Sistema Socio Sanitario
Regione Lombardia
ATS Pavia

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI E STRUMENTI INFORMATICI DELL'ATS DI PAVIA

REG SIA 01

(Approvato con Decreto n. 671/DGi del 19/09/2024)

Preparato	Responsabile SC Sistemi Informativi
Verificato	Direttore Amministrativo
Approvato	Direttore Generale
Identificato ed editato	Responsabile Qualità Aziendale

Rev.	Descrizione modifica	Data di applicazione
1	Aggiunge alla prima emissione del regolamento (approvato con decreto n. 189/DGi del 14.03.2024): Rischio: trasmissione non autorizzata di indirizzi di posta elettronica a soggetti terzi	Data di approvazione del decreto

SOMMARIO

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete Internet da personal computer, tablet e smartphone, espone il Datore di Lavoro ed i suoi dipendenti e collaboratori a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy fra tutte), creando inoltre evidenti problemi alla sicurezza informatica con conseguente danno all'immagine dell'ATS di Pavia.

Il presente Regolamento contiene le istruzioni relative alle modalità ed ai doveri che ciascun dipendente e collaboratore deve osservare nell'utilizzo di computer fissi, computer portatili, telefoni fissi, telefoni cellulari, tablet, smartphone, connessione internet, server per archiviazione file, posta elettronica, servizi applicativi, dati, (di seguito in breve: "risorse informatiche"), messi a disposizione dal Datore di Lavoro nell'ottica di uno svolgimento proficuo e più agevole dell'attività lavorativa.

Le istruzioni di seguito indicate si aggiungono ed integrano anche le specifiche istruzioni fornite a tutti gli Autorizzati, in attuazione del Regolamento Europeo sulla protezione dei dati (di seguito GDPR 2016/679) e del D.Lgs 196/2003 e s.m.i. come meglio precisato nel Modello Organizzativo Privacy approvato da questa ATS con Decreto n. 252/GDi del 04/04/2023.

Definizioni

Ai fini del presente Regolamento si intende per:

Backup: duplicazione di file o di un insieme di dati su un supporto esterno al sistema, per avere una copia di riserva di tali dati.

Data Breach: "violazione dei dati personali", la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dato Personale: sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

Download: "scaricamento", indica l'azione di ricevere da una rete telematica, come un sito web, un file che viene poi trasferito sul disco rigido del computer o su un'altra unità periferica dell'utente.

File di log: rappresentano la registrazione sequenziale e cronologica delle operazioni effettuate su un sistema informatico. Tramite i file di log vengono quindi registrati diversi eventi, come ad esempio l'accesso (login) e l'uscita (logout) da un sistema.

File Server: è uno spazio di lavoro e di archiviazione centralizzato soggetto a tutte le misure di sicurezza atte ad evitare perdite di dati posizionato in locale attrezzato con sistema antincendio e sistema antintrusione.

Firewall: dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi.

GDPR: Regolamento Generale Protezione Dati Personali - Regolamento (UE) n. 2016/679, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018.

Hard Disk: "disco rigido" o "disco fisso" è il dispositivo utilizzato per memorizzare i dati sul Personal Computer (dal Sistema Operativo ad ogni altro tipo di file). Se è di tipo USB trattasi di disco esterno collegabile al Personal Computer tramite porta USB.

Indirizzo IP: "Indirizzo Internet Protocol" è costituito da una serie di numeri assegnata a ogni dispositivo connesso a una rete di computer. L'indirizzo IP è l'identificativo univoco della PdL all'interno della rete.

LDAP: "Lightweight Directory Access Protocol" è un protocollo di autenticazione che permette l'accesso alle risorse informatiche.

Link: "collegamento", solitamente quando viene cliccato un link si viene rinviati ad un'altra pagina web o a un file da scaricare.

Malware: "malicious software" o "software dannoso", indica un qualsiasi programma informatico che agisca contro l'interesse dell'utente. Oltre alla PdL infetta, il malware può colpire anche tutti i dispositivi con cui questa comunica.

Password: parola o sigla di riconoscimento fornita dall'utente per poter accedere a un sistema operativo, a un programma o a un file.

Password Policy: procedura che stabilisce i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite agli utenti per l'accesso alle risorse informatiche.

PdL: "Postazione di Lavoro" informatica, può essere fissa (PC + monitor), portatile (PC portatile + monitor + docking station), virtuale (residente su server e raggiungibile da PdL fissa o portatile).

PIN: codice numerico di protezione, serve per proteggere l'accesso ad alcune risorse (es.: cellulare, pc).

Ransomware: programma informatico dannoso che può infettare un dispositivo digitale (PC, tablet, smartphone, ecc.) bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese "ransom") da pagare per permetterne il riutilizzo.

SFTP: software per la trasmissione sicura di File.

SIM: scheda che viene inserita all'interno di un telefono cellulare/smartphone o tablet. È dotata di un codice identificativo univoco, che permette all'operatore di identificare il cliente e di conseguenza il numero di telefono a cui è stato associato.

Smartphone: "telefono intelligente", unisce alle caratteristiche di un telefono cellulare le potenzialità di un piccolo computer, grazie alla presenza di un sistema operativo completo e autonomo.

Spyware: qualunque software dannoso che infetta PC e dispositivi mobili al fine di raccogliere informazioni sugli utenti e dati sulle abitudini di navigazione, l'utilizzo di internet, ecc.

Tablet: computer portatile di dimensioni ridotte, sul cui schermo è possibile scrivere o impartire comandi col tocco delle dita o mediante un apposito stilo.

Token: dispositivo hardware per la generazione di codici di sicurezza

Username: "nome utente" è il nome con il quale l'utente viene riconosciuto da un computer, da un programma o da un server. Per ottenere un'identificazione univoca da parte del sistema a cui si richiede l'accesso al nome utente viene associata una password.

Virus: applicazione o codice utilizzato per attività malevole su dispositivi o reti locali. Esso può danneggiare i file locali e sulle cartelle di rete connesse, rubare dati, interrompere servizi, scaricare malware, o effettuare qualsiasi altra azione per cui è stato sviluppato.

Windows Update: servizio di aggiornamento software per i sistemi operativi Microsoft Windows. Offre gli aggiornamenti per tutte le componenti del sistema operativo installato sulle PdL, correggendo anche eventuali problemi di sicurezza che vengono via via scoperti.

Art. 1. Oggetto e finalità

1.1 Il presente Regolamento disciplina le modalità di utilizzo delle risorse informatiche che l'ATS di Pavia mette a disposizione del proprio personale dipendente e dei collaboratori per l'esercizio delle funzioni istituzionali di competenza, non solo all'interno dei locali dell'ATS, ma anche in modalità remota o agile (smart working).

1.2 Il presente Regolamento è redatto ai sensi:

a) della legge n. 300/1970 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
b) della Direttiva del 26 maggio 2009 n. 2 del Ministero per la Pubblica Amministrazione e l'Innovazione recante "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro";
c) del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007, recante "Lavoro: le linee guida del Garante per posta elettronica e Internet";
d) della Raccomandazione CM/Rec (2015) del Comitato dei Ministri degli Stati Membri sul trattamento dei dati personali nel contesto occupazionale;
e) del Regolamento UE n. 2016/679
f) del D.Lgs n. 196/2003 e s.m.i. come modificato dal D.Lgs 101/2018 "Codice in materia di protezione dei dati personali"
g) del Codice di comportamento dell'ATS di Pavia.
h) delle misure minime di sicurezza ICT per le P.A. – Circolare AGID n. 2 del 18/04/2017

1.3 Scopo del Regolamento è la tutela dei beni di proprietà dell'ATS di Pavia, consegnati in uso ai propri dipendenti/collaboratori e garantire il corretto utilizzo delle risorse informatiche a tutela della riservatezza dei dati trattati e della sicurezza informatica. Il tutto al fine di evitare che condotte inconsapevoli e/o scorrette possano esporre l'ATS di Pavia a rischi connessi con la sicurezza informatica, danni patrimoniali o di immagine.

Art. 2. Campo di applicazione

2.1 Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i consulenti, fornitori e collaboratori, a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es.: lavoratori somministrati, collaboratori coordinati e continuativi, stagisti, borsisti, tirocinanti, specializzandi, ecc.) autorizzati ad utilizzare le risorse informatiche dell'ATS di Pavia e ad accedere a dati e informazioni ivi conservati e trattati. Gli utilizzatori sopra citati verranno indicati di seguito come "utente".

2.2 È obbligo dei Responsabili di Struttura informare tutti gli utenti afferenti a qualsiasi titolo alla propria Struttura sui contenuti del presente Regolamento e monitorarne con continuità l'applicazione. Si precisa, inoltre, che il Regolamento si applica anche a dipendenti e collaboratori in Telelavoro o Lavoro agile.

Art. 3. Responsabilità personale dell'utente

3.1 Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'ente, nonché dei relativi dati trattati.

3.2 A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con il Datore di lavoro e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale da utilizzi impropri o non autorizzati, danni o

abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse dell'Agenzia.

3.3 Ogni utente è tenuto a operare a tutela della sicurezza informatica aziendale, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero inosservanza del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente.

3.4 L'utente deve in particolare rispettare scrupolosamente quanto riportati in Allegato 1 - Indicazioni specifiche per la Sicurezza Informatica.

Art. 4. Tutela del lavoratore

4.1 Nel rispetto dei principi di pertinenza e di non eccedenza, il Datore di Lavoro, per il tramite del personale incaricato dei SIA, può effettuare controlli anonimi sull'utilizzo degli strumenti informatici aziendali.
Il controllo potrà scaturire:

a) dalla necessità di dovere effettuare verifiche sulla funzionalità e sicurezza del sistema;
b) dal rilevamento di anomalie nell'utilizzo della rete aziendale e/o accesso e uso di Internet.

Il controllo derivante da anomalie rilevate sarà svolto, in via preliminare, su dati aggregati e si concluderà con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite**.**

4.2 Il Datore di lavoro agirà sempre in base al principio della gradualità. In attuazione di tale principio:

a) i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
b) nel caso in cui si dovessero riscontrare violazioni del presente regolamento verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici dell'Agenzia, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;

Art. 5. Assegnazione e gestione delle Credenziali di accesso alle Risorse Informatiche

5.1 Le credenziali di accesso alle risorse informatiche (pc, rete, file server, applicativi, ecc.) sono sempre composte da un codice per l'identificazione dell'utente (username o nome utente) e da una parola chiave (password). Il nome utente viene assegnato dai Sistemi Informativi Aziendali (di seguito "SIA") abbinato ad una password di primo accesso che ogni utente dovrà modificare quanto prima (rispettando i criteri della Password Policy, vedi punto seguente), custodire con la massima diligenza e riservatezza e non divulgare. Per tutti gli utenti vale il divieto assoluto di memorizzare qualsiasi credenziale assegnata su qualsiasi apparecchiatura informatica utilizzata (aziendale o personale). Vale, altresì, il divieto assoluto di utilizzare credenziali aziendali per applicazioni o portali non aziendali (es. casella mail personale, social network, portali e-commerce, ecc.).

5.2 Tutte le password utilizzate per accedere alle risorse informatiche di ATS Pavia devono rispettare i seguenti requisiti minimi:

a) lunghezza minima: 14 caratteri
b) deve contenere almeno un carattere alfabetico minuscolo (a-z)

c) deve contenere almeno un carattere alfabetico maiuscolo (A-Z)
d) deve contenere almeno una cifra decimale (0-9)

e) deve contenere almeno un carattere speciale (! $ _ # ecc.)
f) non deve contenere riferimenti a nome o cognome
g) non deve contenere il nome utente

5.3 Si precisa che, dove possibile, i sistemi verificano in automatico l'applicazione in tutto o in parte della policy. In ogni caso è responsabilità dell'utente rispettarla. È altresì, responsabilità dell'utente modificare prima possibile le password di primo accesso fornite dai SIA (anche nei casi dove i sistemi non forzano questa scelta). Successivamente le password vanno modificate almeno ogni sei mesi.

5.4 Le credenziali di accesso sono classificate secondo le seguenti tipologie:

a) **Credenziali di autenticazione LDAP**: permettono l'accesso alla rete e a vari applicativi/servizi dell'ATS di Pavia (i SIA consegnano all'utente un modulo con indicate le credenziali, le istruzioni per la modifica della password di primo accesso e l'elenco degli applicativi accessibili con queste credenziali).
b) **Credenziali di accesso alle PdL:** permettono l'accesso al Sistema Operativo installato sui pc (fissi o portatili) e sulle macchine virtuali (i SIA consegnano all'utente un modulo con indicate le credenziali, le istruzioni per la modifica della password di primo accesso e le istruzioni relative agli aggiornamenti del Sistema Operativo).
c) **Credenziali File Server:** permettono l'accesso alle cartelle di rete sul file server aziendale (i SIA inviano le credenziali parziali tramite e-mail). La password non è modificabile direttamente dall'utente. In caso di necessità la modifica va richiesta ai SIA.
d) **Credenziali applicativi aziendali:** permettono l'accesso agli applicativi/servizi non accessibili tramite l'autenticazione LDAP (i SIA inviano le credenziali tramite comunicazioni specifiche per l'applicativo/servizio interessato).

5.5 Le credenziali di accesso alle risorse informatiche vengono assegnate dai SIA previa formale richiesta del Responsabile di Struttura nell'ambito della quale verrà inserito ed andrà ad operare ogni nuovo utente, con mail indirizzata alla casella ced@ats-pavia.it. Prima di predisporre le credenziali richieste i SIA verificano che vi sia corrispondenza con la lettera di nomina ad autorizzato al trattamento sottoscritta dall'utente. Le credenziali di accesso alle risorse informatiche di un utente vengono disattivate dai SIA alla cessazione del rapporto di lavoro su notifica della SC Gestione e sviluppo delle risorse umane. È altresì compito del medesimo Responsabile di Struttura richiedere ai SIA la revoca delle credenziali, con mail indirizzata alla casella ced@ats-pavia.it, in caso di utente trasferito, assenza prolungata o modifica delle autorizzazioni assegnate all'utente.

5.6 Per motivi di sicurezza informatica è facoltà del personale incaricato dei SIA procedere al reset delle password sopra citate dandone puntuale comunicazione all'utente.

5.7 È responsabilità di ogni utente utilizzare esclusivamente le proprie credenziali e non cederle ad altri utenti.

5.8 Le password potenzialmente compromesse, violate, rubate o impropriamente diffuse, anche in caso di dubbio, vanno immediatamente modificate dall'utente interessato. Inoltre la violazione va segnalata ai SIA nonché al Responsabile di Struttura.

5.9 Per l'accesso ad alcuni servizi applicativi è necessario utilizzare l'Autenticazione Multifattoriale (MFA Multi Factor Authentication) e cioè con trasmissione di un codice di sicurezza via Token, e-Mail o via SMS su telefono cellulare.

Art. 6. Utilizzo della Postazione di Lavoro Informatica

6.1 La Postazione di Lavoro Informatica (di seguito PdL) può essere:

a) fissa (pc + monitor posizionati su scrivania)
b) portatile (utilizzabile in modalità "stand-alone" oppure connessa con chiave di sicurezza ad una docking station a sua volta vincolata con cavo di sicurezza alla scrivania)
c) virtuale (residente su sistema server centralizzato e accessibile tramite collegamento da una PdL fissa o portatile)

La PdL (fissa, portatile o virtuale) è univocamente assegnata all'utente su richiesta del Responsabile di Struttura. L'utente sottoscrive il verbale di consegna e conseguentemente ne assume la responsabilità fino alla riconsegna ai SIA.
La PdL è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è in generale vietato perché può contribuire ad innescare disservizi, costi di manutenzione e rischi per la sicurezza informatica.
La PdL deve essere custodita con cura da parte degli utenti assegnatari evitando ogni possibile forma di danneggiamento.

6.2 Il Datore di Lavoro autorizza il personale incaricato che opera presso i SIA a compiere interventi sulle PdL diretti a garantire la sicurezza e la salvaguardia delle stesse, nonché per ulteriori motivi tecnici e/o manutentivi (es.: aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.). La stessa facoltà, sempre ai soli fini della garanzia dell'operatività e della sicurezza informatica, si applica anche in caso di assenza o impedimento dell'utente assegnatario. Qualora lo specifico intervento dovesse comportare anche l'accesso ai contenuti delle singole PdL, il personale dei SIA ne darà comunicazione agli utenti interessati, preventivamente o, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

6.3 Il personale incaricato dei SIA ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole PdL al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza in caso di virus, spyware, o altro software malevolo. L'intervento da remoto viene effettuato, di norma, su richiesta dell'utente e previa sua autorizzazione al collegamento o in caso di oggettiva necessità (es.: segnalazione automatica da parte dei sistemi antivirus). In quest'ultimo caso il personale dei SIA, attesa la necessaria tempestività, è autorizzato ad intervenire senza comunicazione preventiva e consenso dell'utente.

6.4 Non è consentito l'utilizzo di programmi/software diversi da quelli installati dal personale dei SIA, né viene consentito agli utenti di installare autonomamente programmi di qualsiasi tipo, sussistendo infatti il grave pericolo di introdurre virus informatici nella rete aziendale e/o di alterare la funzionalità delle applicazioni software esistenti. Inoltre, l'inosservanza della presente disposizione può dar luogo a violazioni della normativa a tutela dei diritti d'autore che impone la presenza sulle PdL di software regolarmente licenziato; violazioni che, in caso di controlli, possono essere sanzionate dalle autorità e comportare il sorgere di una responsabilità amministrativa.

6.5 Salvo preventiva espressa autorizzazione del personale dei SIA, non è consentito all'utente modificare le caratteristiche impostate sulla propria PdL, né procedere ad installare dispositivi di memorizzazione dati, comunicazione o altro (come ad esempio lettori CD, masterizzatori, modem, chiavette o hard disk USB, ecc.). Non è

consentito, inoltre, spostare in autonomia la PdL o modificarne la sua composizione con scambi di periferiche hardware (tastiere, mouse, monitor, ecc.).

6.6 La PdL deve essere spenta prima di lasciare gli uffici, anche al fine di ridurre il consumo di energia elettrica. Quando ci si assenta anche momentaneamente dalla PdL l'accesso deve essere bloccato tramite la combinazione "Tasto Windows + Tasto L". Sulla PdL viene attivato il blocco automatico (screen saver) dopo 5 minuti di inattività.

6.7 I file inerenti l'attività lavorativa non devono essere mantenuti sulla PdL bensì salvati sul Sistema di Gestione Documentale o nelle apposite cartelle del File Server Aziendale. In particolare, non devono in nessun caso essere memorizzati sulla PdL dati personali oggetto di trattamento da parte dell'ATS di Pavia, secondo le direttive del Regolamento Generale Protezione Dati UE del 27 aprile 2016 n. 679 (GDPR) in quanto, in caso di furto del pc o guasto dell'hard disk, la presenza di tali dati costituisce un data breach da comunicare al Garante della Privacy. Il personale dei SIA non esegue copie di sicurezza dei file presenti sulle PdL. Quando la PdL viene riconsegnata ai SIA il disco sarà formattato per permetterne il riutilizzo, quindi tutti i file presenti vengono cancellati in modo definitivo. È responsabilità dell'utente, o in sua vece del Responsabile di Struttura, segnalare ai SIA la presenza di eventuali file da salvare prima della cancellazione definitiva.

6.8 Su tutte le PdL aziendali (fisse e portatili) è implementata la crittografia del disco fisso con PIN di accesso al pc di otto cifre. Il PIN non è modificabile direttamente dall'utente. In caso di necessità la modifica va richiesta ai SIA.
È responsabilità dell'utente conservare il PIN in modo che non sia accessibile ad estranei e non sia riconducibile alla PdL a cui dà l'accesso.

6.9 Su tutte le PdL aziendali è attivo il servizio di Windows Update per l'aggiornamento del Sistema Operativo. Ogni utente deve prestare attenzione affinché la procedura di aggiornamento non venga interrotta e vada a buon fine.

6.10 Tutte le PdL aziendali sono protette da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o altro software aggressivo. Nel caso il software antivirus notifichi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto al personale dei SIA.

6.11 Particolare attenzione va posta da parte degli utenti a cui è stata assegnata, su richiesta del Responsabile di Struttura, una PdL portatile. Questa può essere utilizzata sia all' interno della rete aziendale, che dall'esterno (in mobilità o da casa). Nel secondo caso si utilizzerà una connessione di rete non protetta dal firewall aziendale (es.: tramite cellulare, rete casalinga, ecc.) per cui il rischio di infettare con malware il dispositivo aumenta, considerando che poi questo, una volta infetto e ricollegato alla rete aziendale, potrebbe creare danni alla stessa. Pertanto, si raccomanda vivamente di seguire con ancora più attenzione le indicazioni contenute nel presente Regolamento.

6.12 Essendo la PdL portatile più soggetta a rischio di sottrazione indebita, ogni utente deve custodirla con estrema diligenza, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Durante la permanenza in ufficio la PdL portatile deve sempre essere ancorata alla propria docking station e all'apposito cavo di sicurezza onde evitare furti.
Al di fuori dell'orario di servizio la PdL portatile non può essere lasciata incustodita in ufficio nemmeno se ancorata al cavo. E' a carico dell'utente assegnatario della Pdl portatile provvedere in tal senso (ad esempio riponendola in armadio chiuso a chiave)

Durante l'utilizzo all'esterno dei luoghi di lavoro (come in occasione di convegni, visite in aziende, workshop di lavoro, attività ispettive o di ricerca, smart working), la PdL non deve essere mai lasciata incustodita (prestare particolare attenzione a non lasciare la PdL visibile sull'automobile).
In caso di furto o smarrimento dell'apparecchiatura, l'assegnatario dovrà darne immediata comunicazione al Responsabile di Struttura e ai SIA, inoltre l'utente dovrà immediatamente resettare tutte le proprie credenziali di

accesso alle risorse informatiche. L'utente dovrà quindi presentare formale denuncia di furto o smarrimento presso le autorità competenti e farne pervenire copia al Datore di Lavoro e ai SIA per i successivi adempimenti. Sulla denuncia vanno indicati chiaramente i dati relativi al pc portatile: marca, modello, numero di serie, cespite aziendale, ecc. come da verbale di assegnazione, ed eventuali accessori sottratti/smarriti (es: alimentatore, mouse, ecc.).

Art. 7. Stampanti, fotocopiatrici e fax

7.1 L'utilizzo di stampanti, fotocopiatrici e fax deve avvenire sempre esclusivamente per attività lavorativa. Non è consentito un utilizzo per fini diversi.

7.2 Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

7.3 L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Art. 8. Utilizzo del File Server

8.1 Le cartelle presenti sul File Server dell'ATS di Pavia sono aree di condivisione di informazioni inerenti l'attività lavorativa e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file non legato all'attività lavorativa non può essere archiviato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back-up da parte del personale dei SIA. Si ricorda che le unità di memorizzazione locali (hard disk interno al PC) non sono soggette a salvataggio da parte del personale incaricato dei SIA, la responsabilità in caso di perdita di eventuali dati ivi contenuti è pertanto a carico del singolo utente.

8.2 La richiesta di creazione di una cartella viene richiesta ai SIA , con mail indirizzata alla casella ced@ats-pavia.it, dal Responsabile di Struttura. Per ciascun utente l'accesso a ciascuna cartella viene richiesto/revocato dal Responsabile di Struttura in base all'incarico assegnato all'utente nel rispetto delle misure di sicurezza applicate al trattamento dei dati contenuti nelle cartelle applicando i principi di finalità, proporzionalità e necessità del GDPR.

8.3 Con regolarità periodica (almeno ogni tre mesi), ciascun utente deve provvedere 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 al fine di contenere i costi di gestione e limitare il rischio di data breach. Eventuali file contenenti dati personali vanno crittografati o protetti con password rispondenti ai criteri indicati nella Password Policy, ricordando tuttavia di privilegiare sempre l'utilizzo del sistema di Gestione Documentale.

8.4 Nella gestione del File Server, il personale dei SIA, in qualunque momento, potrà procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza informatica.

Art. 9. Utilizzo della Posta Elettronica

9.1 La casella di posta elettronica viene assegnata all'utente su richiesta del Responsabile di Struttura. La casella di posta elettronica è uno strumento di lavoro. Gli utenti assegnatari delle caselle di posta elettronica aziendale sono

responsabili del corretto utilizzo delle stesse. Le caselle mail con indirizzo non nominativo (caselle generiche) consentono la condivisione tra più persone evitando che le informazioni rimangano in capo ad un solo soggetto; devono essere richieste dai Responsabili di Struttura indicando gli utenti autorizzati ad accedervi. Gli stessi utenti sono responsabili del loro corretto utilizzo.

9.2 È vietato utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. La casella di posta deve essere mantenuta in ordine, cancellando messaggi inutili o non costituenti corrispondenza aziendale. La casella di posta elettronica non è un sistema di archiviazione dati ed in particolare non deve contenere dati personali soggetti a trattamento da parte dell'ATS di Pavia.

9.3 È responsabilità di ogni utente porre la massima attenzione nell'aprire i file allegati ai messaggi di posta, verificando con attenzione il contenuto del messaggio ed il mittente. In ogni caso, non eseguire il download di file ed evitare l'utilizzo di link contenuti nelle mail sospette. In caso di dubbio consultare sempre i SIA.

9.4 È vietato trasmettere attraverso il sistema di posta elettronica dati personali che non siano inseriti in file protetti con password (che rispetti i criteri della Policy Password). È responsabilità di ogni utente cancellare dalla propria casella di posta i messaggi ricevuti contenenti dati personali non protetti da password.

9.5 Al fine di garantire la funzionalità del servizio, in caso di assenze programmate (ferie, attività fuori sede, ecc.) è necessario attivare la funzionalità di risposta automatica che ogni utente può impostare indicando il periodo di assenza ed eventuali altre modalità per contattare la struttura di appartenenza.

9.6 Il personale dei SIA non è autorizzato ad accedere alle caselle di posta elettronica personali se non nella necessità di non pregiudicare la necessaria tempestività ed efficacia del proprio intervento per le sole finalità legate a motivi di sicurezza informatica garantendo la riservatezza dei contenuti.

9.7 La casella di posta elettronica viene disattivata al momento della conclusione del rapporto di lavoro o in caso di assenza prolungata. E' responsabilità del Responsabile di Struttura inoltrare tempestivamente via email alla casella ced@ats-pavia.it la richiesta di disattivazione. Con la disattivazione viene esclusa la possibilità di inviare o ricevere mail ad una casella non presidiata. La cancellazione della casella di posta viene effettuata dai SIA dopo 150 giorni dalla disattivazione. Una volta cancellata, la casella può essere ripristinata entro 30 giorni. Trascorso questo termine, la casella e tutto il suo contenuto non saranno più recuperabili.

9.8 È opportuno che il Responsabile di Struttura, prima dell'avvenuta disattivazione della casella di posta elettronica, attivi comunicazioni ai soggetti terzi con cui il dipendente aveva rapporti indicando l'indirizzo e-mail di casella di posta istituzionale alternativo.

9.9 Il sistema di posta è protetto da software antivirus e antispam che può bloccare la ricezione di mail sospette notificando all'utente l'avvenuto blocco. L'utente può richiedere ai SIA il rilascio del blocco. Il SIA dopo aver preso visione e analizzato il messaggio decide se rilasciarlo all'utente o cancellarlo perché considerato malevolo comunicando all'utente tale esito.

9.10 Nel caso in cui all'utente venga assegnata la gestione di una casella di posta elettronica certificata si applicheranno le medesime disposizioni del presente regolamento.

Art. 10. Utilizzo di Internet

10.1 L'utilizzo della rete Internet aziendale è in generale vietato per motivi diversi a quelli legati all'attività lavorativa. Per limitare i rischi legati alla sicurezza informatica è quindi vietata la navigazione per motivi diversi da tale attività. In questo senso, e a titolo puramente esemplificativo, l'utente non potrà utilizzare la connessione Internet aziendale per:

a) il download di software, filmati, file musicali e altri contenuti non strettamente attinenti all'attività lavorativa;
b) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
c) la partecipazione a forum, social network, chat, news letter non attinenti all'attività lavorativa;
d) l'accesso a sistemi di posta elettronica non aziendali;
e) L'accesso a servizi non aziendali di scambio e condivisione file

10.2 Il personale incaricato dei SIA utilizza i file di log della navigazione Internet al solo fine di garantire la continuità operativa e la sicurezza informatica. Tali file di log includono l'indirizzo IP delle PdL, gli orari di accesso, i siti Internet visitati. I file di log non vengono sistematicamente archiviati, sono presenti sui sistemi Firewall, nello spazio disco ad essi assegnato, per il corretto perseguimento delle finalità di sicurezza informatica per un periodo di circa tre mesi.

10.3 I SIA sono autorizzati a bloccare, per motivi di sicurezza informatica e in generale per ottimizzare il traffico di rete, l'accesso ai siti Internet di alcune categorie di contenuti utilizzando specifici software di filtraggio automatico.

Art. 11. Utilizzo del servizio di telefonia fissa e mobile

11.1 I telefoni aziendali fissi vengono assegnati all'utente su richiesta adeguatamente motivata del Responsabile di Struttura.

11.2 I dispositivi di telefonia mobile (cellulari e tablet) vengono richiesti dal Responsabile di Struttura con parere favorevole del Direttore Strategico di riferimento; l'assegnazione sarà comunque subordinata alla disponibilità economica.

11.3 I telefoni aziendali fissi e i dispositivi di telefonia mobile (cellulari e tablet) devono in generale essere utilizzati esclusivamente per l'attività lavorativa.

11.4 L'uso del telefono cellulare e di altri strumenti per la connettività in mobilità può essere concesso quando la natura delle prestazioni e dell'incarico richiedano pronta e costante raggiungibilità in luoghi diversi dalla sede di lavoro.

11.5 L'utente assegnatario del dispositivo di telefonia mobile è responsabile del suo corretto utilizzo dal momento della presa in consegna fino alla restituzione e/o revoca, e dovrà porre ogni cura nella sua conservazione, per evitare danni, smarrimenti o sottrazioni. Nel caso in cui un apparecchio sia concesso a più utilizzatori per l'erogazione di un servizio (es: servizio di reperibilità), l'assegnatario è il Responsabile della Struttura che eroga il servizio. In ogni caso, la struttura assegnataria dovrà tenere nota degli effettivi utilizzatori per tutta la durata della concessione.

11.6 Il dispositivo di telefonia mobile viene concesso per il tempo strettamente necessario all'esigenza di servizio, in base alle indicazioni del Responsabile di Struttura e in ogni caso deve essere restituito alla cessazione del rapporto di lavoro. Pertanto, al venire meno dei requisiti indicati nella richiesta o in caso di cessazione del rapporto di lavoro, l'utente assegnatario dovrà provvedere prima possibile alla restituzione di quanto fornito dai SIA (apparato e relativa dotazione così come indicati nel verbale firmato alla consegna). Gli incaricati dei SIA provvederanno al controllo di quanto riconsegnato rilasciando all'utente apposito verbale di restituzione.

11.7 L'assegnatario del dispositivo di telefonia mobile deve prestare attenzione alla sicurezza informatica ed in particolare attenersi scrupolosamente alle seguenti indicazioni:

a) È obbligatorio l'attivazione del sistema di blocco del dispositivo e della SIM (PIN).
b) È vietato spostare la SIM in dotazione su dispositivi diversi da quello assegnato.
c) È vietata l'attivazione di servizi interattivi a pagamento che potrebbero comportare elevati costi aggiuntivi.
d) È vietata la sostituzione degli accessori originali (carica batterie, cavo USB, auricolari) consegnati con l'apparato.
e) È vietato memorizzare sull'apparato password di accesso ad applicativi aziendali (es.: e-mail).
f) Limitare l'installazione di eventuali App alle sole esigenze inerenti l'attività lavorativa.
g) Prestare estrema attenzione nell'autorizzare determinate App all'accesso ai dati e alle risorse dell'apparato (es.: GPS, fotocamera, microfono, account, ecc.) anche a tutela della propria privacy.

11.8 In caso di furto o smarrimento del dispositivo di telefonia mobile, l'assegnatario dovrà darne immediata comunicazione ai SIA, ai fini dell'immediato blocco dell'utenza. L'assegnatario dovrà quindi presentare formale denuncia di furto o smarrimento presso le autorità competenti e farne pervenire copia al Datore di Lavoro e ai SIA per i successivi adempimenti. Sulla denuncia vanno indicati chiaramente i dati relativi all'apparato (Modello – cod. IMEI), il numero ad esso associato ed eventuali accessori sottratti/smarriti (es: carica batterie, cavo USB, ecc.). Inoltre per limitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente resettare eventuali password memorizzate incautamente sul dispositivo stesso (es. accesso alla webmail aziendale).

11.9 Il Datore di lavoro non è responsabile per la perdita o compromissione di dati personali che l'utente ha trasferito o memorizzato sul dispositivo mobile.

Art. 12. Utilizzo del servizio VPN

12.1 L'accesso da remoto alla rete aziendale attraverso il servizio VPN è consentito, al personale dei SIA, ai fornitori autorizzati per attività di assistenza sui sistemi aziendali e ai dipendenti con contratto di Telelavoro. L'accesso è altresì consentito agli utenti, su richiesta motivata del Responsabile di Struttura, per il tempo strettamente necessario alla gestione di rilevanti criticità operative purché dotati di postazione di lavoro fornita dall'ATS di Pavia.

Art. 13. Sanzioni

13.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, fatte salve le ulteriori responsabilità civili, penali e contabili previste dalla normativa vigente. Sul punto si rinvia al Codice di Comportamento dell'ATS di Pavia.

13.2 Nei confronti di consulenti, fornitori e collaboratori, a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es.: lavoratori somministrati, collaboratori coordinati e continuativi, stagisti, borsisti, tirocinanti, specializzandi, ecc.) autorizzati ad utilizzare le risorse informatiche dell'ATS di Pavia e ad accedere a dati e informazioni ivi conservati e trattati, verificata la gravità della violazione contestata, l'ATS di Pavia si riserva di agire con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

Art. 12. Entrata in vigore e aggiornamento

14.1 Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, poiché sostituite dalle presenti.

14.2 Il presente Regolamento è soggetto periodicamente a revisione.

ALLEGATO 1 - Indicazioni specifiche per la Sicurezza Informatica

Premessa

Scopo delle seguenti indicazioni è informare gli utenti su cosa "fare" e cosa "non fare" in alcune tipiche situazioni a rischio che possono compromettere il Sistema Informativo Aziendale.
La compromissione del Sistema Informativo Aziendale può determinare la mancata erogazione di prestazioni, la perdita o il furto di dati con conseguenti danni in termini di immagine e di sanzioni per violazione della riservatezza dei dati trattati.
Tutti gli utenti sono tenuti a conoscere e rispettare queste indicazioni, comprendere i rischi derivanti dalla mancata applicazione e, in caso di situazione dubbia, contattare sempre il personale dei SIA.

Descrizione rischi e indicazioni da seguire

rischio: il collegamento non autorizzato di un dispositivo alla rete causa malfunzionamenti che possono portare anche alla completa indisponibilità del Sistema Informativo Aziendale.
Cosa fare: **NON** collegare dispositivi alla rete dati aziendale senza autorizzazione.

rischio: l'apertura di un messaggio di posta elettronica, l'apertura di un allegato o l'attivazione di un link che apre una pagina web espone l'utente al rischio di trasmettere virus che possono distruggere dati e/o bloccare servizi informatici vitali per l'attività dell'ATS di Pavia.
Cosa fare: astenersi dall'apertura di messaggi con oggetto e/o mittente non chiaramente riconducibile al contesto di lavoro e cancellare il messaggio. Se il messaggio viene aperto leggere con attenzione il testo. Spesso i messaggi malevoli contengono forme grammaticali scorrete, errori, parole in altre lingue, in questo caso cancellare il messaggio immediatamente senza aprire allegati o link a pagine web. **Mai** rispondere a un messaggio fornendo informazioni riservate (es: password o credenziali in genere).

rischio: la navigazione Internet veicola virus che possono distruggere dati e/o bloccare servizi informatici vitali per l'attività dell'ATS di Pavia.
Cosa fare: è necessario limitare la navigazione Internet al contesto lavorativo e cioè ai siti web istituzionali (governativi, pubbliche amministrazioni, organizzazioni e società che operano nel settore della Sanità, ecc.).

Rischio: l'installazione di un software non controllato può nascondere virus che possono distruggere dati e/o bloccare servizi informatici vitali per l'attività dell'ATS di Pavia.
Cosa fare: **NON** installare software sulle PdL.

Rischio: il mancato aggiornamento del software della PdL consente ai virus di sfruttare le vulnerabilità per fare danni.
Cosa fare: è necessario prendersi cura delle PdL che si utilizzano, comprendendo che le operazioni di aggiornamento automatico del software (sistema operativo/antivirus/applicativi) sono inevitabili anche se possono interferire con l'attività lavorativa in quanto la postazione può rimanere inutilizzabile per alcuni minuti. Questi processi di aggiornamento **NON** devono essere assolutamente interrotti (ad esempio spegnendo la PdL durante l'aggiornamento).

Rischio: l'utilizzo di sistemi e-mail non aziendali veicola virus che possono distruggere dati e/o bloccare servizi informatici vitali per l'attività dell'ATS di Pavia
Cosa fare: **NON** utilizzare sistemi di posta elettronica non aziendali sulle PdL.

Rischio: la memorizzazione delle password su computer o cellulari equivale a consegnare le proprie password al software malevolo che le può utilizzare, ad esempio, per entrare nella casella e-mail e cancellare o rubare i messaggi e gli indirizzi contenuti.
Cosa fare: **NON** memorizzazione mai le password su computer o cellulari. Occorre fare attenzione al fatto che sia i browser che molti programmi consentono di farlo per comodità dell'utente. In caso di furto o smarrimento di qualsiasi dispositivo su cui sono state incautamente memorizzate delle credenziali è obbligatorio, come forma di mitigazione del rischio, modificare le password di dette credenziali con le seguenti modalità:

- Per le PDL: combinazione tasti CTRL + ALT + CANC - > Cambia password

- Per il File Server Aziendale: contattare l'HelpDesk con le consuete modalità - >
    c) Inserendo una richiesta al link: https://bcsfwesp.service-now.com/bcs
    d) Numero verde 800185441
    e) Inviando una mail all'indirizzo hdatspavia@bcs.it

- Per le credenziali LDAP (Posta, Firewall, Protocollo, Angolo del Dipendente, Intranet aziendale, Atti): accedere a https://password.ats-pavia.it - > eseguire Login con le credenziali LDAP in uso e cliccare su Cambia Password seguendo la procedura.

- Per Applicativi aziendali non integrati LDAP (Screening, ADIWEB, ERP, altro): contattare l'HelpDesk con le consuete modalità - >
    a) Inserendo una richiesta al link: https://bcsfwesp.service-now.com/bcs
    b) Numero verde 800185441
    c) Inviando una mail all'indirizzo hdatspavia@bcs.it

Rischio: l'utilizzo di dispositivi esterni (pen drive, dischi USB, smartphone, ecc.) compromessi da virus può danneggiare le PdL.
Cosa fare: **NON** collegare dispositivi esterni alle PdL.

Rischio: accesso alla PdL da parte di estranei o di colleghi non autorizzati durante la temporanea assenza dell'assegnatario.
Cosa fare: quando ci si assenta dalla propria postazione bloccarla in modo che questa non sia accessibile tramite la combinazione tasto Windows + tasto L. Al termine dell'orario di servizio spegnere la postazione. Modificare la password di accesso alla postazione ogni 6 mesi secondo la Policy Password aziendale. Custodire in luogo sicuro la password di accesso alla postazione (e in generale ogni altra tipologia di password), **NON** lasciarla mai in vista sulla scrivania o accanto al monitor.

Rischio: memorizzazione, archiviazione e gestione di file contenenti dati personali su file server aziendale.

Cosa fare: file con dati personali salvati sul file server devono essere protetti da password al fine di garantire la riservatezza e la sicurezza al dato trattato.

Rischio: pubblicazione di documenti contenenti dati personali su portale Internet dell'ATS di Pavia.
Cosa fare: occorre evitare la pubblicazione di documenti contenenti dati personali sul portale Interne dell'ATS di Pavia. Nel caso in cui il documento da pubblicare contenga in origine dei dati personali è necessario procedere all'oscuramento di tali dati, eventualmente chiedendo supporto tecnico ai SIA.

Rischio: utilizzo del sistema di posta elettronica per invio email per la condivisione di dati personali.
Cosa fare: occorre innanzi tutto progettare (privacy by design) il trattamento dei dati utilizzando per la trasmissione sistemi più sicuri (protocollo, SFTP, altri sistemi di file sharing). Una volta valutati i rischi connessi alla trasmissione via email è necessario che i dati personali vengano inseriti in file protetti da password (che rispetti i criteri della Policy Password contenuta nel presente Regolamento) e la condivisione della password tra trasmittente e destinatario deve essere comunicata per altra via (es.: sms, a voce). Occorre inoltre fare attenzione al fatto che molti sistemi antispam bloccano i messaggi con allegati file protetti da password. E' per tanto opportuno concordare con i destinatari questa modalità di trasmissione in modo tale che ciascuno possa controllare con i propri SIA l'avvenuta trasmissione/ricezione.

Rischio: conservazione accidentale di file indesiderati sulla PdL.
Cosa fare: quando vengono effettuate operazioni di download di un file questo può rimanere memorizzato nella cartella "Download" sulla PdL. Quando viene cancellato un file viene mantenuta una copia nel "Cestino". In entrambi i casi l'utente deve controllare il contenuto delle cartelle Download e Cestino e cancellare definitivamente file indesiderati con particolare attenzione ai file contenenti dati personali seppur protetti da password.

Rischio: trasmissione non autorizzata di indirizzi di posta elettronica a soggetti terzi
Cosa fare: nelle comunicazione via posta elettronica a soggetti terzi e soprattutto quanto il numero di indirizzi è elevato (es. gruppi di lavoro, comunità di settore ecc.) è sempre necessario valutare se gli indirizzi possono essere visibili a tutti oppure è più opportuno che ciascun soggetto destinatario della comunicazione veda solo il proprio indirizzo. Sia i sistemi di posta elettronica che i sistemi di protocollo consentono di spedire comunicazioni con gli indirizzi NON visibili a tutti.
In generale la modalità suggerita è di NON rendere visibili a tutti gli indirizzi. Quando invece si ritiene più efficace la scelta di rendere gli indirizzi visibili a tutti, prima di effettuare le comunicazioni, è necessario acquisire il consenso.