ASSOCIAZIONE CSV FVG
Ente gestore del Centro Servizi Volontariato
del Friuli Venezia Giulia

Regolamento privacy

Istruzioni e regole di comportamento per il trattamento dei dati personali attraverso l'utilizzo di strumenti informatici

SCOPO E CAMPO DI APPLICAZIONE

1.1 Lo scopo del presente documento è quello di definire un insieme di norme comportamentali cui tutti i dipendenti, i collaboratori ed eventuali terze parti che operano per l'Associazione CSV-FVG devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

1.2 Il Regolamento è realizzato in conformità alle richieste previste dal Regolamento EU 2016/679 (General Data Protection Regulation – GDPR), costituendone la base per le lettere di nomina e incarico e dei Provvedimenti del Garante.

1.3 Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, dirigenti, consulenti esterni nonché a tutti i collaboratori dell'Associazione CSV-FVG a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, ecc.).

1.4 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni individuo in possesso di specifiche credenziali di autenticazione.

1.5 Si esplicita che tutti gli utenti nell'ambito della loro attività e dei loro diritti d'accesso sono nominati, in forma diretta oppure indiretta attraverso le aziende partner, quali "incaricati del trattamento dei dati" nei limiti dei compiti e delle abilitazioni attribuite.

DEFINIZIONI

Nell'ambito di tutte le attività dell'**Associazione CSV-FVG** sono trattati dall'organizzazione due tipologie di dati:

A. DATI PERSONALI
(tutelati ai sensi del GDPR)
B. DATI AZIENDALI

DATI PERSONALI

I **dati personali** sono qualunque informazione relativa a persona fisica identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Si sottolinea l'importanza di comprendere quando un dato è considerato sensibile: a questi dati è infatti garantita una tutela più intensa, per cui sono imposti maggiori obblighi ed oneri nell'effettuare il trattamento e nella loro custodia.

I **dati sensibili** sono i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.
I **dati giudiziari** sono i dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Trattamento che presenta rischi specifici Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
Il **trattamento dei dati personali** corrisponde a qualunque operazione o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati. È quindi indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.
La **comunicazione di dati personali** corrisponde nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

La **diffusione di dati personali** avviene quando viene data conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Titolare del trattamento (Titolare) è l'organizzazione nel suo complesso l'**Associazione CSV-FVG** nella persona del suo Legale Rappresentante (Presidente) che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Responsabile del trattamento è la persona fisica preposta dal Titolare al controllo delle procedure e modalità di trattamento dei dati personali in base alle scelte organizzative.

Amministratore di sistema: è la persona preposta dal Titolare cui spetta la gestione della sicurezza del sistema informatico.

Incaricato del trattamento: è la persona fisica autorizzata a compiere operazioni di trattamento dati in base alle regole definite dall'organizzazione.

DATI AZIENDALI

Tutti i dati e le informazioni aziendali (strutturati o destrutturati, in formato cartaceo o digitale) trattati nell'ambito dell'**Associazione CSV-FVG** rappresentano una proprietà aziendale, patrimonio dell'**Associazione CSV-FVG**.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

Come prescritto anche nella lettera di nomina a responsabile del trattamento dei dati e di designazione ad attenersi alle disposizioni in materia di privacy e di misure di sicurezza, ai sensi dell'art. 32 del GDPR.

GESTIONE DEI LOCALI E DELLE RISORSE FISICHE

I locali e tutte le risorse fisiche dell'**Associazione CSV-FVG** devono essere utilizzate e custodite con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni.

Tutto il personale dipendente e tutti i soggetti terzi che collaborano con l'**Associazione CSV-FVG** aventi accesso ai locali e alle risorse fisiche, devono attenersi alle policy per garantire la sicurezza fisica di aree ed *asset* aziendali.

ACCESSO AGLI UFFICI E ALLE AREE PROTETTE

Uffici. L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso solo a personale espressamente incaricato dal Responsabile di Direzione/Servizio/Area, munito di chiave, in base a precise e motivate esigenze di accedere a tali ambienti, per finalità lavorative.
In qualunque area dell'Associazione CSV-FVG è vietato l'utilizzo di strumenti in grado di effettuare foto/riprese video/audio, a meno che non sia stato preventivamente e formalmente autorizzato dal Titolare rispettivamente Responsabile di Direzione/Servizio/Area .

POSTAZIONI DI LAVORO

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi assegnati.
Scrivania pulita. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti atti riservati (particolari, sensibili, giudiziari, commercialmente sensibili) senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

MISURE FISICHE DI CUSTODIA DEI DOCUMENTI E ATTI CARTACEI

I dati cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi negli armadi posti nel proprio ufficio. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti ed i supporti informatici necessari per lo svolgimento delle mansioni lavorative. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.
Gli archivi di documenti e atti contenenti dati personali sensibili dovranno essere custoditi in armadi chiusi a chiave.
L'eliminazione fisica di ogni documento cartaceo contenete dati e informazioni aziendali e /o personali deve essere effettuata solo utilizzando l'apposito elimina-documenti.

GESTIONE DEI DATI PERSONALI E AZIENDALI

Il trattamento di qualunque dato e informazione deve prevedere da parte del collaboratore incaricato ogni ragionevole misura per assicurare che tali dati e informazioni rimangano tali, come pure tutti i dati elaborati in ordine a quelle informazioni. I dati e le informazioni potranno essere comunicate a terzi parti, esclusivamente nell'ambito delle proprie attività lavorative.
È vietata ogni attività di trattamento di dati e informazioni (comunicazione, modifica, copia, cancellazione, fornitura ad esterni, ecc.) non espressamente autorizzata e concordata con il proprio Responsabile di Direzione/Servizio/Area.
È assolutamente vietato pubblicare in internet (*Social media, forum, chat, blog, siti internet*) dati ed informazioni di carattere aziendale non autorizzate e concordate con il proprio Responsabile di Direzione/Servizio/Area.

È assolutamente vietato il salvataggio di dati e informazioni in sistemi *cloud* (*per esempio Dropbox, Google+, Evernote, ecc.*) non autorizzati dall'Amministratore di sistema. È invece prevista la modalità di salvataggio indicata e autorizzata dall'Amministratore di sistema.
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 aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale (Direzione IT) o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

POSTAZIONE DI LAVORO

Il dispositivo informatico (Personal Computer, Notebook, Tablet, Smartphone) affidato all'utente è uno strumento di lavoro.
Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
Il PC dato in affidamento all'utente permette l'accesso alla rete dell'Associazione CSV-FVG solo attraverso specifiche credenziali di autenticazione.

L'utilizzo del PC e conseguentemente l'accesso ai dati, programmi e risorse informatiche, è consentito nei limiti della propria funzione e dei propri incarichi assegnati, nei limiti del profilo utente assegnato.
È obbligatorio non lasciare incustodito o accessibile lo strumento elettronico assegnato durante la pausa di una sessione di trattamento.
Per questo motivo tutti i PC devono essere bloccati manualmente se lasciati incustoditi e devono inoltre essere dotati di uno *screen saver*, protetto da *password*, ad attivazione automatica al massimo dopo 10 minuti di inattività.
Tutte le postazioni di lavoro sono dotate di *software antivirus*.

GESTIONE DELLE CREDENZIALI DI ACCESSO - PASSWORD

Occorre seguire la seguente policy per la gestione della password:

- utilizzare solamente password che rispettino i criteri di complessità previsti dalla Direzione IT;
- *effettuare* il cambio *password* almeno ogni 3 mesi ovvero anche prima / in qualsiasi momento qualora richiesto dalla Direzione IT;
- evitare di annotare la propria *password* all'interno dell'ufficio, o di conservarla online;

- evitare di comunicare la propria *password* su questionari e/o moduli;

- nel caso qualcuno insista nel cercare di conoscere la propria password contattare il proprio Responsabile di Direzione/Servizio/ Area che provvederà ad informare l'Amministratore di sistema e/o la Direzione;

- fare attenzione a non digitare la propria *password* nel momento in cui ci sono altre persone, nei pressi della postazione di lavoro, che potrebbero osservare tale operazione;
- evitare di utilizzare l'opzione "*ricorda password*" presente in alcuni programmi;

- in caso di dimenticanza e/o ripristino della *password*, dovrà essere inoltrata una richiesta all'Amministratore di sistema.

Nell'ambito della gestione delle credenziali di autenticazione e dei profili utente ricordiamo che è compito dell'Amministratore di sistema:
- verificare periodicamente gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete;
- verificare periodicamente i profili utente al fine di controllare che siano coerenti con le responsabilità assegnate.

ACCESSO ALLA RETE

Per l'accesso alla rete dell'Associazione CSV-FVG ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

È assolutamente proibito connettersi alla rete ed ai sistemi applicativi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
I dischi di rete presenti sui server dell'Associazione CSV-FVG 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 inerente all'attività lavorativa non può essere salvato, nemmeno per brevi periodi, in queste unità.
Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale IT.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali - quali, ad esempio, disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato della Direzione Informatica (IT). La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente. Le informazioni ivi archiviate devono essere esclusivamente quelle necessarie all'attività lavorativa.
Il personale della Direzione Informatica (IT) può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza sia sui PC degli incaricati sia sulle unità di rete; di tale intervento ne è informato l'utente e il Responsabile di Direzione/Servizio/Area.

Al fine di garantire l'accesso alle informazioni aziendali è fatto divieto applicare sistemi di crittografia, codificazione, protezione tramite password o simili ai dati senza autorizzazione del proprio Responsabile di Direzione/Servizio/Area.

SALVATAGGIO DATI

Tutti i dati e le informazioni elaborati durante il lavoro svolto dal dipendente o collaboratore devono essere salvati esclusivamente sulle unità di rete predisposte.
Non è ammissibile un salvataggio su dischi locali; per dati salvati su dischi locali non viene effettuato il backup.

SOFTWARE ANTIVIRUS

La gestione (installazione, aggiornamento, ecc..) del *software antivirus* è di competenza della Direzione IT.

È vietato:

- disabilitare, per qualsiasi motivo, il sistema *antivirus*;
- installare *software antivirus* diverso da quello già installato dall'Amministratore di sistema.

DOWNLOAD E GESTIONE DEL SOFTWARE

Ogni utente deve utilizzare esclusivamente i software di cui dispone l'organizzazione, le cui specifiche tecniche sono fornite dall'Amministratore di sistema, ogni volta che vi sono dei significativi aggiornamenti.
Ogni utente deve:

- evitare di installare software e/o applicativi che non appartengano all'organizzazione;

- controllare metodicamente tutti i files provenienti dall'esterno e adottare le opportune cautele al momento della trasmissione all'esterno di files;
- evitare qualunque utilizzo di hardware e software privato per usi aziendali, salvo esplicita autorizzazione da parte del Responsabile di Direzione/Servizio/Area attraverso richiesta scritta (anche per software in versione demo).

GESTIONE DELLA POSTA ELETTRONICA AZIENDALE

L'assegnazione di una casella di posta elettronica dell'Associazione CSV-FVG (*email aziendale*) deve essere seguita da un utilizzo della stessa esclusivamente per finalità legate alla attività lavorativa. Gli utenti dell'email aziendale sono responsabili del corretto utilizzo delle stesse e devono mantenere un corretto comportamento nell'utilizzo dello strumento di posta elettronica.
In particolare devono essere seguite le seguenti disposizioni:

- è obbligatorio porre la massima attenzione nell'aprire i file *attachments* ed i *links* di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti);
- al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, si invita, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede) ad attivare le "Regole Fuori Sede" per l'invio automatico di un messaggio di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente;
- l'email aziendale non deve essere utilizzate per l'invio o la ricezione di messaggi personali al di fuori dalle finalità lavorative o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione del Responsabile di Direzione/Servizio/Area;
- nell'eventualità in cui l'uso personale della posta elettronica aziendale si rendesse eccezionalmente necessario, gli utenti dovranno cancellare i messaggi di natura personale dal sistema;
- è fatto assoluto divieto divulgare a terzi informazioni riservate, confidenziali o comunque di proprietà dell'Associazione CSV-FVG, senza espressa autorizzazione del Responsabile di Direzione/Servizio/Area;
- è fatto assoluto divieto inviare o conservare messaggi di posta elettronica o più in generale dati, programmi o altro materiale di natura informatica pericolosi/vietati e/o aventi contenuti illegali, - a titolo esemplificativo e non esaustivo - dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terroristico o comunque inappropriato o illegale;

- in caso di assenza prolungata (ferie, malattia, aspettativa, lunga attività fuori sede) o non programmata dell'utente, l'utente deve prevedere delle opportune procedure in grado di garantire la continuità delle attività.

Si avvisa che:
- tutta la posta elettronica in entrata è controllata da un software antispam. È comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale: quindi è necessario prestare la massima attenzione a email sospette, avvisando l'Amministratore di sistema in caso di dubbi sulla provenienza/contenuto delle stesse.

- tutti i messaggi ricevuti, spediti o salvati, potranno essere letti dall'Amministratore di sistema, dalla Direzione e dal Responsabile di Direzione/Servizio/Area esclusivamente per i seguenti motivi:

- in caso di assenza improvvisa al fine di garantire una regolare continuità dell'attività lavorativa;
- per motivi di sicurezza informatica.

In tutti questi casi l'utente verrà informato.

La Posta Elettronica Certificata (PEC) potrà essere utilizzata solamente su incarico del Responsabile di Direzione/Servizio/Area cui compete la specifica PEC.

NAVIGAZIONE INTERNET

L'accesso ad Internet (tramite PC, *tablet o smartphone* aziendali) è fornito allo scopo di consentire l'acceso ad eventuali informazioni e contenuti necessari allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo.
Si informa che il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli, compiuti dal personale incaricato della Direzione IT, potranno avvenire mediante un sistema di analisi dei contenuti o mediante "*file di log*" della navigazione svolta.
Per prevenire eventuali abusi nell'uso di Internet il sistema è provvisto di filtri d'accesso.

Si devono comunque osservare le seguenti regole di navigazione della rete Internet:

- è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da *copyright*, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di *software* che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;
- è tassativamente vietato effettuare ogni genere di transazione finanziaria di interesse personale ivi comprese le operazioni di home banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Responsabile di Direzione/Servizio/Area e comunque nel rispetto delle normali procedure di acquisto, pagamento, ecc.
- è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali, - a titolo esemplificativo e non esaustivo - dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terroristico o comunque inappropriato o illegale;

- è vietato effettuare copia non autorizzata di materiale coperto da *copyright* compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietata la condivisione di file in modalità peer-to-peer;

- è vietato scaricare programmi, anche se privi di licenza o in prova (*freeware e shareware*), se non in caso di espressa autorizzazione da parte del proprio Responsabile di Direzione/Servizio/Area. Eseguire il *download* di file da Internet è infatti un'operazione intrinsecamente pericolosa in quanto può essere il veicolo per l'introduzione di *virus e malware*;

- è vietato immettere sulla rete o sui server *software* dannoso per i sistemi o comunque non autorizzato;
- è vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione con le normative vigenti;
- è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'*host* dell'utente (*sniffing*) a meno che questa attività non faccia parte dei compiti dell'utente e quindi formalmente autorizzata dal proprio Responsabile di Direzione/Servizio/Area;
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque *host*, rete, account.

CONNESSIONE VPN

La connessione VPN viene messa a disposizione esclusivamente per il collegamento sicuro con la rete aziendale devono essere usati dispositivi aziendali, che vengono messi a disposizione dall'azienda e sono stati configurati dalla stessa per l'accesso. L'utilizzo deve essere limitato ai soli scopi lavorativi. Valgono le stesse disposizioni dell'utilizzo interno dei dispositivi.

UTILIZZO DI SMARTPHONE, TABLET, TELEFONI AZIENDALI E SISTEMI DI STAMPA

Telefono fisso aziendale. L'utilizzo del telefono aziendale deve essere limitato allo svolgimento delle proprie attività lavorative. Per prevenire eventuali abusi all'uso del telefono è previsto un monitoraggio sul traffico di ogni utenza.
Smartphone e Tablet. L'accesso allo *Smartphone o Tablet* deve avvenire attraverso l'attivazione di una *password* personale (attivazione dello *screen saver* automatico).

È vietata la conservazione di documenti scaricati come allegati (a titolo esemplificativo: *email, skype, Whatsapp, etc,*), il cui contenuto sia di carattere aziendale, se non per il tempo strettamente necessario.
Si raccomanda la massima attenzione nell'utilizzo di *App* sul proprio dispositivo, in relazione all'eccessivo consumo di traffico dati ed alla sicurezza del proprio apparato.
Per motivi di sicurezza e per prevenire eventuali abusi è previsto un sistema monitoraggio (Mobile Device Manager) sulla quantità del traffico dati generato, attraverso il quale potranno essere cancellate/bloccate le *App* inappropriate.
Sistemi di stampa. È vietato l'utilizzo per fini personali dei sistemi multifunzione (sistemi di stampa, copia ed invio fax) e dei sistemi fax e aziendali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di Direzione/Servizio/Area.
Si raccomanda di non lasciare documenti incustoditi presso i suddetti dispositivi.

RIUTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE

Al termine dell'utilizzo dei supporti di memorizzazione contenenti dati (chiavette USB, Hard Disk interni ed esterni), questi dovranno essere cancellati secondo procedura, per eliminare ogni informazione contenuta prima di autorizzarne qualunque tipo di nuovo utilizzo.

SISTEMI DI MONITORAGGIO

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 aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale dell'IT e/o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico e ai servizi di stampa.
Periodicamente e in presenza di anomalie (intervento antivirus, segnalazione di rallentamenti del computer, utilizzo aziendalmente eccessivo dell'accesso Internet, dimensione elevata della casella di posta elettronica o dello spazio disco utilizzato, ecc.), il personale incaricato dell'IT effettuerà verifiche di funzionalità approfondite che potranno determinare segnalazione ed avvisi generalizzati diretti ai dipendenti della funzione in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

SISTEMA DI VIDEOSORVEGLIANZA

Il **sistema di videosorveglianza** è realizzato in alcune specifiche aree dal Titolare (adeguatamente indicate da cartelli informativi) con finalità di sicurezza e controllo da accessi non autorizzati o guasti tecnici e strutturali, per tutelare il patrimonio della società contro atti vandalici, comportamenti illeciti e/o fraudolenti e per agevolare gli operatori nel controllo della sicurezza delle strutture. L'accesso alle immagini videoregistrate è permesso esclusivamente per le finalità sopra indicate ad incaricati del trattamento del Titolare ed in caso di necessità agli organi di polizia preposti.

SPECIFICI DIVIETI

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- caricare programmi non provenienti da una fonte certa e autorizzata dalla Società;
- acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;
- detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);
- installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;
- utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;

- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
- distribuire il software aziendale a soggetti terzi;
- realizzare codice software che violi copyright di terzi;
- accedere illegalmente e duplicare banche dati.

PRESCRIZIONI RESIDUALI

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, può rivolgersi al proprio Responsabile di Direzione/Servizio/Area per ricevere le opportune istruzioni.

SANZIONI

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite

AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione periodica. La versione aggiornata viene pubblicata sul sito internet associativo.