Stato	Versione
Data di approvazione 03/06/2026	N. 1.0

Nome e Cognome	Verificato ed approvato	Firma
MASSIMO DEL RE		

1. PREMESSA E AMBITO DI APPLICAZIONE

Gli strumenti informatici rappresentano da un lato un mezzo insostituibile di lavoro, se adoperati nel rispetto del principio della diligenza e correttezza, e dall'altro lato un rischio per la sicurezza del patrimonio aziendale, qualora utilizzati in modo non idoneo.

Si rende pertanto necessaria l'adozione da parte di ASF SAN GIULIANO MILANESE del presente Regolamento aziendale finalizzato a disciplinare il regolare utilizzo dei predetti strumenti, con particolare riferimento alle seguenti problematiche:

- utilizzo del computer (fisso e portatile)
- gestione delle credenziali
- utilizzo della rete (aziendale e internet)
- utilizzo della posta elettronica
- dispositivi rimovibili
- protezione, salvataggio e resilienza dei dati
- gestione incidenti
- controlli, inosservanza e sanzioni

Le disposizioni di seguito devono essere conosciute ed applicate dai soggetti autorizzati che accedono agli strumenti informatici aziendali e/o connessi al perseguimento di finalità aziendali.

2. UTILIZZO DEL COMPUTER

Questo capitolo definisce le norme comportamentali per l'uso dei dispositivi hardware forniti dall'Azienda, intesi come "endpoint" critici per la sicurezza della rete e la continuità dei servizi di ASF San Giuliano Milanese.

2.1. FINALITA' E NATURA DELLO STRUMENTO

Il computer (fisso o portatile) è uno strumento di lavoro assegnato esclusivamente per perseguire finalità aziendali e/o previste dalla legge.

L'utente è tenuto a utilizzarlo nel rispetto dei principi di correttezza, diligenza e buona fede, in linea con le direttive sulla sicurezza informatica.

2.2. INTEGRITA' DEL SISTEMA

Le caratteristiche hardware e le configurazioni software (inclusi sistemi operativi e agenti di sicurezza) sono impostate dal Sistema Informatico e non possono essere modificate, manomesse o disabilitate dall'utente.

È severamente vietata l'installazione di software, applicazioni o estensioni del browser non preventivamente autorizzati dal Sistema Informatico.

È vietato l'utilizzo di strumenti informatici non censiti (es. storage cloud personali, software di telecontrollo non autorizzati o servizi di messaggistica non aziendali) per il trattamento o il trasferimento di dati professionali.

Il Sistema Informatico ha la facoltà di rimuovere file, applicazioni o configurazioni ritenute pericolose per la sicurezza o la conformità del perimetro aziendale.

La gestione locale dei dati (salvataggio su Desktop o cartelle locali "C:") deve essere evitata a favore della memorizzazione centralizzata su server aziendali o aree cloud autorizzate, onde garantire la disponibilità del dato e l'efficacia dei sistemi di backup.

2.3. SICUREZZA FISICA E VIGILANZA

È vietato l'uso di supporti rimovibili (chiavette USB, hard disk esterni) per la memorizzazione di dati particolari o giudiziari. L'uso di tali supporti per altre finalità è consentito solo previa scansione antivirus obbligatoria.

L'utente deve vigilare costantemente affinché i dati contenuti nel dispositivo non siano oggetto di accesso non autorizzato da parte di terzi.

Alla fine della giornata lavorativa è necessario spegnere completamente il computer e tutti gli asservimenti ad esso collegati.

In pausa pranzo e in ogni caso di allontanamento dalla postazione, è obbligatorio attivare la modalità "Blocca computer".

Al termine della giornata lavorativa, il computer e le periferiche collegate devono essere spenti completamente per ridurre rischi elettrici e consentire il completamento dei cicli di aggiornamento automatici.

È responsabilità dell'utente provvedere alla cancellazione periodica di file obsoleti o inutili per mantenere l'efficienza del sistema.

2.4. SPECIFICHE PER I DISPOSITIVI PORTATILI E CONNETTIVITA'

L'utente è custode responsabile del computer portatile assegnatogli e deve proteggerlo con la massima diligenza sia durante l'utilizzo che durante gli spostamenti.

Il dispositivo deve essere costantemente presidiato o riposto in un luogo sicuro e non visibile dall'esterno.

È vietato l'utilizzo di abbonamenti internet privati o reti Wi-Fi pubbliche non protette per effettuare collegamenti alla rete aziendale, se non attraverso l'uso di sistemi di cifratura (VPN) autorizzati.

È severamente vietata la riproduzione o la duplicazione di programmi informatici in violazione delle leggi antipirateria.

3. GESTIONE DELLE IDENTITA' E DELLE CREDENZIALI

Il presente capitolo definisce le modalità di gestione delle credenziali per l'accesso alla rete, ai software e ai servizi cloud di ASF San Giuliano Milanese, al fine di garantire l'integrità e la riservatezza delle informazioni aziendali.

3.1. IDENTIFICAZIONE E PROFILAZIONE

L'accesso alla rete e ai sistemi aziendali è consentito esclusivamente tramite il profilo personale configurato e autorizzato dal Sistema Informatico.

Le credenziali di autenticazione (quali username, password, smart card, token biometrici) sono personali, segrete, non cedibili e di uso esclusivo dell'utente a cui sono assegnate.

È severamente vietato l'utilizzo di account condivisi o "di gruppo" per lo svolgimento delle attività lavorative, salvo casi eccezionali esplicitamente autorizzati e tracciati dal Sistema Informatico.

3.2. REQUISITI DI ROBUSTEZZA DELLE PASSWORD

L'utente deve creare password (o *passphrase*) prive di riferimenti banali o riconducibili alla propria sfera privata (es. nome, data di nascita, nomi di familiari).

Le password devono avere una lunghezza minima di 12 caratteri e includere una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali.

È vietato il riutilizzo di password precedentemente utilizzate per l'account aziendale o l'impiego di password già usate per account personali esterni (es. social network, e-mail privata).

L'autenticazione a due o più fattori (MFA) è obbligatoria per l'accesso a tutti i servizi aziendali esposti su internet (es. posta elettronica, VPN, portali HR) e per tutti gli account dotati di privilegi amministrativi.
L'utente è tenuto a custodire con la massima cura il secondo fattore di autenticazione (sia esso un codice ricevuto via app, una chiave fisica o un SMS) e a segnalarne immediatamente lo smarrimento.

3.3. CICLO DI VITA DELLE CREDENZIALI

L'utente deve modificare la password assegnata al primo utilizzo.
La password deve essere cambiata immediatamente qualora l'utente reputi che la stessa abbia perso la necessaria caratteristica di segretezza o in caso di segnalazione di compromissione da parte del Sistema Informatico.
La rotazione periodica della password (almeno ogni 3 o 6 mesi) resta obbligatoria esclusivamente per gli utenti autorizzati al trattamento di dati particolari o giudiziari e per gli amministratori di sistema.

3.4. OBBLIGHI DI CUSTODIA E SEGRETEZZA

L'utente deve adottare ogni cautela per assicurare la segretezza della password.
È tassativamente vietato:

- Scrivere le password su fogli, promemoria o post-it applicati al computer o conservati in luoghi accessibili.
- Salvare le password all'interno di file di testo non protetti o in funzioni di compilazione automatica del browser non autorizzate.
- Comunicare le proprie credenziali a colleghi, superiori o presunti tecnici del supporto informatico (pratica del *vishing*/phishing).

In caso di sospetta compromissione, la password deve essere sostituita immediatamente previa comunicazione al Sistema Informatico.

4. UTILIZZO DELLA RETE E NAVIGAZIONE IN INTERNET

Il presente capitolo disciplina l'accesso alla rete locale (LAN), alla rete Wi-Fi aziendale e alla rete esterna Internet, con l'obiettivo di garantire la protezione dell'infrastruttura di ASF San Giuliano Milanese contro attacchi informatici e intrusioni.

4.1. PRINCIPI GENERALI DI UTILIZZO

L'accesso alla rete è consentito esclusivamente per il perseguimento delle finalità istituzionali e lavorative dell'Azienda, nel rispetto dei principi di correttezza e diligenza.
L'utilizzo della rete internet attraverso le infrastrutture aziendali è finalizzato esclusivamente a ragioni di ufficio, quali studio, ricerca, documentazione e aggiornamento professionale.
L'uso della rete per scopi privati è vietato, salvo casi eccezionali e per comunicazioni di entità trascurabile, sempre nel rispetto dei massimi criteri di sicurezza.

4.2. RESTRIZIONI E DIVIETI OPERATIVI

È severamente vietato connettere alla rete aziendale postazioni di lavoro, dispositivi personali o apparecchiature hardware (es. router, switch, access point) senza la preventiva autorizzazione scritta del Sistema Informatico.
È vietata l'installazione di modem o dispositivi di comunicazione non autorizzati che possano creare punti di accesso non protetti verso l'esterno.

È vietato l'utilizzo della rete per attività ludiche, partecipazione a forum, chat-line o bacheche elettroniche non strettamente necessarie all'attività lavorativa.
È tassativamente vietato scaricare programmi, file eseguibili o software da siti internet, se non previa autorizzazione del Sistema Informatico e successiva verifica di sicurezza.

4.3. SICUREZZA
Non è consentita la visualizzazione, la memorizzazione o la diffusione di materiale di natura oltraggiosa, minacciosa, offensiva, oscena o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinioni e appartenenza politica.
È vietato l'accesso a siti che violino il diritto d'autore o che promuovano attività illecite.
L'utente non può utilizzare servizi di archiviazione cloud (es. Dropbox, Google Drive personale, WeTransfer) o strumenti di produttività online non approvati ufficialmente dall'Azienda per il trattamento di documenti e dati aziendali.
È vietato l'uso di "Shadow IT" (software o servizi web-based non censiti) per evitare la creazione di vulnerabilità non monitorate lungo la catena di approvvigionamento digitale.
Al fine di garantire la sicurezza del patrimonio informativo e la protezione contro i malware, l'Azienda implementa sistemi di filtraggio DNS e web-filtering.
L'Azienda si riserva la facoltà di bloccare l'accesso a categorie di siti ritenuti a rischio (es. siti di file sharing, siti compromessi, categorie non inerenti al lavoro) o di limitare la banda per determinate applicazioni.
Tali misure sono adottate esclusivamente per finalità di sicurezza informatica e protezione della rete, in conformità con quanto previsto dal Garante Privacy e dallo Statuto dei Lavoratori.
L'utente è tenuto a segnalare tempestivamente al Sistema Informatico ogni comportamento anomalo della rete (es. estrema lentezza, comparsa di pop-up sospetti, reindirizzamenti automatici su siti non richiesti), in quanto possibili indicatori di un incidente di sicurezza in corso.

4.4. CONNESSIONI REMOTE E RETI ESTERNE
L'accesso alla rete aziendale da postazioni remote (smart working) deve avvenire esclusivamente tramite canali cifrati (VPN aziendale) e con l'ausilio di sistemi di autenticazione forte (MFA).
È vietata la navigazione su siti sensibili o l'accesso ad applicativi aziendali critici quando si è connessi a reti Wi-Fi pubbliche o non protette, a meno che non sia attiva la VPN aziendale.

5. UTILIZZO DELLA POSTA ELETTRONICA
La casella di posta elettronica assegnata dall'Azienda è uno strumento di lavoro di cui l'utente è titolare e responsabile. Il suo utilizzo deve essere improntato alla massima prudenza per prevenire la diffusione di malware e la compromissione del patrimonio informativo aziendale.

5.1. ABILITAZIONE E ACCESSO
L'abilitazione alla posta elettronica deve essere richiesta dal Responsabile di funzione al Sistema Informatico.
Ciascuna casella è protetta da una password che l'utente deve modificare al primo accesso. La gestione, la segretezza e la modifica periodica della stessa sono sotto la completa responsabilità dell'utente, come specificato nel Capitolo 2.

È consentito consultare la posta aziendale esclusivamente tramite il sistema ufficiale di ASF San Giuliano Milanese e solo su dispositivi mobili autorizzati dall'Azienda.

5.2. SICUREZZA E PREVENZIONE

L'utente deve prestare massima attenzione a messaggi provenienti da mittenti sconosciuti o con contenuti insoliti (es. richieste urgenti di bonifici, reset password non richiesti). Tali messaggi devono essere cancellati senza essere aperti.

È tassativamente vietato aprire allegati sospetti, con particolare riferimento a file eseguibili o script (es. .exe, .scr, .pif, .bat, .cmd), anche se provenienti da mittenti apparentemente conosciuti.

Prima dell'utilizzo o del salvataggio, ogni allegato deve essere controllato dal sistema antivirus aziendale.

L'utente è considerato direttamente responsabile per eventuali danni alla rete aziendale causati dall'introduzione di virus informatici dovuti all'inosservanza di tali regole.

Ogni tentativo di phishing o messaggio sospetto deve essere segnalato immediatamente al Sistema Informatico come "potenziale incidente di sicurezza", per consentire l'adozione di contromisure a livello di rete (es. blocco del mittente a livello centralizzato).

5.3. COMUNICAZIONI VERSO L'ESTERNO

È vietato inviare a soggetti terzi o esterni all'Azienda materiale di proprietà di ASF San Giuliano Milanese senza preventiva autorizzazione.

L'invio di documenti contenenti dati particolari (sensibili) o giudiziari deve avvenire esclusivamente tramite strumenti di trasmissione sicura o file crittografati con password condivisa attraverso un canale secondario.

In caso di invio di allegati voluminosi, l'utente deve utilizzare formati compressi (es. .zip, .jpg) per non sovraccaricare il sistema.

La casella deve essere mantenuta in ordine, eliminando documenti inutili o ingombranti e procedendo all'archiviazione periodica dei messaggi obsoleti.

5.4. RISERVATEZZA E TUTELA DEL LAVORATORE

L'uso della posta elettronica aziendale per finalità strettamente personali è consentito in via eccezionale, a condizione che l'impegno di tempo e le risorse impiegate siano di entità trascurabile e non pregiudichino l'attività lavorativa.

L'Azienda raccomanda di non utilizzare la casella istituzionale per comunicazioni di natura privata che possano contenere dati appartenenti a categorie particolari (es. dati sanitari o sindacali), per i quali l'utente ha un'elevata aspettativa di riservatezza.

È fatto divieto assoluto di procedere alla lettura, registrazione o monitoraggio sistematico e prolungato dei messaggi di posta elettronica o dei relativi dati esterni (log di traffico).

Eventuali verifiche tecniche sui sistemi sono effettuate esclusivamente per garantire la funzionalità e la sicurezza del servizio e, ove possibile, avvengono in forma anonima o aggregata.

Qualora sorga il fondato sospetto di comportamenti illeciti o di minacce alla sicurezza informatica, l'Azienda può disporre verifiche mirate seguendo un criterio di gradualità:

- Controlli Anonimi: Analisi di dati aggregati per rilevare anomalie.
- Avviso Generalizzato: Richiamo collettivo al rispetto delle policy aziendali.
- Controlli Individuali: Solo come extrema ratio, in presenza di specifiche criticità e previo avvertimento dell'interessato (ove non pregiudichi le finalità del controllo), procedendo all'analisi dei log o del contenuto dei messaggi limitatamente a quanto necessario per accertare l'illecito.

Qualsiasi anomalia nei processi di salvataggio automatico o nell'accesso ai file server deve essere segnalata tempestivamente per evitare lacune nella copertura dei backup.

7. GESTIONE DEGLI INCIDENTI E SEGNALAZIONE

Il presente capitolo stabilisce le procedure che ogni utente deve seguire in caso di evento avverso, reale o sospetto, che possa pregiudicare la sicurezza dei sistemi informatici o la continuità operativa di ASF San Giuliano Milanese. Maggiori dettagli sulla gestione degli incidenti informatici sono contenuti nel documento INCIDENT RESPONSE PLAN.

7.1. DEFINIZIONE DI INCIDENTE INFORMATICO

Ai fini del presente regolamento e in conformità alla Direttiva NIS2, si definisce "incidente" qualsiasi evento che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati, o dei servizi offerti. Esempi includono, ma non sono limitati a:

- Anomalie del sistema, smarrimento o furto di informazioni e violazioni di sicurezza.
- Infezioni da malware o ransomware (es. file non più apribili o criptati).
- Smarrimento o furto di dispositivi aziendali (PC, smartphone, token MFA).
- Ricezione di e-mail di phishing mirate o tentativi di accesso non autorizzati.

7.2. OBBLIGO DI SEGNALAZIONE TEMPESTIVA

Ogni dipendente che rilevi o sospetti un incidente informatico ha l'obbligo di informare immediatamente il Titolare e il Sistema Informatico.

La segnalazione deve essere effettuata nel minor tempo possibile dal momento della scoperta. Questo è fondamentale per consentire all'Azienda di adempiere all'obbligo di "Allerta Precoce" (Early Warning) verso le autorità competenti entro 24 ore dall'evento, come previsto dai nuovi protocolli di cybersicurezza.

In caso di violazione che comporti un rischio per i dati personali (Data Breach), resta fermo l'obbligo di notifica al Garante Privacy entro 72 ore.

Nella segnalazione, l'utente deve fornire ogni dettaglio utile alla comprensione dell'accaduto, evitando di intraprendere iniziative autonome (come il riavvio forzato o la cancellazione di file) che potrebbero inquinare le prove digitali.

7.3. ANALISI POST INCIDENTE

Il dipendente si impegna a collaborare pienamente con il Titolare, il DPO e il personale tecnico nelle indagini volte a chiarire le dinamiche dell'incidente.

A seguito di un incidente, l'Azienda potrà effettuare verifiche informatiche e analisi dei file di log per ricostruire l'evento e prevenire future violazioni, agendo nel rispetto della normativa sulla privacy e dello Statuto dei Lavoratori.

I dati raccolti durante queste verifiche saranno trattati esclusivamente per finalità di tutela della sicurezza e del patrimonio aziendale.

La mancata segnalazione di un incidente di cui si è venuti a conoscenza è considerata una violazione del presente regolamento.

L'utente è considerato direttamente responsabile per eventuali aggravamenti del danno alla rete aziendale derivanti dal ritardo o dall'omessa comunicazione del problema.

I dati relativi ai log di traffico e-mail sono conservati per un periodo non superiore a quello strettamente necessario alle finalità di sicurezza e tutela del patrimonio.

5.5. GESTIONE DELLA CASELLA IN CASO DI ASSENZA O CESSAZIONE

- Assenze programmate: il lavoratore deve attivare un sistema di risposta automatica che informi i mittenti dell'assenza e indichi un contatto alternativo, evitando il reindirizzamento automatico (*forward*) dell'intera corrispondenza verso altri soggetti, se non strettamente necessario.
- Assenze improvvise: in casi di improrogabile necessità e solo per finalità di continuità operativa, l'Amministratore di Sistema può accedere alla casella dell'assente per attivare il messaggio di risposta automatica o verificare comunicazioni urgenti, preferibilmente in presenza dell'interessato o di un suo delegato/fiduciario.
- Cessazione del rapporto: alla cessazione del rapporto di lavoro, l'Azienda provvederà alla disattivazione della casella e-mail entro tempi tecnici brevi. Per un periodo limitato di 30 giorni, potrà essere attivo un messaggio automatico che informi della cessazione e fornisca nuovi recapiti aziendali. È vietata la conservazione a tempo indeterminato o l'accesso indiscriminato ai messaggi archiviati dal lavoratore cessato.

6. PROTEZIONE, SALVATAGGIO E RESILIENZA DEI DATI

Il presente capitolo definisce le misure tecniche e organizzative volte a garantire l'integrità, la disponibilità e la resilienza dei dati e dei sistemi informatici di ASF San Giuliano Milanese.

6.1. PROTEZIONE E INTEGRITA' DEI SISTEMI

L'utente deve tenere comportamenti volti a ridurre il rischio di attacchi informatici (es. non cliccare su link sospetti, non inserire dispositivi USB sconosciuti).

È obbligatorio verificare la presenza e il regolare funzionamento del programma antivirus/EDR aziendale. È severamente vietato disabilitare o manomettere tali sistemi di protezione.

L'utente deve consentire i periodici aggiornamenti di sicurezza (*patching*) del sistema operativo e delle applicazioni, riavviando il dispositivo quando richiesto dal Sistema Informatico.

Nel caso in cui il programma di protezione rilevi una minaccia (virus/malware), l'utente deve sospendere ogni attività, non spegnere il computer e segnalare immediatamente l'accaduto al Sistema Informatico.

Ogni dispositivo di archiviazione esterno (USB, hard disk) deve essere verificato mediante il programma antivirus prima di ogni utilizzo.

6.2. SALVATAGGIO DEI DATI

Al fine di garantire la continuità operativa, l'utente è tenuto a memorizzare i documenti di lavoro esclusivamente sulle cartelle di rete condivise (Server) o negli spazi Cloud aziendali autorizzati.

Il salvataggio dei dati (backup) avviene in modo centralizzato e automatizzato secondo le policy definite dal Sistema Informatico. I dati salvati esclusivamente sul disco locale del computer ("Desktop", "Documenti") non sono soggetti a backup aziendale e sono a rischio di perdita definitiva in caso di guasto o attacco.

In conformità con la Direttiva NIS2, l'Azienda adotta un piano di per assicurare il ripristino dei dati e dei sistemi critici entro tempi certi in caso di incidente catastrofico. L'utente è tenuto a collaborare alle eventuali simulazioni di ripristino o test di continuità operativa organizzati dal Sistema Informatico.

8. CONTROLLI, INOSSERVANZA E SANZIONI

Il presente capitolo definisce le modalità con cui ASF San Giuliano Milanese verifica il rispetto delle norme sopra esposte e le conseguenze derivanti dalla loro violazione, garantendo un equilibrio tra sicurezza informatica e diritti dei lavoratori.

8.1. VERIFICA E CONTROLLI

L'Azienda si riserva la facoltà di verificare, per finalità di sicurezza e tutela del patrimonio aziendale, l'utilizzo corretto degli strumenti elettronici, dell'accesso a Internet e della posta elettronica.
Tali verifiche si svolgeranno nel pieno rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dallo Statuto dei Lavoratori e dal Regolamento UE 2016/679 (GDPR).
Qualora dalle analisi aggregate emergano anomalie nel traffico dati o rischi per la sicurezza (es. tentativi di connessione a domini malevoli), l'Amministratore di Sistema invierà un avviso generalizzato richiamando gli utenti al rispetto del regolamento.
Solo in caso di reiterate violazioni o di sospetto di gravi illeciti, l'Azienda potrà restringere il campo di intervento ed effettuare controlli mirati, fino all'analisi dei singoli file di log, nel rispetto delle procedure legali.
Le informazioni raccolte saranno trattate secondo i principi di pertinenza e non eccedenza rispetto alla finalità di tutela della sicurezza.

8.2. INOSSERVANZA E PROVVEDIMENTI

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce illecito disciplinare ed è perseguibile con le sanzioni previste dal CCNL applicato, oltre che con eventuali azioni civili e penali.
L'utente è considerato direttamente responsabile in caso di:

- Accesso illecito a sistemi o dati.
- Appropriazione indebita di materiale aziendale o stampa non autorizzata di documenti riservati.
- Danneggiamento della rete aziendale causato dall'introduzione colposa di virus o malware per inosservanza delle norme di sicurezza.

Resta salvo il diritto dell'Azienda di richiedere il risarcimento per l'eventuale maggior danno subito a causa della condotta del dipendente.

8.3. FORMAZIONE E COLLABORAZIONE

La sicurezza informatica è un obbligo collaborativo: ogni utente è tenuto a segnalare tempestivamente anomalie o violazioni al Sistema Informatico.
La mancata partecipazione ingiustificata alle sessioni di formazione obbligatoria sulla cybersicurezza, previste dalla Direttiva NIS2, potrà essere oggetto di valutazione in sede disciplinare, data l'importanza della consapevolezza del personale nella prevenzione degli attacchi.

9. AGGIORNAMENTO

Il presente Regolamento è soggetto a revisione con frequenza periodica e si inquadra nel più ampio obbligo di sicurezza che l'Azienda adempie al fine di proteggere i dati personali e le informazioni aziendali, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.