REGOLAMENTO GENERALE
DEL CENTRO SERVIZI FORMATIVI SAN GAETANO
PER L'UTILIZZO DEL SISTEMA INFORMATICO

INDICE

PREMESSA

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica del CSF San Gaetano e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.
Premesso quindi che l'utilizzo delle risorse informatiche deve sempre ispirarsi al principio della diligenza e correttezza, il CSF San Gaetano ha adottato un Regolamento interno diretto a:

- delineare un gruppo di principi di comportamento e misure organizzative finalizzate a rafforzare la sicurezza dei trattamenti di dati personali svolti con gli strumenti informatici del CSF;
- evitare che comportamenti non adeguati possano innescare problemi o minacce alle attrezzature nonché alla Sicurezza per quanto riguarda il trattamento dei dati;
- evitare che comportamenti inadeguati o scorretti possano comportare la violazione del diritto d'autore di terzi o di altri diritti di terzi;

1. DEFINIZIONI E RESPONSABILITÀ

TITOLARE: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Il Titolare del Trattamento è la Fondazione San Gaetano – Centro Servizi Formativi (di seguito anche "CSF") rappresentato dal legale rappresentante pro-tempore.

REFERENTE INTERNO AL TRATTAMENTO DEI DATI: il soggetto incaricato dal titolare alla gestione del sistema privacy, alla vigilanza sulla corretta esecuzione dei compiti da parte delle persone autorizzate al trattamento e di valutare l'adeguatezza delle misure organizzative e tecniche.

RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. La Fondazione San Gaetano – Centro Servizi Formativi provvede a incaricare formalmente i Responsabili del Trattamento di cui si avvale con specifico contratto ai sensi dell'art. 28 del Regolamento UE 679/2016.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informatico ha le responsabilità indicate nella lettera di incarico.

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

PERSONA AUTORIZZATA DAL TRATTAMENTO: il soggetto, nominato dal titolare, che tratta i dati personali sotto l'autorità del titolare stesso. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico. Si intende per incaricato anche il docente che utilizza Personal Computer ubicato nelle aule docenti o nelle aule di informatica e destinati solo al docente suddetto per produrre, consultare, controllare e archiviare documenti strettamente legati all'attività didattica e formativa per cui è incaricato.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

PARTICOLARI CATEGORIE DI DATI PERSONALI: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI: i dati personali idonei a rivelare provvedimenti di condanne penali, misure di sicurezza o reati.

2. TITOLARE, RESPONSABILI, INCARICATI

Titolare del trattamento:	La Fondazione rappresentata dal Presidente Longo Mario
Referente interno al trattamento dei dati:	Direttore Gambaretto Attiliano
Responsabile della sicurezza informatica:	Ing. Gambaretto Attiliano
Amministratore di sistema:	Ing. Gambaretto Attiliano
Custode delle password:	Direttore Gambaretto Attiliano

Persone autorizzate al trattamento dei dati: come da tabella sottoriportata.

Elenco del personale incaricato del trattamento dei dati

Nome e cognome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
Tonin Elena	Uffici amministrativi	PC in rete; Armadi Uffici Amministrativi; Scaffalature, cassaforte	Custode delle chiavi degli uffici amministrativi
Gambaretto Attilianole	Sede Centrale	PC in rete; Armadi Sede Centrale;	Custode delle password, custode delle chiavi degli armadi ubicati in sede centrale e delle chiavi per accedere alle varie zone della sede
Gambaretto Attiliano	Uffici amministrativi e Sede Centrale	PC in rete; Server	Responsabile della sicurezza informatica e amministratore di sistema
Avogaro Fernando Doppioclic Informatica	Uffici amministrativi e Sede Centrale	PC in rete; Server	Organizzazione e supervisione delle misure di sicurezza adottate, Responsabile rotazione unità di backup.
Docenti delle varie materie teorico-pratiche	Aula docenti Aula informatica utilizzata	PC in rete	Responsabile della password assegnata

3. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
La stessa password deve essere attivata per l'accesso alla rete e per il collegamento a Internet.
Il custode delle password per l'espletamento delle sue funzioni ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.
Il custode delle password potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere al Titolare del trattamento di accedere ai dati trattati da ogni incaricato, con le modalità fissate dal CSF San Gaetano, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività istituzionale nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato).
Non è consentito installare autonomamente programmi provenienti dall'esterno. L'unica figura autorizzata è il Responsabile della sicurezza informatica e amministratore di sistema.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Responsabile della sicurezza informatica e amministratore di sistema. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre il trasgressore e il CSF San Gaetano a gravi responsabilità civili penali e amministrative in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Responsabile della sicurezza informatica e amministratore di sistema.
Il Personal Computer deve essere sempre spento al termine dell'attività lavorativa. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso; per tale ragione in caso di assenza dalla postazione non per brevissimi periodi deve essere effettuato il logout o impostato il blocco con screensaver e password.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile della sicurezza informatica e amministratore di sistema nel caso in cui vengano rilevati virus.

4. UTILIZZO DELLA RETE DEL CSF SAN GAETANO

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il Responsabile della sicurezza informatica e amministratore di sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

5. GESTIONE DEL NOME UTENTE E DELLA PASSWORD

Le credenziali di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Responsabile della sicurezza informatica e amministratore di sistema.
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di particolari categorie di dati o dati relativi a condanne penale o reati, la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Custode delle password.
La password deve essere formata da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle password, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia alla Direzione e al Responsabile della sicurezza informatica e amministratore di sistema.

6. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (CD, pen-drive) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato.
Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati personali devono essere custoditi in archivi chiusi a chiave.
In caso di smarrimento del supporto deve essere immediatamente avvertito il Referente interno al trattamento dei dati, così come in caso di virus o altri software dannosi.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun utente dovrà contattare l'amministratore e seguire le istruzioni da questo impartite.

7. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal Responsabile della sicurezza informatica e amministratore di sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.
In caso di smarrimento del PC deve essere immediatamente avvertito il Referente interno al trattamento dei dati.

8. USO DELLA POSTA ELETTRONICA

Ciascun utente accede alla posta elettronica sul dominio @fondazionesangaetano.org utilizzando delle credenziali costituite da un nome utente ed una password.
Il Responsabile della sicurezza informatica e amministratore di sistema assegna le credenziali e una casella di posta elettronica ai dipendenti (docenti, amministrativi e ausiliari) e le credenziali e una casella di posta agli allievi frequentanti i corsi triennali di IeFP previo espresso consenso scritto dei genitori.
L'indirizzo di casella di posta istituzionale è il seguente: info@fondazionesangaetano.it
L'indirizzo di casella di posta legale è il seguente: fondazionesangaetano@legalmail.it

Casella di posta elettronica assegnata ai dipendenti

La casella di posta, assegnata dal Responsabile della sicurezza informatica e amministratore di sistema al dipendente, è uno **strumento di lavoro**.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento dì allegati contenenti foto, filmati o brani musicali non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on-line, concorsi, forum, mailing-list, social network, app di messaggistica e archiviazione sul cloud, etc., non legati all'attività lavorativa;
- la partecipazione a catene telematiche (cd. di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
- la registrazione a servizi on-line personali.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il CSF San Gaetano deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127) e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.
Per la trasmissione di file all'interno del CSF San Gaetano è possibile utilizzare la posta elettronica prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Casella di posta assegnata agli allievi frequentanti i corsi triennali di IeFP.

Ciascun allievo accede alla posta elettronica sul dominio @csfsangaetano.it utilizzando delle credenziali costituite da un nome utente ed una password.
Il Responsabile della sicurezza informatica e amministratore di sistema assegna le credenziali e una casella di posta agli allievi previo espresso consenso scritto dei genitori.
Non è consentito:

- utilizzare le caselle di posta elettronica assegnate per scopi personali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti.

9. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

La rete per la didattica è gestita dal dominio CLASSROOMS.LOCAL con classe di indirizzi 192.168.00/24.
La rete amministrativa è gestita dal dominio ASG.LOCAL con classe di indirizzi 192.168.20/24.
E' vietato utilizzare i dispositivi forniti dall'Ente o la rete del CSF per:

- il reperimento o l'elaborazione di documenti non strettamente attinenti all'attività lavorativa.
- Prima di scaricare documenti finalizzati all'attività lavorativa bisognerà effettuare previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venire a tal fine contattato il Responsabile della sicurezza informatica e amministratore di sistema;

- l’effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote bankìng, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione e comunque nel rispetto delle normali procedute di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all’attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), di social network, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati;
- l’accesso a caselle webmail di posta elettronica personale.

Al fine di evitare la navigazione in siti non pertinenti all'attività, il CSF rende peraltro nota l’adozione di uno specifico sistema di blocco o filtro automatico (Firewall) che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti o servizi. Qualora venga bloccato un sito che in realtà debba essere usato a fini lavorativi, previa richiesta al Responsabile della sicurezza informatica e amministratore di sistema, si potrà procedere con il suo sblocco.
Gli eventuali controlli, compiuti dal personale incaricato, potranno avvenire mediante un sistema di controllo dei "file di log" della navigazione svolta, il quale permette di risalire ai siti visitati e alla quantità di traffico effettuata.

10. SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete del CSF San Gaetano tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione e allievi dei vari corsi di formazione professionale limitatamente alle esigenze didattiche e formative previste dalla programmazione di cui è responsabile il docente incaricato.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
Il Responsabile della sicurezza informatica e amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili il Responsabile della sicurezza informatica e amministratore di sistema può proporre al Titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

11. MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

12. UTILIZZO DI PERSONAL COMPUTER E DI DEVICE DI PROPRIETÀ DEL SINGOLO UTENTE

Per lo svolgimento delle attività nell’interesse del CSF, non è consentita la possibilità di utilizzare strumenti informatici personali, fatta eccezione nei seguenti casi:

- Utilizzo dello smartphone per comunicare con il personale del CSF e per accedere alla posta istituzionale;
- Utilizzo del proprio personal computer per la predisposizione di materiale didattico, l’archiviazione e la correzione di esercitazioni/compiti/verifiche, l’effettuazione di esercitazioni, l’accesso alla posta istituzionale.

L’utilizzo nei suddetti casi viene effettuato sotto la responsabilità dell’utente, previo avvertimento alle funzioni competenti del CSF. Nell’utilizzo dei dispositivi propri, per le finalità sopra indicate, l’Fondazione conserverà tuttavia il proprio ruolo di Titolare del Trattamento in relazione ai dati personali eventualmente trattati per conto del CSF ed è pertanto tenuto a formulare le seguenti specifiche prescrizioni al personale autorizzato:

- I dispositivi personali dovranno essere protetti da sistema di autenticazione (es: username/password; codice di accesso) e da misure di sicurezza (antivirus, firewall ecc.). La Direzione potrà verificare la presenza di adeguati sistemi di autenticazione e sicurezza e formulare eventuali prescrizioni;
- I dispositivi personali dovranno essere custoditi con la massima diligenza nella vita quotidiana, contenendo dati trattati sotto la responsabilità dell’Ente. In caso di problematiche quali guasti, smarrimento, furto o altri problemi che impediscano o limitino l’accesso ai dati o ne possano potenzialmente compromettere l’integrità e la sicurezza, sarà necessario avvisare immediatamente la Direzione;
- I dati relativi alle attività del CSF dovranno essere oggetto di backup secondo le modalità definite dalla Direzione;
- Alla cessazione del rapporto con l’Ente, l’utente dovrà riconsegnare alla Direzione copia dei dati e degli archivi presenti sui dispositivi personali relativi a dati personali o informazioni riconducibili all’attività svolta per CSF, provvedendo successivamente all’immediata cancellazione dai propri dispositivi personali. Potrà essere richiesto un impegno scritto a riguardo;
- I dispositivi che accedono alle reti dell’Ente non devono contenere software o altri beni protetti da diritto d’autore privi di licenza o utilizzati in violazione della licenza d’uso.

13. UTILIZZO DELLE FOTOCOPIATRICI

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione.

14. USO DI IMMAGINI, MUSICA, FILMATI

E’ vietato riprodurre nel materiale destinato alla diffusione (materiale didattico e di comunicazione, sito internet, social network ecc.)

fotografie o immagini reperite senza averne acquistato la licenza d'uso o averne riscontrato la liceità dell'utilizzo. In caso di ragionevoli dubbi, il personale dovrà contattare il Responsabile della sicurezza informatica e amministratore di sistema.
E' vietato riprodurre opere cinematografiche o musicali non contenute su supporti originali e contrassegnati dal bollino SIAE.
La riproduzione di video o musica in streaming dalla rete internet può essere effettuata previa verifica della legittimità dell'utilizzo in base alla licenza specifica, che dovrà essere verificata dal soggetto interessato all'utilizzo.

15. FORME DI CONTROLLO
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, tramite il personale o addetti autorizzati, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico di device.
Anche alla luce del potenziale carattere personale dei dati contenuti sui log, verranno adottate tutte le cautele necessarie per evitare di pregiudicare il diritto alla riservatezza del soggetto, nel rispetto delle disposizioni di legge e della normativa in materia di privacy.
Il CSF non utilizza sistemi hardware e software preordinati al controllo a distanza attraverso i quali sia possibile:

- effettuare costantemente ed indiscriminatamente controlli sull'attività lavorativa;
- riprodurre e memorizzare sistematicamente le pagine Web visualizzate;
- utilizzare strumenti di lettura e di registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
- effettuare analisi occulte di dispositivi informatici affidati in uso.

Al fine di tutelare il diritto alla riservatezza dei dati delle persone autorizzate al trattamento, il CSF ha adottato le seguenti misure:

- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni;
- conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

L'eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere luogo solo in relazione a:

- esigenze tecniche, organizzative, produttive, di tutela del patrimonio o di sicurezza del lavoro;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
- controlli saltuari o occasionali per ragioni legittime quali le verifiche sulla funzionalità e sicurezza del sistema attraverso l'analisi dei log che contengono l'indirizzo IP, il tipo di servizio richiesto e la quantità di traffico.

Il CSF applica una graduazione dei controlli. Inizialmente il controllo è diretto a dati aggregati, riferiti all'intera struttura organizzativa o a sue aree, per arrivare eventualmente ad un avviso circoscritto a gruppi di utenti afferenti all'area/settore in cui è stata rilevata l'anomalia. Laddove l'anomalia persista e si possa configurare il rischio di commissione di illeciti (siano essi civili o penali) il controllo potrà essere effettuato su base individuale e potranno essere adottati opportuni provvedimenti contro chiunque trasgredisca il presente regolamento.
Periodicamente potranno essere effettuati controlli sui dispositivi informatici, al fine di prevenire violazioni della legge e del presente regolamento, anche a tutela del diritto d'autore sul software. Nel caso vengano rinvenuti software non autorizzati installati, verranno immediatamente rimossi. L'Ente potrà procedere anche ad una verifica del numero di licenze software presenti al fine di accertare eventuali situazioni di mancanza, nel qual caso provvederanno alla loro integrazione nel tempo più breve possibile, salvo quanto previsto per la rimozione di software non autorizzati.

16. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY
È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza ai sensi del D.Lgs. 196/2003 e GDPR e reg. EU 679/2016

17. NON OSSERVANZA DELLA NORMATIVA AZIENDALE
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

18. AGGIORNAMENTO E REVISIONE
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data 01/09/2022

Il Direttore Gambaretto Attiliano …….

Il Responsabile della sicurezza informatica
e amministratore di sistema Gambaretto Attiliano ……