APPROVATO CON DELIBERA 133 DEL 19.02.2026

A.S.L. TO4

Azienda Sanitaria Locale
di Ciriè, Chivasso e Ivrea

REGOLAMENTO AZIENDALE
UTILIZZO PC E RETE INFORMATICA

S.C. SISTEMI INFORMATIVI E UFFICIO FLUSSI

ELENCO DELLE REVISIONI

Paragrafo	Descrizione Modifica	Rev. N.	Data Rev.
	Stesura	1	08/08/2025
Uso dispositivi personali	Modifica	2	14/08/2025
Generale	Modifica	3	12/02/2026

Sommario

Premessa

La progressiva diffusione delle nuove tecnologie ICT ed in particolare l'utilizzo della posta elettronica ed il libero accesso alla rete Internet, espone l'Azienda Sanitaria Locale Torino 4 e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura tecnica, patrimoniale e reputazionale, oltre alle responsabilità legali conseguenti alla violazione di specifiche disposizioni di legge (diritto d'autore, privacy, ecc.), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'ASL Torino 4 ha predisposto il presente Regolamento Informatico Aziendale per il corretto utilizzo delle e-mail, allo scopo di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati. Considerato inoltre che l'Azienda, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori apparecchiature informatiche e mezzi di comunicazione, sono stati inseriti nel regolamento alcuni articoli relativi alle modalità ed alle regole che ciascun utente deve osservare nell'utilizzo delle apparecchiature informatiche.

Campo di Applicazione

Il presente regolamento si applica a tutti i dipendenti - senza distinzione di ruolo e/o livello - nonché a tutti i collaboratori dell'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (consulenti, lavoratori somministrati, collaboratori a progetto, in stage, volontari, tirocinanti, ditte esterne autorizzate, ecc.).

Finalità

Le apparecchiature informatiche, gli applicativi ed in generale tutte le risorse informatiche che l'ASL Torino 4 mette a disposizione dei suoi utenti, ivi compresi i servizi di internet e posta elettronica, devono essere utilizzati esclusivamente per fini lavorativi e non personali e nel pieno rispetto della normativa vigente, nonché del presente Regolamento Aziendale. Ciò al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso, oltre che garantire il rispetto dei principi generali in materia di trattamento dei dati personali sanciti dal Regolamento Europeo Generale sulla Protezione dei Dati – GDPR.

Tutto il personale interessato dalle disposizioni del presente Regolamento è tenuto a contattare la S.C. Sistemi Informativi e Ufficio Flussi prima di intraprendere qualsiasi attività tecnica non esplicitamente compresa nel presente regolamento, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

Competenze

Nell'ambito della gestione delle risorse e dei servizi informatici aziendali risultano essere direttamente coinvolte determinate Strutture, ciascuna con specifiche competenze.

Al fine di agevolare l'utente nella risoluzione delle problematiche relative all'utilizzo dei servizi già menzionati, si descrivono nel seguito le specifiche competenze della S.C. Sistemi Informativi e Ufficio Flussi.

La S.C. Sistemi Informativi e Ufficio Flussi è l'unica articolazione aziendale, fatte salve eventuali deroghe che possono essere concesse di volta in volta, preposta all'acquisto di hardware, software e servizi di natura informatica. È l'articolazione aziendale preposta a garantire il corretto funzionamento del S.I.A. (Sistema Informativo Aziendale) e le cui principali competenze possono essere sintetizzate come segue:

- fornire parere tecnico e consulenza in merito ad acquisto e gestione di software ed apparecchiature informatiche (compresi sistemi in gestione alla S.C. Servizio Tecnico) fatta eccezione per i dispositivi elettromedicali la cui competenza è in capo all'Ufficio Ingegneria Clinica;
- fungere da interfaccia tecnica fra gli utenti del S.I.A. e le ditte fornitrici;
- garantire il corretto funzionamento delle postazioni di lavoro informatiche (nel seguito PdL);
- fornire a tutti gli utenti, durante il normale orario di lavoro, un Call Center di primo livello per la segnalazione di malfunzionamenti;
- gestire gli utenti del S.I.A. con i dovuti criteri di sicurezza e riservatezza;
- gestire e monitorare la rete aziendale;
- assegnare le apparecchiature informatiche;
- formare il personale sul corretto uso delle risorse e delle procedure di Office Automation utilizzate.

Si precisa che la S.C. Sistemi Informativi e Ufficio Flussi non è in alcun caso proprietaria dei dati gestiti dal S.I.A. e che pertanto eventuali statistiche o report dovranno essere richiesti alle strutture di competenza (Controllo di Gestione, S.C. Amministrazione del Personale, S.C. Gestione Economico-Finanziaria, ecc.). Analogamente, il corretto utilizzo delle procedure applicative (contabili, sanitarie, gestione del personale, ecc.) è di competenza delle diverse articolazioni aziendali che utilizzano il software.

Hardware e Software

Acquisto / Noleggio di hardware e software

Tutto l'hardware ed il software potrà essere acquistato/noleggiato solo previa richiesta di parere tecnico favorevole da parte della S.C. Sistemi Informativi e Ufficio Flussi, che controllerà le richieste di acquisto al fine di valutare la compatibilità e prevenire la compromissione della sicurezza del sistema informatico aziendale.

Tutto il software in uso presso l'ASL TO4 deve essere ottenuto seguendo le procedure e le linee guida dell'Ente e deve essere registrato a nome dell'ASL TO4.

A tal fine le richieste di acquisto dell'hardware e del software dovranno essere redatte su apposito modulo disponibile nel sito aziendale nella sezione modulistica. Tale modulo dovrà essere inviato a mezzo e-mail all'indirizzo "sistemiinformativi@aslto4.piemonte.it". Le richieste incomplete o compilate in modo errato non potranno essere prese in considerazione e verranno restituite al mittente.

Alla S.C. Sistemi Informativi e Ufficio Flussi spetta la verifica tecnica della compatibilità degli strumenti richiesti con l'infrastruttura dell'Ente. Nel caso in cui gli strumenti proposti non possano - per ragioni tecniche - essere installati, verranno individuate - ove possibile - soluzioni alternative, d'intesa tra la S.C. Sistemi Informativi e Ufficio Flussi ed il servizio richiedente.

In ogni caso, prima dell'acquisizione di nuovi software e/o hardware (specialmente se devono essere collegati alla rete aziendale) verrà sempre effettuata un'analisi del relativo rischio, tendente a valutare l'impatto potenziale della modifica richiesta sulla sicurezza delle informazioni e a pianificare le necessarie azioni di ripristino, subordinando l'acquisizione all'esito positivo della predetta analisi.

I supporti originali dei software acquistati e le relative licenze devono essere conservati presso la S.C. Sistemi Informativi e Ufficio Flussi, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale re-installazione delle procedure.

L'acquisto e la gestione dei materiali di consumo (carta, toner, etichette, CD/DVD, ecc.) non sono di competenza della S.C. Sistemi Informativi e Ufficio Flussi.

Utilizzo dei software

Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di Autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere rispettate da tutti gli utenti. (DLG. 518/92 sulla tutela giuridica del software e L. 248/2000 "*nuove norme di tutela del diritto d'autore*"). Pertanto, il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (*copyright*) e non può in alcun caso installare, duplicare od utilizzare software ottenuto illegalmente o comunque sprovvisto delle necessarie licenze.

Non è consentito in alcun caso installare ed utilizzare programmi diversi da quelli ufficialmente installati dai tecnici della S.C. Sistemi Informativi e Ufficio Flussi per conto dell'Azienda, salvo specifiche deroghe che dovranno essere preventivamente richieste, giustificate ed autorizzate, nonché concretamente gestite e monitorate dalla S.C. Sistemi Informativi e Ufficio Flussi.

Al fine di proteggere l'integrità del S.I.A. dell'ASL TO4, al personale non è consentito nemmeno installare ed utilizzare eventuale software di proprietà personale. Tale principio vincolante si applica anche alle applicazioni regolarmente acquistate e registrate, programmi shareware o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

L'utente è responsabile del software installato sul proprio PC e di come lo utilizza; se ne raccomanda pertanto un uso diligente ed accorto.

Non è in alcun caso consentita la disinstallazione/rimozione dei software presenti sui sistemi. I suddetti interventi saranno effettuati, in caso di necessità, solo a cura dei tecnici della S.C. Sistemi Informativi e Ufficio Flussi dietro segnalazione dell'utente e relativa approvazione.

In particolare, non è consentito in alcun caso rimuovere, disinstallare o disabilitare - anche temporaneamente - il software antivirus presente sui computer, oppure compiere qualsiasi altra azione comunque tendente ad impedirne l'aggiornamento automatico o la piena funzionalità.

Nell'eventualità di PC non collegati alla rete aziendale e/o la cui gestione, per svariati motivi, non sia a carico della S.C. Sistemi Informativi e Ufficio Flussi, sarà cura del fornitore procedere al regolare aggiornamento del software.

Rientra nelle facoltà della S.C. Sistemi Informativi e Ufficio Flussi bloccare automaticamente il download - da siti non istituzionali o non affidabili - di software potenzialmente infetto. Nel caso in cui sia ritenuto necessario "scaricare" determinati files dalla rete ed il relativo download risulti bloccato, l'utente dovrà formulare una richiesta. La S.C. Sistemi Informativi e Ufficio Flussi, previe le verifiche tecniche del caso, provvederà ad autorizzare il download. Nel caso in cui la richiesta di download sia legata alla necessità di installazione di un software non ricompreso tra quelli aziendali, il richiedente dovrà fare inoltrare dal proprio responsabile una richiesta alla S.C. Sistemi Informativi e Ufficio Flussi che procederanno dopo valutazione tecnica.

Gli utenti devono essere consapevoli che l'inosservanza delle disposizioni sopra elencate potrebbe esporre l'Azienda a gravi ripercussioni in sede di giustizia civile; si evidenzia altresì come le violazioni della normativa a tutela del diritto d'Autore vengano sanzionate anche penalmente.

Si richiede pertanto agli utenti di tenere sempre un comportamento diligente ed attento nell'utilizzo del software, in modo da rendere sicuro il proprio lavoro e tutelare altresì l'Ente.

Utilizzo del Personal Computer

La postazione di lavoro o PDL (Personal Computer, monitor, stampante, etichettattrice, scanner, ecc.) affidata all'utente è uno strumento di lavoro che deve essere custodito con cura, adottando ogni precauzione necessaria ad evitare qualsiasi possibile forma di danneggiamento. L'utilizzo non inerente all'attività lavorativa è vietato, poiché può comportare disservizi e - soprattutto - minacce alla sicurezza.

Gli utenti, nel compimento delle normali attività mediante gli strumenti informatici:

- devono accedere al dominio aziendale utilizzando esclusivamente le credenziali assegnate identificandosi con nome utente e relativa password. I lavoratori che per determinate e circoscritte finalità, hanno necessità di utilizzo di un account con privilegi amministrativi, verificato che sono in possesso delle necessarie competenze, ricevono a tal fine, dalla S.C. Sistemi Informativi e Ufficio Flussi, un account privilegiato che dovrà essere utilizzato solamente quando necessario per la realizzazione delle specifiche e limitate attività che lo richiedono. Al contrario, per le operazioni ordinarie anche tali utenti dovranno utilizzare l'account senza privilegi amministrativi;

- non devono in alcun modo modificare, rimuovere e/o disattivare le misure di sicurezza predisposte nel dispositivo, né compiere azioni di modifica dei sistemi (ad esempio: disattivare gli aggiornamenti del sistema operativo, la protezione in tempo reale dell'antivirus o il suo aggiornamento automatico, il firewall del sistema operativo);

- non devono utilizzare account di accesso al dominio aziendale e alle diverse procedure informatiche, diversi da quello assegnato.

Gli utenti dovranno prestare la massima attenzione nell'apertura di documenti che richiedono l'attivazione di particolari funzionalità (ad esempio le c.d. macro nei file Excel e Word). Le stesse dovranno essere consentite esclusivamente quando l'utente è certo della provenienza legittima del documento e, in caso di minimo dubbio, non dovrà mai essere consentita l'esecuzione del codice, dovendosi piuttosto rivolgere per la necessaria consulenza ai tecnici della S.C. Sistemi Informativi Ufficio Flussi. La stessa regola di prudenza vale altresì per l'apertura di link inviati mediante e-mail od altre forme di comunicazione, i quali dovranno prima essere vagliati circa la loro provenienza ed apparente sicurezza.

Le credenziali di accesso al sistema non vanno in alcun modo riportate in fogli od altri supporti cartacei, né vanno salvate in file di testo sul computer od altri documenti digitali ovunque riposti. Inoltre le stesse non devono in alcun caso essere comunicate (a voce o in altre forme) ad altri collaboratori e/o terzi.

Nel modificare la password di accesso al dominio aziendale, dovranno essere sempre rispettati i necessari parametri di sicurezza, ovvero:

- lunghezza minima di 12 caratteri;
- utilizzo di almeno un carattere minuscolo, almeno un carattere maiuscolo e di almeno un numero;
- utilizzo di almeno un carattere speciale (es, - @ # $ % ^ & * - _ ! + = , . ? ( ) ; <>) ;
- divieto di utilizzo di parole troppo "semplici" (es. "password") e di informazioni relative alla persona contenute nel nome utente (es. il cognome);
- la nuova password deve essere diversa dalle ultime 4 utilizzate in precedenza.

In base alla normativa vigente, la password di accesso dovrà essere modificata ogni 3 mesi.

Le postazioni di lavoro fisse devono essere mantenute in ordine, pulite e prive di pericoli per i sistemi informatici.

È fatto assoluto divieto all'utente di intervenire in qualunque modo sull'hardware in dotazione. In caso di malfunzionamento delle apparecchiature assegnate dalla S.C. Sistemi Informativi e Ufficio Flussi, l'utente è tenuto a darne tempestiva segnalazione al personale addetto. La manutenzione di tali apparecchiature è di assoluta pertinenza dei tecnici della S.C. Sistemi Informativi e Ufficio Flussi.

Il Personal Computer, al termine dell'utilizzo o comunque in caso di assenze prolungate dall'ufficio deve essere spento. Inoltre, la sessione va bloccata non appena ci si allontana dalla postazione di lavoro al fine di impedirne l'uso, con le proprie credenziali, da parte di terzi. Qualora l'utente sia costretto ad assentarsi dal locale in cui è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima, dovrà pertanto eseguire una delle seguenti operazioni: spegnimento del PC, blocco o disconnessione della sessione di lavoro; si ricorda che lasciare un elaboratore incustodito dopo aver fatto accesso con le proprie credenziali può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Sulle postazioni di lavoro è stata implementata una policy che prevede il blocco automatico della sessione di lavoro dopo 20 minuti di inattività con l'attivazione della schermata di blocco e la richiesta di inserimento di password per lo sblocco.

I tecnici della S.C. Sistemi Informativi e Ufficio Flussi sono autorizzati a compiere interventi nel Sistema Informatico Aziendale diretti a garantirne la manutenzione e la sicurezza. Nel rispetto della

normativa Europea e Nazionale in tema di protezione dei dati personali, detti interventi potranno anche comportare - ove necessario - l'accesso ai dati trattati dal sistema, ivi compresi gli archivi di posta elettronica.

I tecnici della S.C. Sistemi Informativi e Ufficio Flussi potranno in qualunque momento procedere alla rimozione di file ed applicativi ritenuti non sicuri.

Il personale incaricato S.C. Sistemi Informativi e Ufficio Flussi ha la facoltà - in caso di richiesta o di stretta necessità - di collegarsi da remoto al desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica necessaria nonché la sicurezza contro eventuali malware.

Utilizzo di dispositivi personali

È vietato agli utenti la connessione alla rete aziendale di PC, laptop, tablet, smartphone, periferiche quali stampanti o scanner e di ogni altro dispositivo personale, salvo nei casi espressamente autorizzati dalla Direzione Generale.

Utilizzo dei supporti rimovibili

Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti a controllo antivirus prima di essere aperti e/o utilizzati.

L'utilizzo di supporti rimovibili (CD e DVD anche riscrivibili, supporti USB, hard disk esterni, ecc.) deve essere limitato a quanto strettamente indispensabile alle attività aziendali; in tali supporti non devono essere conservati, nemmeno provvisoriamente, file aziendali congiuntamente a file personali.

Non è permesso scaricare o copiare file contenuti in supporti removibili esterni (chiavette USB, hard disk esterni, schede di memoria) sulle PdL aziendali.

Utilizzo di PC portatili e Tablet

Considerati i maggiori rischi di sicurezza derivanti dall'utilizzo di dispositivi mobili, l'Ente potrà assegnare all'utente un PC portatile solamente nel caso di effettiva necessità e previa ed esauriente relazione, sottoscritta dal Direttore del Servizio o Responsabile della Struttura, e parere favorevole della S.C. Sistemi Informativi e Ufficio Flussi. Per le figure dirigenziali amministrative e/o responsabili di uffici amministrativi, che ruotano su più sedi nel territorio, può essere assegnato il PC portatile al posto del PC desktop.

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con la massima diligenza possibile, sia durante gli spostamenti che durante l'utilizzo sul luogo di lavoro, evitando di esporre lo stesso al rischio di manomissioni e furto.

Ai PC portatili si applicano le medesime regole di utilizzo previste dal presente regolamento per i Personal Computer.

Particolare attenzione deve essere rivolta all'utilizzo temporaneo del PC portatile, essendo necessario rimuovere - prima della riconsegna - documenti e altri files salvati nel periodo d'uso.

Eventuali connessioni di rete, dirette verso la rete aziendale o verso la rete esterna, possono essere configurate esclusivamente richiedendole alla S.C. Sistemi Informativi e Ufficio Flussi.

Tutti i notebook con sono protetti da crittografia del disco e la chiave di ripristino è conservata presso la S.C. Sistemi Informativi e Ufficio Flussi.

Trattamento e conservazione dei dati

Ciascun utente è responsabile del corretto trattamento e dell'archiviazione sicura dei dati e delle informazioni utilizzate (documenti informatici, database, registrazioni audio/video, ecc.).

A tal fine, gli utenti devono conservare i files, i documenti informatici ed in generale tutte le informazioni digitali create/utilizzate, unicamente nel File Server / Share Point (cartelle condivise o aree di lavoro) rese disponibili dall'Ente a mezzo della S.C. Sistemi Informativi e Ufficio Flussi. I documenti ad uso esclusivo del singolo utente devono essere memorizzati sul dispositivo personale nella propria cartella Documenti, in modo di avere la sincronizzazione con OneDrive ed il relativo backup e non devono essere depositati nel File Server / Share Point. In tali aree devono essere solamente depositati file di carattere condiviso tra gli utenti. Solamente queste due modalità sono volte ad evitare perdite di dati derivanti dal mancato backup dei dati oltre alla maggior resilienza del sistema ai tentativi di furto o di accesso illecito di persone non autorizzate. Si ricorda che nelle aree condivise non devono essere depositati file di carattere personale ed extra lavorativo (a titolo esemplificativo foto/video personali, file musicali, ecc).

Ai dipendenti che trattano dati personali e/o informazioni aziendali riservate è richiesto di prestare la massima diligenza possibile – imposta anche dal rispettivo ruolo – nel trattamento dei predetti dati.

In particolare, gli utenti sono tenuti al riserbo sulle informazioni di cui vengono a conoscenza e tale obbligo si traduce altresì nell'utilizzo corretto e attento degli strumenti informatici che contengono quei dati.

Pertanto, i dipendenti dovranno attenersi alle misure di sicurezza indicate e fare quanto in loro potere per proteggere la riservatezza, l'integrità e la disponibilità dei dati aziendali, senza duplicarli, trasferirli, distruggerli e modificarli indebitamente.

I dipendenti dovranno altresì segnalare prontamente qualsiasi vulnerabilità di cui vengono a conoscenza, nonché l'utilizzo improprio dei dispositivi e dei software da chiunque posto in essere.

Agli utenti è altresì richiesto di impegnarsi attivamente nella formazione offerta dall'Azienda e/o da fornitori terzi, in modo da acquisire e rinforzare le competenze necessarie a trattare in sicurezza i dati personali e/o comunque riservati.

In caso di cessazione del rapporto di lavoro gli account utente vengono disattivati e i dati delle cartelle condivise restano sul server aziendale. Nel caso in cui l'utente avesse in uso un PC portatile, lo stesso viene restituito al proprio Dirigente/Responsabile che provvederà a riassegnarlo ad altra unità di personale oppure a restituirlo alla S.C. Sistemi Informativi e Ufficio flussi. Per i dispositivi oggetto di rottamazione si procederà con l'estrazione delle memorie di massa contenenti i dati affinché siano conservate in luogo sicuro per 30 giorni trascorsi i quali si procederà con la definitiva distruzione rendendo impossibile l'accesso ai dati memorizzati.

Accesso alla rete aziendale, Internet e Gestionali

Gestione credenziali

Per la gestione delle credenziali, l'Azienda è dotata di una piattaforma, denominata CredNET, accessibile da tutti i PC collegati alla rete aziendale, nella quale viene centralizzata la richiesta ed il rilascio degli account (credenziali di accesso) per i diversi applicativi.

A seguito dell'inserimento delle richieste di creazione/modifica/eliminazioni di credenziali da parte del Responsabile della Struttura o del suo delegato, la piattaforma, inoltra in automatico le richieste ai rispettivi Amministratori di sistema che gestiscono gli applicativi di interesse.

L'esito delle attività viene notificato al Responsabile mentre le credenziali vengono inviate direttamente all'assegnatario.

Assegnazione e gestione account

L'assegnazione dell'account personale per l'accesso al dominio aziendale viene fatta dal personale della S.C. Sistemi Informativi e Ufficio Flussi, con l'applicazione di un automatismo che inserisce la richiesta sulla piattaforma di richieste/rilascio credenziali CredNET per tutti i dipendenti, mentre per i casi di personale con contratti di appalto, consulenti, tirocinanti, borsisti, stagisti, ecc., le richieste devono essere effettuate dal Responsabile.

Le credenziali di accesso al dominio vengono revocate alla chiusura del rapporto di lavoro tra l'assegnatario e l' ASL TO4.

Si sottolinea l'importanza nel mantenere la riservatezza delle proprie credenziali in quanto tutte le attività informatiche e gli accessi ai dati, effettuate a seguito di autenticazione sono ricondotte alla persona fisica assegnataria delle stesse.

Alcuni utenti della S.C. Sistemi Informativi e Ufficio Flussi sono assegnatari di utenze con privilegi amministrativi, anch'esse sempre riconducibili alle persone fisica a cui sono state assegnate

Per tutti gli utenti le password di accesso al dominio devono rispettare i seguenti criteri:

- lunghezza minima di 12 caratteri (16 caratteri per gli utenti con privilegi amministrativi)
- utilizzo di almeno un carattere minuscolo, almeno un carattere maiuscolo e di almeno un numero;
- utilizzo di almeno un carattere speciale (es: , - @ # $ % ^ & * - _ ! + = , . ? ( ) ; <>) ;
- divieto di utilizzo di parole troppo "semplici" (es. "password") e di informazioni relative alla persona contenute nel nome utente (es. il cognome);
- la nuova password deve essere diversa dalle ultime 4 utilizzate in precedenza.

Relativamente all'accesso al dominio le password scadono dopo 90 giorni (60 per gli utenti con privilegi amministrativi).

Le credenziali di accesso a specifiche procedure aziendali devono sempre essere richieste dal Responsabile o dal suo delegato tramite la piattaforma CredNET.

Le credenziali di autenticazione consistono in un nome utente o *userid,* assegnato dalla S.C. Sistemi Informativi e Ufficio Flussi, volto ad identificare univocamente il soggetto e una password che dovrà essere custodita dall'utente e da questi mantenuta riservata.

Non è ammesso in alcun caso l'accesso a servizi e sistemi senza previa autenticazione con le predette credenziali identificative.

Al primo accesso, sarà necessario procedere alla modifica della password e, successivamente, variarla ogni tre mesi (due mesi nel caso di accesso come Amministratori di Sistema) senza utilizzare password già impiegate ed attenendosi strettamente ai requisiti di robustezza indicati in precedenza. La password dovrà essere immediatamente modificata nel caso in cui si sospetti che la stessa sia stata violata, comunicando l'anomalia alla S.C. Sistemi Informativi e Ufficio Flussi.

Le uniche eccezioni che consentono l'utilizzo di utenze generiche di reparto e non nominali per l'accesso al dominio sono riservate per quei servizi/reparti le cui attività rivestono carattere di urgenza (nel caso solamente Laboratorio Analisi, DEA, Monitor Medicali di Rianimazione) comunque bloccate solamente su determinate PDL individuate e dove l'accesso alle procedure dipartimentali avviene comunque con utenze nominali riconducibili alle persone fisiche assegnatarie.

Alcune procedure sono accessibili anche dall'esterno della rete aziendale. Per tali procedure (posta elettronica, VPN, aree di lavoro Share Point) è stato attivato l'accesso condizionale che prevede una procedura di autenticazione multi-fattore qualora il tentativo di accesso non provenga da un dispositivo connesso alla rete aziendale.

L'autenticazione multi-fattore (MFA) impone all'utente che tenta l'accesso, oltre all'inserimento della password, anche la dimostrazione di essere in possesso di un dispositivo registrato con l'inserimento di un codice (OTP o un authentication code) ricevuto sullo stesso.

La registrazione del dispositivo consente anche il recupero in autonomia della password da parte dell'utente nel caso di smarrimento o scadenza della stessa. Qualora la password venisse dimenticata e l'utente non avesse eseguito la registrazione del dispositivo di recupero, si procederà alla sua sostituzione d'intesa con il personale della S.C. Sistemi Informativi e Ufficio Flussi che provvederà, in seguito alla segnalazione, a fornire direttamente all'interessato le nuove credenziali di autenticazione dopo identificazione dello stesso; resta inteso che sarà cura dell'utente modificare la password al primo accesso.

Utilizzo firma digitale

I Responsabili di struttura possono richiedere, per motivate esigenze operative, il rilascio di certificati di firma remota per i propri collaboratori (firma digitale).

Le firme digitali vengono utilizzate come sistema di sicurezza informatico allo scopo di firmare digitalmente un documento elettronico affinché abbia validità legale al pari di un testo autografato a mano.

L'utilizzo della firma digitale è sempre riconducibile al titolare, salvo che questi ne dia prova contraria.

La generazione e l'emissione di un nuovo certificato di firma può richiedere un tempo variabile da 2 a 4 giorni (InfoCert S.p.a.) dopo l'invio di tutta la documentazione alla S.C. Sistemi Informativi e Ufficio Flussi o alla S.C. Amministrazione del Personale.

Per evitare disservizi legati alla scadenza dei certificati è automatizzata la procedura per il rinnovo, il sistema invia una notifica via email al dipendente almeno 90 giorni prima della scadenza con le istruzioni necessarie per procedere al rinnovo in autonomia. E' onere del dipendente procedere al rinnovo della firma digitale prima della scadenza, per evitare la disabilitazione e dover rifare il processo di emissione (che comporta costi aggiuntivi all'Azienda)

È obbligo del titolare:

• utilizzare personalmente il certificato di firma;

• custodire i codici di accesso (PIN e PUK) e non comunicarli a nessuno;

Utilizzo della rete fisica locale (LAN)

La rete fisica (LAN – Local Area Network) si basa sul protocollo TCP/IP ed è una risorsa strategica per l'Azienda in quanto interconnette non più solo i dispositivi informatici tradizionali come i PC desktop, i PC portatili, i telefoni IP con i server e i centralini telefonici ma anche una moltitudine di altri device che vanno dai dispositivi elettromedicali quali diagnostiche, analizzatori, monitor di dati vitali, agli impianti tecnologici di video sorveglianza e di building automation, ai dispositivi cosiddetti IoT (Internet of Things), veicolando i dati conservati negli archivi centrali e consentendo la comunicazione dei dispositivi interni con la rete Internet.

Funge da mezzo di trasporto per diversi tipi di informazioni e pertanto, ogni disservizio o sua interruzione, comporta notevoli disagi per l'operatività dell'Azienda medesima. Tutte le postazioni di lavoro operano interconnesse alla rete aziendale e possono così accedere ai dati e alle risorse aziendali secondo prestabilite regole di abilitazione.

La rete aziendale interna non può esser utilizzata per scopi diversi da quelli per i quali è destinata. Il dipendente che si rende conto che nella rete interna circolano dati, notizie ed informazioni non pertinenti l'attività lavorativa o che possono essere riconducibili ad illecito è tenuto ad informare immediatamente il proprio responsabile e la S.C. Sistemi Informativi e Ufficio Flussi.

La configurazione e la gestione di tutti gli apparati attivi e dell'infrastruttura di collegamento sono a carico della S.C. Sistemi Informativi e Ufficio Flussi.

Non è consentita la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, impianti wireless, ecc.). Un eventuale uso di tali apparati, qualora necessario, dovrà essere richiesto alla S.C. Sistemi Informativi e Ufficio Flussi e ricevere autorizzazione dalle Direzioni competenti. Analogamente non è ammesso, se non per esigenze estemporanee e previa autorizzazione della struttura S.C. Sistemi Informativi e Ufficio Flussi, l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub/switch).

Viene fatto esplicito e tassativo divieto di connettere in rete postazioni di lavoro ed ogni altro dispositivo informatico (es. computer e portatili non aziendali). Introdurre una macchina con un indirizzo IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti alla rete.

È fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS, DHCP, NTP, mailing, accesso remoto, proxy server.

È fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware. L'utilizzo di tali strumenti è strettamente riservato al personale tecnico afferente alla struttura S.C. Sistemi Informativi e Ufficio Flussi, al fine di monitorare le prestazioni della rete aziendale.

Nel caso si riscontrasse la presenza di PC che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del personale della struttura S.C. Sistemi Informativi e Ufficio Flussi procedere al blocco, se necessario, dell'attività di rete della postazione.

È fatto divieto di svolgere attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti.

Non è consentito l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto. Non è consentito depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio.

Utilizzo della rete Wireless (WLAN)

L’infrastruttura Wireless aziendale è implementata tramite Access Point gestiti centralmente dalla S.C. Sistemi Informativi e Ufficio Flussi.

Gli Access Point distribuiscono **due SSID distinti**, configurati come estensione diretta della rete LAN cablata:

1. **TO4-Medicali** – dedicato ai dispositivi elettromedicali autorizzati.
2. **TO4-PC**– dedicato ai Personal Computer aziendali membri del dominio.

I client connessi ereditano le stesse policy e autorizzazioni dei dispositivi collegati alla LAN cablata, inclusi accesso alle risorse interne, servizi di rete e criteri di sicurezza.

L’accesso ai SSID aziendali è consentito esclusivamente ai PC aziendali configurati secondo i seguenti requisiti obbligatori:

- **Dominio**: il PC deve essere correttamente inserito nel dominio **ASLCANAVESE**.
- **Protezione**: il PC deve avere installato e attivo l’antivirus aziendale.
- **Provisioning iniziale**: il primo collegamento alla rete WiFi deve essere effettuato dal personale della S.C. Sistemi Informativi e Ufficio Flussi, al fine di:
    - installare i certificati digitali necessari all’autenticazione;
    - verificare la conformità del dispositivo alle policy aziendali;
    - registrare il device nella piattaforma di gestione della WLAN.

Entrambe le reti WiFi risultano a tutti gli effetti un’estensione della rete LAN, pertanto, i client connessi, avranno la possibilità di accedere alle medesime risorse della rete locale cablata. La tecnologia è configurata e governata dalla S.C. Sistemi Informativi e Ufficio Flussi, la quale dispone il rilascio delle abilitazioni alle reti.

È **tassativamente vietato** connettere alla rete WiFi aziendale qualsiasi dispositivo non preventivamente configurato e autorizzato dalla S.C. Sistemi Informativi e Ufficio Flussi, in particolare:

- smartphone personali;
- tablet o notebook personali;
- dispositivi non conformi agli standard di sicurezza aziendali;
- Access Point non autorizzati.

Ogni violazione costituisce incidente di sicurezza e può comportare la sospensione immediata dell'accesso alla rete.

Internet

Il computer aziendale abilitato alla connessione Internet è da considerarsi uno strumento essenziale per lo svolgimento delle attività lavorative e formative. Di conseguenza, è espressamente vietato accedere a siti web il cui contenuto non sia strettamente correlato all'attività professionale.

L'abilitazione alla navigazione è assegnata a livello di macchina è configurato specificamente per ciascun dispositivo e non per singoli utenti.

È attivo un sistema di protezione automatica che filtra il traffico Internet per categorie di contenuti ed è inoltre presente una funzionalità per la gestione di blacklist specifiche, che consente il blocco mirato di URL non conformi.

Restrizioni tecniche

- È vietata la connessione autonoma alla rete Internet tramite modem, router, hotspot o altri dispositivi di connettività non autorizzati.
- Non è consentito effettuare download o upload di file o software da siti Internet che comportino l'accesso abusivo a sistemi informatici protetti da misure di sicurezza.
- È altresì vietata la permanenza non autorizzata in sistemi informatici, servizi applicativi o ambienti digitali contro la volontà espressa o implicita dell'Azienda.

Responsabilità e sicurezza

- Ogni file o software scaricato da Internet è sotto la responsabilità esclusiva del dipendente.
- Prima di procedere al download, è obbligatorio effettuare una verifica antivirus per tutelare l'integrità del patrimonio informatico aziendale.
- Qualora il dipendente non sia in grado di eseguire autonomamente tale controllo, è tenuto a contattare la S.C. Sistemi Informativi e Ufficio Flussi.

Servizi e comportamenti vietati

- È vietato l'utilizzo di servizi di messaggistica istantanea, salvo quelli espressamente autorizzati dall'Azienda né programmi di condivisione file (file sharing) o software basati su tecnologie P2P (peer-to-peer).

- È rigorosamente vietata la registrazione e partecipazione a forum non professionali, chatline, social network, bacheche elettroniche e guest books, anche sotto pseudonimo, salvo esplicita autorizzazione aziendale.
- È assolutamente proibita qualsiasi attività riconducibile a hackeraggio, pirateria informatica o violazione dei sistemi digitali.

Monitoraggio e tracciamento

ASL TO4 si riserva il diritto di bloccare l'accesso a siti non pertinenti all'attività lavorativa e di tracciare tutte le attività di navigazione effettuate all'interno della rete aziendale (URL/domini, timestamp, indirizzi IP), al fine di garantire la sicurezza e il rispetto delle normative vigenti. Tali dati verranno per la durata di 30 giorni. Le finalità per il trattamento dei dati raccolti sono le seguenti:

Sicurezza informatica della rete e dei sistemi

Per garantire integrità, disponibilità e protezione dell'infrastruttura IT, prevenendo malware, attacchi informatici, accessi non autorizzati e incidenti di sicurezza.

Corretta erogazione dei servizi istituzionali

La navigazione Internet è uno **strumento di lavoro**, e il controllo tecnico serve ad assicurarne l'utilizzo adeguato nell'ambito dei compiti istituzionali.

Gestione, manutenzione e funzionamento tecnico dei sistemi

I sistemi di filtraggio e logging (es. proxy, firewall) raccolgono dati **necessari al funzionamento** dell'infrastruttura e alla diagnosi di anomalie.

Prevenzione e contrasto di utilizzi impropri degli strumenti di lavoro

Finalità organizzativa e di tutela dell'ente contro abusi, violazioni di policy, comportamenti che possano danneggiare l'amministrazione.

Tutela del patrimonio pubblico (controlli difensivi)

Solo quando vi siano **indizi concreti** di comportamenti illeciti (es. violazioni di sicurezza, divulgazione di dati, attività estranee all'impiego con impatto significativo).

Adempimento a obblighi normativi

Ad esempio obblighi previsti dal Codice dell'Amministrazione Digitale, norme sulla sicurezza IT, misure minime AgID, obblighi di protezione dei dati personali. (Principio di sicurezza del GDPR e Codice Privacy)

Monitoraggio e controlli

Le attività sull'uso del servizio di accesso a internet sono automaticamente registrate in files di LOG, che riportano i dettagli della navigazione, i siti e i documenti consultati.

Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima e/o aggregata (riferita alla singola Struttura).

I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

I dati anonimi e/o aggregati sono disponibili agli Amministratori di sistema del S.I.A. e/o dai fornitori esterni che svolgono l'attività per l'ASL TO4.

I dati personali contenuti nei LOG possono essere trattati esclusivamente nei seguenti casi:

- per rispondere ad eventuali richieste dell'autorità giudiziaria o della polizia giudiziaria;
- su richiesta della Direzione Generale qualora si verifichi un evento dannoso o di pericolo che richieda un immediato intervento;
- su richiesta della Direzione Generale qualora si verifichi un utilizzo anomalo degli strumenti da parte degli utenti di una specifica Struttura;
- qualora vi sia l'evidenza o comunque il fondato sospetto che sia in corso o sia stato posto in essere un illecito.

Il sistema informatico è programmato e configurato per cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico la cui conservazione non sia necessaria. Verranno prolungati i tempi di conservazione (limitatamente, comunque, alle sole informazioni indispensabili per perseguire finalità preventivamente determinate) solo in caso di:

- esigenze tecniche o di sicurezza specifiche;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o conservare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Qualora le misure tecniche preventive non siano sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Azienda effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intera Azienda o a sue Strutture e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro o su base individuale.

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.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile procedere con un'analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Programmi Gestionali

È possibile ottenere l'assegnazione di credenziali di autenticazione per l'utilizzo di programmi gestionali, inserendo specifiche richieste sul sistema autorizzativo aziendale CredNET, da parte del Responsabile del Servizio o del suo delegato.

Se è nota la data di scadenza del rapporto sottostante la necessità di rilascio delle credenziali, va inserita già in fase di richiesta in modo che, al superamento della stessa, le credenziali vengano automaticamente revocate.

L'intero ciclo di vita delle credenziali utente è gestito mediante la piattaforma CredNET, comprese le modifiche per spostamento di servizi del dipendente.

Tutte le credenziali sono comunque revocate con la cessazione del rapporto di lavoro.

VPN (Accesso alle risorse interne all'Azienda dall'esterno della rete)

Come per l'email ("Regolamento Aziendale Email" approvato con delibera n. 667 del 12/09/2024) anche l'utilizzo delle VPN è protetto tramite l'autenticazione a più fattori, che è un metodo di autenticazione che si basa sull'utilizzo congiunto di più metodi di autenticazione indipendenti. Questo è legato al concetto di out of band authentication: l'uso di più canali per autenticarsi verso un asset in modo da garantire la sicurezza all'accesso da dispositivi collegati all'esterno della rete aziendale. Per fare un esempio di autenticazione a due fattori basti pensare al metodo di accesso al conto corrente: vengono sfruttati un ID utente, una password e una one-time password (OTP), cioè un codice usabile una volta sola generatosi attraverso un token. Un'autenticazione a due fattori viene detta "autenticazione forte" (strong authentication) mentre l'uso di un solo fattore, come una password, viene considerato un'autenticazione debole.

L'accesso in VPN è nominale e le relative credenziali sono pertanto assegnate a persone fisiche (dipendenti o fornitori esterni) chiaramente identificate. Ogni VPN rilasciata è configurata in modo da consentire solamente la raggiungibilità delle risorse effettivamente necessarie al richiedente.

È compito della S.C. Sistemi Informativi in collaborazione con Leonardo s.p.a. definire la configurazione delle stesse.

Il rilascio delle credenziali per l'accesso in VPN avviene a seguito dell'inserimento di specifica richiesta sul sistema aziendale CredNET da parte del Responsabile del Servizio o suo delegato evidenziando per ogni singolo utente le risorse/servizi informatici aziendali da dover raggiungere.

Con la cessazione del rapporto di lavoro degli utenti le credenziali di accesso in VPN vengono revocate.

Controllo remoto per manutenzioni IT e accesso degli utenti esterni

Per facilitare e rendere maggiormente tempestive le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, i tecnici informatici possono avvalersi di strumenti di controllo remoto che consentano di compiere le necessarie operazioni attraverso la rete locale o comunque un collegamento protetto.

La connessione da e verso i sistemi avviene attraverso protocolli dotati di meccanismi che garantiscono nativamente sicurezza o protezione della connessione stessa (ad es. RDP, SSH e HTTPS) utilizzando canali sicuri o reti interne.

Eventuali specifiche situazioni di impossibilità di utilizzo del protocollo crittografato sono gestite puntualmente attraverso una valutazione del rischio.

Sui dispositivi informatici aziendali è di norma installato un componente di accesso remoto configurato in modo che, nel caso sia necessario interagire con la sessione utente, sia l'Utente stesso ad autorizzare l'intervento del personale tecnico accettandone la connessione. La durata del collegamento è limitata al tempo strettamente necessario per l'esecuzione e la verifica dell'intervento effettuato.

L'Amministratore del Sistema, per l'espletamento delle sue funzioni (ad esempio il salvataggio e il ripristino degli archivi, la tutela della sicurezza informatica, ecc.) ha la facoltà di accedere, nel rispetto della normativa vigente, ai dati trattati da ciascun utente.

L'Amministratore del Sistema può altresì, in qualunque momento, procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza.

I fornitori che, a fini manutentivi o correttivi, devono accedere da remoto agli applicativi o ai server in loro manutenzione, possono farlo solamente in VPN con modalità di autenticazione multi-fattore. I Firewall perimetrali e interni davanti ai datacenter, garantiscono la visibilità per questo tipo di accessi, delle sole risorse necessarie e concordate con la S.C. Sistemi Informativi e Ufficio Flussi.

L'abilitazione e le credenziali di accesso vengono forniti dal personale della struttura S.C. Sistemi Informativi e Ufficio Flussi, a seguito di richiesta di VPN sul Sistema CredNET. Le utenze sono nominali ed inserite sull'albero di Active Directory in unità organizzative (OU) preposte.

È fatto divieto l'utilizzo di altre modalità di collegamento diverse dalla VPN Aziendale.

Misure di sicurezza in modalità di Lavoro Agile

Con delibera numero 79 del 29.01.2026 l'ASL TO4 ha deliberato le modalità e le regole organizzative di svolgimento del Lavoro Agile.

Ogni utente coinvolto nell'attività di Lavoro Agile è vincolato ad applicare le norme descritte nel regolamento deliberato. Il dipendente è responsabile della sicurezza dei dati. Il Lavoro Agile, per i rischi maggiori che lo stesso comporta, richiede una maggiore attenzione agli utenti, i quali dovranno attenersi scrupolosamente alle istruzioni impartite. Il materiale informatico per permettere questa attività è a carico del dipendente e non con strumenti di proprietà ASL TO4.

La S.C. Sistemi Informativi e Ufficio Flussi, competente in materia di sistemi informativi, supporta il servizio di assistenza agli utenti, avvalendosi di personale specializzato, sia esso personale dipendente dell'azienda stessa, che personale esterno in outsourcing. L'accesso al Lavoro Agile può avvenire solamente per gli utenti autorizzati dall'Azienda e dietro richiesta di credenziali VPN sul sistema CredNET.

Al dipendente vengono fornite le credenziali per accedere da remoto alla rete aziendale in VPN a doppio fattore, l'utente dovrà solamente registrare sul proprio profilo (qualora non lo avesse fatto per la registrazione della mail aziendale) il cellulare per la connessione a doppio fattore. Una volta configurata la VPN l'utente lavora a tutti gli effetti come se fosse in presenza.

L'accesso in VPN è consentito solo tramite dispositivi compliance alle politiche aziendali:

- Sistema Operativo Windows 10/11 Pro con aggiornamento alle ultime patch di sicurezza;
- Antivirus installato e aggiornato alle ultime firme;
- Connessione Internet stabile e privata (non connessioni WiFi pubbliche).

Il dipendente dovrà applicare quanto già previsto in ambito di sicurezza informatica nel presente regolamento informatico aziendale.

Le prescrizioni del presente documento si applicano ai dipendenti aziendali coinvolti nell'espletamento dell'attività lavorativa in modalità Lavoro Agile.

L'Azienda si riserva di effettuare verifiche sul corretto utilizzo degli strumenti informatici.

La violazione da parte degli utenti delle norme contenute nel presente documento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

In caso di smarrimento e/o il furto di un Desktop e/o portatile, è necessario segnalarlo in maniera tempestiva alla S.C. Sistemi Informativi e Ufficio Flussi in quanto sarà necessario provvedere al blocco della connessione VPN.

Non osservanza della normativa aziendale

Le disposizioni di cui al presente regolamento rivestono carattere di obbligatorietà e la loro non osservanza costituisce illecito che, quando rilevato, può portare all'instaurazione di procedimenti disciplinari a carico dell'utilizzatore che lo ha posto in essere e, ricorrendone gli estremi, alla segnalazione dello stesso alle autorità competenti.