vietato installare software, componenti aggiuntivi o hardware senza preventiva autorizzazione da parte del Responsabile U.O.S. Sistemi Informativi e DWH. 40. In caso di furto o smarrimento si deve effettuare tempestivamente la denuncia, informando il Responsabile U.O.S. Sistemi Informativi e DWH e al Responsabile UOC Approvvigionamenti. 41. I Personal Computer portatili devono essere collegati almeno una volta al mese alla rete aziendale per consentire l'aggiornamento delle misure di sicurezza (antivirus, aggiornamenti al sistema operativo…). 42. Non è consigliabile salvare dati sensibili sull'hard disk di computer portatili. Se nel Personal Computer portatile sono comunque custoditi dati sensibili o importanti occorre accordarsi con il Responsabile U.O.S. Sistemi Informativi e DWH per implementare un sistema di salvataggio dei dati.

Aree Comuni	43. L'azienda mette a disposizione ove necessario delle aree comuni (cartelle condivise), che sono aree in rete, fisicamente residenti su server centralizzati e visibili come dischi aggiuntivi o comunque accessibili da personale debitamente autorizzato. 44. La richiesta di creazione di una Area Comune deve avvenire in forma scritta da un responsabile di Servizio/Dipartimento tramite le modalità previste dal servizio di Fleet Management (numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche). La richiesta deve indicare esplicitamente nome e cognome delle persone che saranno autorizzate ad accedervi in lettura/scrittura. Non sono previste modalità diverse o diversi diritti di accesso. Sempre con la medesima modalità scritta devono essere richieste le variazioni delle persone autorizzate (aggiunta o eliminazione di accessi). Tutti gli utilizzatori devono essere consapevoli che, trattandosi di aree/cartelle comuni, le loro azioni (inserimenti, modifiche e soprattutto cancellazioni) si ripercuotono su tutti gli altri utilizzatori. 45. La U.O.S. Sistemi Informativi e DWH configura operazioni di backup delle aree comuni con periodicità di salvataggio almeno ogni 3 giorni. Non viene garantita profondità storica dei salvataggi.

Capitolo 2. Riservatezza e Privacy

Il Regolamento 679/2016/UE e il D.lgs. 196/2003, come novellato dal D.lgs. 101/2018, afferma che è onere del titolare del trattamento, ATS Val Padana, adottare le misure di sicurezza necessarie al fine di proteggere effettivamente i dati personali degli interessati secondo il principio di responsabilizzazione.

Definizioni	1. "**trattamento":** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. 2. **"dato personale**" **:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. 3. **"dati sensibili" :**dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Trattamento dei dati	4. La legge richiede che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. 5. **Principio di necessità nel trattamento dei dati:** Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Sicurezza	6. La ATS della Val Padana provvede ad effettuare un censimento periodico delle raccolte di dati personali che vengono trattati per lo svolgimento dei propri compiti istituzionali. Provvede inoltre a verificare sistematicamente che le misure di sicurezza, di natura fisica, logica od organizzativa, applicate a tutela dei dati stessi siano adeguate e riducano il rischio residuo ad un livello accettabile. 7. Parte integrante delle misure adottate ed in vigore presso la ATS della Val Padana sono quelle contenute nel presente regolamento. In particolare quelle relative all'uso di password, antivirus e copia di sicurezza dei dati. La loro violazione comporta quindi anche una violazione di legge della quale si può essere tenuti a rispondere. 8. Altre raccolte dati: qualora vengano create raccolte, archivi, Data Base, ecc. di dati personali o sensibili (anche e soprattutto in caso di immissione di tali dati su siti Web in ottemperanza di normative regionali o nazionali) del fatto va tempestivamente informato Il Responsabile della Sicurezza delle Informazioni (possibilmente prima dell'inizio del trattamento) che si farà carico di verificare il rispetto delle norme di sicurezza e di pianificare gli eventuali interventi di adeguamento. In mancanza di tale segnalazione la responsabilità di eventuali conseguenze (perdita, danneggiamento, utilizzo improprio, ecc.) rimane totalmente a carico di chi raccoglie e tratta i dati. 9. Ai sensi dell'articolo 33 e 34 del Regolamento 679/2016/UE, qualunque perdita, danneggiamento, furto, ecc. che determini violazione di dato personale degli interessati dovrà necessariamente essere fatta avviando segnalando la perdita via email a sistemi.informativi@ats-valpadana.it.

Capitolo 3. Uso di Internet e Posta Elettronica

Posta Elettronica

La posta elettronica è uno strumento fondamentale per le comunicazioni sia all'interno che all'esterno della ATS della Val Padana.

Come ogni altro strumento, il suo utilizzo può comportare dei rischi. Questo capitolo contiene le regole mirate a ridurre tali rischi sia per quanto riguarda le possibili responsabilità e conseguenze sugli utenti che per la protezione delle informazioni riservate o di natura proprietaria.

Il rispetto delle seguenti regole viene richiesto per tutti gli utilizzatori del sistema di posta elettronica (dipendenti, consulenti, lavoratori con contratto temporaneo, ecc.).

Autorizzazione	1. I sistemi di comunicazione elettronici, tra i quali la posta elettronica, possono, in generale, essere utilizzati esclusivamente per attività legate alla ATS della Val Padana. 2. Non sono consentiti utilizzi per attività professionali personali, divertimento, intrattenimento o qualunque altra finalità non consona alla pubblica immagine della ATS della Val Padana.

Identificativo	3. Ad ogni dipendente è assegnata una casella di posta (sono inoltre definite caselle di posta elettronica "di servizio" o "per argomento" anche in forma condivisa con altri utenti, ma il cui accesso è comunque subordinato all'appartenenza ad un gruppo specifico legato alla attività di ciascuno). La password relativa alla casella non deve essere condivisa fra più persone né rivelata a terzi. Gli utenti possono cambiare autonomamente la password della propria casella (modificando la password di accesso al PC, che è sincronizzata con quella della posta). In caso di dimenticanza della password gli addetti U.O.S Sistemi Informativi e DWH (o loro incaricati) re-impostano la password ed invitano l'assegnatario a modificarla al primo accesso successivo. Ciascun assegnatario di una casella di posta elettronica è tenuto a consultare i messaggi in arrivo con regolarità, sulla base della organizzazione data dal Responsabile del servizio di appartenenza. 4. Non è consentito nascondere o modificare l'identità dell'utente. Il nome utente, l'indirizzo di posta elettronica, l'organizzazione di appartenenza e le relative informazioni incluse nei messaggi e specificate tramite le Preferenze/Opzioni di ciascuna casella devono riflettere l'effettiva identità di chi ha originato il messaggio. 5. Al personale esterno non può essere assegnato un nome utente per l'utilizzo della posta elettronica che lo identifichi come dipendente della ATS Val Padana. Nel caso di collaboratori esterni temporaneamente in forza all'ATS (contratti temporanei, borsisti, …) è possibile l'assegnazione agli stessi di una casella di posta elettronica personale. La firma dei messaggi da essi inviati deve in questo caso obbligatoriamente indicare il mittente con lo specifico ruolo (es. borsista assegnato al Servizio). Parimenti nel caso di personale ATS cessato oppure in comando ad altro ente l'utenza di posta elettronica è bloccata salvo diverse indicazioni della Direzione. 6. La casella di posta elettronica ATS assegnata NON deve essere utilizzata in fase di registrazione a portali non istituzionali.

Protezione	7. Gli utenti devono tenere presente che tutti i messaggi di posta elettronica usuali, anche quelli destinati ad altri operatori dell'ATS, viaggiano tramite rete pubblica. Pertanto, per inviare informazioni sensibili o comunque riservate e non di pubblico dominio è necessario utilizzare tecniche di cifratura od equivalenti (ad esempio con allegati firmati e criptati, formato *.p7m.p7e*, tramite l'utilizzo della carta SISS operatore e del software DigitalSign). Nel caso di comunicazioni interne ad ATS si suggerisce di optare per l'utilizzo di cartelle di rete condivise ai fini della trasmissione/condivisione di dati personali/sensibili. 8. Il messaggio deve, nel caso, indicare la natura delle informazioni in esso contenute (riservate, sensibili, personali, ecc). 9. Si ricorda che non viene fornita alcuna garanzia che i messaggi rimangano riservati: le comunicazioni elettroniche, per la natura stessa della tecnologia, possono essere inoltrate a persone diverse, intercettate, stampate e conservate da altri.
Privacy e riservatezza	10. I contenuti delle comunicazioni e l'utilizzo dei sistemi comunicativi possono essere controllati, in caso di necessità, per effettuare e supportare attività operative, di manutenzione, auditing, sicurezza, investigative, statistiche e quant'altro previsto da norme legislative. Agli utenti viene richiesto di tenerne in debito conto nell'utilizzo della posta elettronica. 11. Il contenuto di messaggi di posta elettronica può, nel corso di attività rivolte alla soluzione di problemi tecnici, essere visto dal personale tecnico di supporto. L'eventuale accesso avviene in maniera controllata, limitato allo stretto necessario. Allo stesso personale è esplicitamente vietato accedere al contenuto di un messaggio per semplice curiosità o su richieste non debitamente autorizzate.

Contenuto del messaggio	12. Non si possono fare commenti osceni, imprecazioni o denigrazioni nei messaggi di posta elettronica scambiati con colleghi, clienti, fornitori di beni e servizi o altri. 13. Molestie sessuali, etniche e razziali attraverso la posta elettronica sono severamente proibite e possono essere causa di sanzioni disciplinari. 14. Si scoraggiano gli utenti dal rispondere ai messaggi offensivi, promozionali o in genere a messaggi spam (messaggi di carattere generico, commerciale, catene di Sant'Antonio o contenenti materiale pornografico inviati a milioni di utenti con l'obiettivo di raccogliere indirizzi e-mail e nominativi). Nei casi più gravi, è opportuno informare il Responsabile U.O.S. Sistemi Informativi e DWH. 15. Nessuna informazione sensibile può essere inoltrata all'esterno della ATS della Val Padana se non dopo approvazione della Direzione o comunque sulla base di specifica normativa relativa. 16. Qualora si ricevano messaggi di posta elettronica non desiderati o sollecitati (non pertinenti all'attività istituzionale) ci si deve astenere dal rispondere direttamente al mittente.
Destinatari del messaggio	17. È necessario prestare attenzione quando si inoltrano messaggi, assicurandosi che i destinatari siano effettivamente coloro cui si intende inviare l'informazione.

Virus e allegati	18. Se si sospetta la presenza di virus informare immediatamente i Sistemi Informativi tramite le modalità previste dal servizio di Fleet Management (numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche). Tutti gli utenti di posta elettronica sono tenuti a diffidare dei messaggi provenienti da mittenti sconosciuti o dubbi, o contenenti comunicazioni allettanti, Nel caso di dubbi tutti gli utenti sono invitati a **NON aprire gli eventuali allegati**, a **evitare di cliccare su link contenuti all'interno del messaggio** e a richiedere un parere preventivo ai U.O.S. Sistemi Informativi e DWH tramite le modalità previste dal servizio di Fleet Management (numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche) , evitando di inoltrare il messaggio sospetto nell'apertura della segnalazione. 19. E' vietato inviare e allegare a messaggi di posta virus, trojan o altri programmi che possano danneggiare i sistemi del destinatario del messaggio. 20. E' vietato inviare o allegare software o file protetti da copyright e legge sul diritto d'autore (musica, video, immagini e altro). 21. E' necessario limitare l'utilizzo della posta elettronica per trasferire allegati di grosse dimensioni se non espressamente richiesto e per motivazioni importanti (si consiglia di comprimere gli allegati tramite l'apposito software Winzip, 7zip o WinRar nel caso di allegati superiori a 4Mb). Nel caso il sistema blocchi comunque il messaggio a causa della sua dimensione (oltre i 20Mb) contattare l'help desk tramite le modalità previste dal servizio di Fleet Management (numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche). 22. Attualmente tutti file che potrebbero essere veicolo di virus vengono automaticamente bloccati dal sistema (come per esempio file con estensione *.bat, *.avi, *.cmd, *.com, *.dll, *.drv, *.exe, *.scr…..) e sono scaricabili solo previa autorizzazione del Responsabile U.O.S. Sistemi Informativi e DWH.

Internet

Internet offre un insieme di servizi e possibilità di interconnessione che costituiscono importanti opportunità, ma presentano anche una nuova serie di rischi. In questo capitolo verranno indicate le regole minime da adottare per ridurre i rischi entro un limite considerato accettabile.
Il rispetto di queste regole è richiesto a tutti coloro che, indipendentemente dalla organizzazione di appartenenza (impiegati, consulenti, impiegati a tempo determinato, borsisti, ecc.) si connettono a Internet utilizzando reti o sistemi della ATS della Val Padana.

Autorizzazione	1. L'utilizzo di Internet è consentito per scopi di servizio (in ogni caso la U.O.S. Sistemi Informativi e DWH configura tramite apposite politiche sul firewall aziendale le categorie di siti accessibili o inaccessibili, vedi paragrafo relativo al Controllo Accessi).
Integrità dell'informazione	2. Tutte le informazioni scaricate da Internet devono considerarsi dubbie finché non vengono confermate da informazioni ricavate da altre fonti. Non esiste una procedura di controllo di qualità su Internet e un numero considerevole di informazioni sono datate, imprecise ed, in alcuni casi, deliberatamente errate. Quindi, prima di utilizzare informazioni attinte da Internet per decisioni riguardanti il proprio lavoro, le stesse vanno quanto meno confermate consultando altre fonti. 3. Tutti i file che non siano in formato testo (DataBase, Programmi eseguibili, Fogli di calcolo, Documenti Word, ecc.) scaricati da qualunque fonte di Internet devono essere controllati con programmi antivirus prima di essere utilizzati. Il programma antivirus li controllerà automaticamente e di conseguenza non deve mai e per nessun motivo essere disattivato. In ogni caso tutti gli utenti sono tenuti a chiedere autorizzazione scritta alla U.O.S. Sistemi Informativi e DWH (tramite le modalità previste dal servizio di Fleet Management - numero verde 800.811.193 oppure email a hdatsvalpadana@bcs.it – riferimento procedura PP1.19.2 Assistenza e Richieste Informatiche) prima di utilizzare programmi scaricati via Internet.

Rapporti con l'esterno	4. L'appartenenza dell'utente alla ATS della Val Padana può essere indicata in mailing list, sessioni chat, ecc solo nei casi in cui sia in diretta relazione con il proprio lavoro o ricerca scientifica. In tutti i casi deve essere precisato chiaramente che le opinioni espresse sono proprie e non rappresentano necessariamente quelle della ATS della Val Padana. L'approvazione di prodotti/servizi effettuata tramite Internet è vietata senza la preventiva autorizzazione del superiore diretto. 5. In nessuna circostanza possono essere inviati messaggi che rientrano nelle seguenti categorie: dichiarazioni politiche o religiose, imprecazioni o linguaggio scurrile, dichiarazioni dirette a offendere altri, specie a causa della razza, colore, credo, età, sesso, handicap od orientamento sessuale. 6. L'utilizzo di programmi di chat, video-audio conferenze e/o instant-messaging è consentito esclusivamente per fini aziendali.
Copyrights	7. È proibito scaricare o inviare su Internet software in difformità dalla licenza del venditore. La riproduzione o distribuzione di materiale devono essere effettuati esclusivamente con il consenso dell'autore. 8. Il materiale su Internet è protetto da copyright salvo diversa indicazione. Quando si utilizzano informazioni ricavate da Internet è necessario includere, nel caso, la formula 'copyright, tutti i diritti riservati' indicando la fonte dell'informazione (nome dell'autore, URL, …).

Controllo accessi	9. Non si possono attivare connessioni di rete verso l'esterno via internet o altri sistemi che non siano autorizzati. In particolare è espressamente vietato l'utilizzo di modem (o equivalenti) interni o esterni (i computer portatili, quando non connessi alla rete aziendale, possono accedere ad Internet solo con apposite chiavette aziendali o altro dispositivo munito di SIM). 10. Può essere bloccato l'accesso a siti sicuramente non attinenti a finalità di lavoro, che stimolino comportamenti contro la morale o che causino elevato traffico per finalità ludiche o di intrattenimento. A questo scopo può essere effettuato un monitoraggio dei siti maggiormente frequentati e, nel caso si rilevino anomalie, l'accesso ad alcuni siti può venir limitato e/o consentito solo ad utenti autorizzati. 11. Qualora ci si connetta erroneamente a siti con contenuti sessuali, razzisti, violenti o altro materiale potenzialmente offensivo o contro la morale è necessario disconnettersi immediatamente.
Privacy e Internet	12. Le comunicazioni non sono automaticamente protette e possono essere lette da altri. A meno che non vengano utilizzate tecniche di cifratura, non è opportuno inviare informazioni riservate su internet.
Segnalazioni di problemi di sicurezza	13. Qualora informazioni sensibili della ATS della Val Padana siano state perse, rivelate a soggetti non autorizzati (o vi è solo il sospetto), è necessario notificarlo immediatamente al Responsabile della Sicurezza delle Informazioni (tramite email a sistemi.informativi@ats-valpadana.it). 14. Qualora password, smart card o altri meccanismi di accesso (ad esempio a portali su Internet) siano persi, rubati o rivelati (o vi è solo il sospetto), è necessario notificarlo immediatamente al Responsabile della Sicurezza delle Informazioni (tramite email a sistemi.informativi@ats-valpadana.it).

Capitolo 4. Utilizzo di sistemi aziendali per usi personali

Premessa	1. Il personal computer fisso o portatile è uno strumento aziendale concesso in uso al dipendente (o collaboratore) esclusivamente per finalità legate alla propria attività lavorativa. 2. Per brevi periodi, senza che questo infici l'operatività del servizio di appartenenza) è consentito l'utilizzo del Personal Computer aziendale per scopi personali a patto che vengano rispettate le norme di comportamento del presente regolamento ed in particolare quelle che seguono. 3. Rimangono comunque in vigore, nel caso di utilizzo per usi personali, tutte le norme precedenti anche se non comprese nella presente sezione.
Autorizzazione	4. E' necessario informare il Responsabile della U.O.S. Sistemi Informativi e DWH dell'utilizzo del Personal Computer per scopi personali (via email a sistemi.informativi@ats-valpadana.it). Questi valuterà rischi e modalità di utilizzo per prevenire danni al Personal Computer stesso ed alla rete della ATS della Val Padana.
Antivirus	5. L'utilizzo ed il trasporto di file da altri sistemi al Personal Computer della ATS della Val Padana deve essere fatto nel rispetto delle norme antivirus e di quant'altro previsto dal presente regolamento. 6. Se un file viene trasportato su un dispositivi rimuovibile (es. chiavetta USB) è bene controllare tale dispositivo prima di caricare o eseguire i file ivi contenuti (tramite l'opzione di "scansione alla ricerca di virus" del software antivirus, attivabile da Risorse del Computer, cliccando con il tasto desto del mouse sullo specifico dispositivo o comunque contattando la U.O.S. Sistemi Informativi e DWH in caso di dubbi).
Utilizzo del Software	7. I file personali possono essere elaborati esclusivamente con i software in dotazione alla ATS della Val Padana. 8. In nessun caso possono essere installati programmi aggiuntivi per uso personale non correlato alle attività aziendali.

Connessione ad altri sistemi	9. In nessun caso è possibile collegarsi per scopi personali a sistemi all'esterno della ATS della Val Padana per caricare o salvare file attraverso l'utilizzo di sistemi FTP, VPN, file sharing o altro senza preventivo consenso del Responsabile della U.O.S. Sistemi Informativi e DWH.
Personal Computer Portatili e supporti rimovibili	10. Per i Personal Computer portatili valgono le stesse regole dei Personal Computer fissi presenti all'interno della ATS della Val Padana. 11. Inoltre cura particolare va posta nell'utilizzo dei Personal Computer portatili e dei supporti rimovibili (ad esempio chiavette USB) per evitare che le informazioni in essi contenute vadano perse o siano comunicate a terzi non autorizzati. 12. Non è consentito prestare a terzi anche temporaneamente i Personal Computer portatili, ma possono essere utilizzati solo dall'utente a cui sono affidati. 13. I tecnici (addetti della U.O.S. Sistemi Informativi e DWH o loro incaricati) sono tenuti a rimuovere ogni programma installato diverso da quelli in dotazione alla ATS della Val Padana ed a segnalare il fatto al Responsabile della U.O.S. Sistemi Informativi e DWH.
Gestione dei File	14. Non è consentito effettuare copie di salvataggio di file personali sui computer della ATS della Val Padana. 15. Gli eventuali file personali devono stare sul disco C del proprio Personal Computer in una cartella che li identifichi chiaramente (es: cartella <FILE PERSONALI NOME UTENTE>) per evitare che siano cancellati durante le operazioni di manutenzione. 16. La ATS della Val Padana non garantisce in alcuno modo la riservatezza, la disponibilità e l'integrità dei file personali degli utenti. Essi non sono oggetto di backup.

IL DIRETTORE GENERALE

Richiamati:
- il Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (d'ora innanzi GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- il D.Lgs. 30 giugno 2003, n. 196, cosi come modificato dal D.Lgs. 10 Agosto 2018, n. 101: "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e che abroga la direttiva 95/46/CE";

Ricordata la necessità di regolamentare l'utilizzo degli strumenti informatici e, in particolare, quello della posta elettronica e di Internet;

Ravvisata l'opportunità di procedere ad una revisione del Regolamento sulla Sicurezza Informatica per dare uniforme applicazione agli analoghi regolamenti precedentemente in uso nelle aziende Asl delle province di Cremona e di Mantova, adottando l'allegato "Regolamento dell'Agenzia di Tutela della Salute della Val Padana sulla sicurezza informatica", parte integrante del presente provvedimento;

Dato atto che dal presente provvedimento non discendono oneri per l'Agenzia;

Vista l'attestazione del responsabile del procedimento amministrativo dott. Ugo Boni e del Direttore dell'UOC Sistemi Informativi e Controllo Direzionale dott. Marco Villa in ordine alla regolarità tecnica ed alla legittimità del presente atto;

Acquisiti i pareri favorevoli del Direttore Amministrativo, Sanitario e Sociosanitario;

D E C R E T A

1. di approvare l'allegato "Regolamento dell'Agenzia di Tutela della Salute della Val Padana sulla sicurezza informatica", parte integrante del presente provvedimento;

2. di dare atto che dal presente provvedimento non discendono oneri per l'Agenzia;

3. di disporre, a cura dell'U.O.C. Affari Generali, Legali e Istituzionali, la pubblicazione all'Albo on-line ai sensi dell'art. 32 della L. 69/2009 e nel rispetto del Regolamento UE 679/2016.

Firmato digitalmente
Dott. Salvatore Mannino