REGOLAMENTO INFORMATICO

Rev.	Oggetto	Data approvazione
00	Regolamento Informatico	C.d.A. 30/07/2018
01	Revisione	C.d.A. 11/07/2022

1. PREMESSE

La diffusione delle nuove tecnologie informatiche, l'utilizzo della rete internet tramite le risorse informatiche e l'aumento delle informazioni trattate con strumenti elettronici, hanno aumentato di fatto i rischi legati alla sicurezza e all'integrità delle informazioni e le responsabilità previste dalla normativa civile e penale.

acquevenete (nel seguito "Società"), pertanto, deve provvedere a garantire la continuità dell'attività e assicurare nel contempo la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti anche inconsapevoli possano minacciare o compromettere la sicurezza nel trattamento dei dati, diminuire l'efficienza delle risorse informatiche o che comportamenti impropri distolgano le risorse aziendali dall'uso a cui sono deputate.
In questo contesto, la Società ha ritenuto necessario adottare il presente Regolamento al fine di evidenziare ai propri dipendenti, collaboratori e altri soggetti autorizzati, le indicazioni e le misure necessarie e opportune per il corretto utilizzo nel rapporto di lavoro degli apparati elettronici in dotazione, quali personal computer (fissi e portatili), smartphone e tablet, e dei software applicativi, gestionali, posta elettronica, Internet e social network. Vengono pertanto definite le modalità di utilizzo degli strumenti nell'ambito dell'attività lavorativa, disciplinato il corretto utilizzo degli strumenti stessi e data la massima diffusione alla cultura sulla sicurezza informatica intesa come capacità e consapevolezza dell'utilizzo delle risorse informatiche.

2. PRINCIPI GENERALI

Con l'approvazione del presente regolamento *acquevenete* si pone l'obiettivo di fornire a tutti i dipendenti le linee di comportamento per il corretto utilizzo delle risorse informatiche, della posta elettronica e dell'accesso alla rete Internet.
Inoltre, la Società, in qualità di Titolare del trattamento dei dati personali, ritiene opportuno dotarsi di questo Regolamento anche al fine di adempiere agli obblighi fissati dal Regolamento Europeo sul trattamento dei dati personali (GDPR).

I trattamenti effettuati dalla Società rispettano le garanzie poste in essere dal legislatore in materia di protezione dei dati personali e si svolgono nell'osservanza dei principi sanciti dalla normativa privacy.

3. CAMPO DI APPLICAZIONE

Il presente Regolamento si applica a tutti i lavoratori e i collaboratori della Società, a prescindere dal rapporto contrattuale intrattenuto con la stessa, e a tutti coloro ai quali vengono assegnate delle credenziali per accedere alla rete.
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "Utente" deve intendersi ogni dipendente, collaboratore o altro soggetto autorizzato, in possesso di specifiche

credenziali di autenticazione per l'utilizzo delle risorse informatiche, destinatario del presente Regolamento.

4. REGOLE DI COMPORTAMENTO GENERALI

acquevenete è titolare di qualsiasi diritto connesso ai sistemi informativi e alle risorse informatiche, ai dati, ai contenuti di ogni tipo e genere, elaborati, creati, o modificati nell'ambito delle attività lavorative e tramite l'opera dei suoi dipendenti e collaboratori.
Per "risorsa informatica" si intende qualsiasi strumento informatico di proprietà della Società ed utilizzato dal lavoratore per rendere la prestazione lavorativa. A titolo esemplificativo ma non esaustivo sono risorse informatiche: personal computer, tablet, telefoni fissi e mobili, multifunzioni, viacard, telepass, carte di credito, sistemi di geolocalizzazione (navigazione satellitare e sistemi di antifurto satellitare) installati su veicoli aziendali, indirizzo e-mail aziendale, rete aziendale.
L'utilizzo delle risorse informatiche e telematiche aziendali, deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra la Società e i propri dipendenti.
L'Utente dovrà adottare tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre. La Società, pertanto, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dei propri dipendenti e collaboratori esclusivamente per finalità di tipo lavorativo.
Non è quindi permesso utilizzare, tranne espressa autorizzazione, detti strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino qualsiasi disposizione normativa.
Al riguardo si evidenzia che la Società adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardando il rispetto della libertà e della dignità dei lavoratori.

In generale l'Utente deve osservare le regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa privacy, contenute nel "Manuale Privacy" pubblicato sulla intranet aziendale (GpWeb).

5. UTILIZZO DELLE RISORSE INFORMATICHE

Di seguito vengono descritte le linee di comportamento a cui i destinatari del presente Regolamento devono attenersi nel corso dell'attività lavorativa.
Gli strumenti e le dotazioni informatiche, necessari a rendere la prestazione lavorativa, devono esser utilizzati per soli fini lavorativi considerato che i dati eventualmente raccolti potranno essere utilizzati per tutti i fini connessi al rapporto di lavoro, compresi quelli disciplinari. Sono esclusi, pertanto, gli utilizzi personali, anche a scopo illecito.
I medesimi strumenti devono essere custoditi in modo appropriato.
Nel particolare caso di telefoni cellulari, vale quanto riportato nel successivo paragrafo "Utilizzo dei device".
Le richieste di nuove dotazioni, assistenza, riparazione e sostituzione vanno inoltrate e gestite secondo le indicazioni del paragrafo "Richieste e assistenza informatica" (punto 5.14).

I dipendenti dotati di strumenti informatici sono responsabili della loro custodia e utilizzo. Il dipendente che, venendo meno al dovere di diligenza nella custodia, causi il danneggiamento o lo smarrimento delle dotazioni informatiche affidategli, risponderà del danno patrimoniale arrecato a *acquevenete*.
I dipendenti sono tenuti a comunicare tempestivamente all'Ufficio IT eventuali furti e/o danneggiamenti di tali strumenti, nonché eventuali anomalie di funzionamento che ne possano pregiudicare la regolare funzionalità. Nel caso di furto o smarrimento di un qualsiasi dispositivo *acquevenete*, il dipendente ha il compito di:

- sporgere denuncia presso le forze dell'ordine quali Polizia o Carabinieri (specificando il codice IMEI nel caso di cellulari);
- richiedere una nuova dotazione informatica allegando la denuncia alle forze dell'ordine.

5.1 Uso del Pc

Per i Personal computer (comprese le periferiche ad esso connesse) e i relativi programmi e/o applicazioni valgono, in particolare, le seguenti regola operative:

- il Personal computer dato in affidamento all'Utente permette l'accesso alla rete della Società solo attraverso specifiche credenziali di autenticazione;
- non è consentito l'uso di programmi diversi da quelli ufficialmente installati dalla Società, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti;
- non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge 21/05/2004 n. 128. L'inosservanza della presente disposizione espone la stessa Società a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni 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, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Società ai sensi del D.Lgs. 231/2001, con applicazione di sanzioni pecuniarie e interdittive;
- non è consentita l'attivazione della password d'accensione (Bios) senza preventiva autorizzazione dell'Amministratore di SSistema, né modificare le caratteristiche hardware e software impostate sul proprio Pc, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (ad esempio: masterizzatori, modem, hard disk esterni, chiavette usb o supporti di memorizzazione in genere considerati esterni), salvo previa autorizzazione esplicita da parte dell'amministratore di sistema;
- ogni Utente deve prestare la massima attenzione ai supporti di origine esterna (supporti usb), avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus;
- ogni Utente dovrà effettuare i salvataggi dei file su server evitando di effettuare salvataggi sul disco rigido del Pc o su supporti di archiviazione removibili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti da evitare l'archiviazione ridondante;
- il Pc deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio e in caso di suo inutilizzo. È buona norma attivare lo screensaver con password anche per assenze di brevi periodi.

5.2 Utilizzo di Pc portatili

Relativamente ai Pc portatili valgono le seguenti regole:

- anche qualora utilizzati all'esterno della Società, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni;
- non devono essere lasciati incustoditi e sul disco devono essere conservati solo i file strettamente necessari;
- nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server)/Accesso RemotoVPN (Virtual Private Network), deve essere utilizzato l'accesso in forma esclusivamente personale attraverso le Credenziali di Autenticazione alla rete. Al termine della sessione di collegamento, dovrà essere effettuata la disconnessione attraverso il software utilizzato;
- dovranno essere periodicamente collegati alla Rete interna al fine di consentire gli aggiornamenti software e policy.

5.3 Uso dei dischi di rete (directory)

È obbligatorio il salvataggio dei dati sulle apposite unità di rete messe a disposizione dell'Utente, al fine di evitare perdite di dati e agevolare le operazioni di backup degli stessi.

5.4 Uso dei supporti rimovibili

Tutti i supporti rimovibili (floppy, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e/o informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela al fine di evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

L'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Al fine di assicurare la distruzione e/o l'inutilizzabilità dei supporti rimovibili contenenti dati personali, ciascun Utente dovrà contattare l'amministratore di sistema e seguire le istruzioni da questo impartite.

In ogni caso, i supporti rimovibili contenenti dati personali devono essere adeguatamente custoditi dagli Utenti.

È vietato l'utilizzo di supporti rimovibili personali.

5.5 Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al Pc, la connessione alla rete e/o per l'accesso ai diversi applicativi, vengono assegnate all'Utente dall'Amministratore di sistema, in seguito alla sottoscrizione del contratto di assunzione o di collaborazione.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (user id), associato a una parola chiave riservata (password), che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata.

La password, che rappresenta la parte segreta delle credenziali ed è conosciuta solo dall'Utente, è composta da almeno 8 caratteri, può essere formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, e non deve contenere riferimenti facilmente riconducibili all'Utente (nome, cognome, data di nascita, ecc.).

L’Utente ha l’obbligo di modificare la password dopo il primo utilizzo e di cambiarla con cadenza trimestrale.

Per garantire la segretezza delle credenziali e la sicurezza durante le sessioni di trattamento dei dati, ogni Utente dovrà:

- evitare di condividere in qualsiasi modo la password;
- non lasciare accessibile l’elaboratore durante una sessione di trattamento dei dati;
- impostare uno screen saver dotato di password (con tempi di avvio brevi) che blocchi l’accesso all’elaboratore in caso sia necessario allontanarsi per un tempo prolungato;
- qualora l’elaboratore sia utilizzato da più incaricati, ricordarsi sempre al termine del lavoro effettuato di disconnettersi dal sistema (dal menù avvio/start cliccare sul proprio nome quindi “Disconnetti”).

Le credenziali sono strettamente personali e non possono essere cedute a terzi. Il mantenimento della segretezza delle credenziali è ad esclusivo carico dell’Utente, il quale sarà il solo responsabile per qualsiasi attività posta in essere tramite l'utilizzo delle stesse.

5.6 Uso antivirus

Il sistema informatico e i Pc collegati alla rete della Società sono protetti da software antivirus aggiornati quotidianamente e automaticamente.

È vietato cancellare, riconfigurare o disattivare il software antivirus.

Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus.

L’Utente dovrà tempestivamente segnalare eventuali anomalie all’amministratore di sistema o altro referente della Società:

- qualora vi sia motivo di ritenere che il Pc sia stato infettato o che non sia installata l’ultima versione aggiornata dell’antivirus;
- nel caso di riconoscimento di virus, per il quale il sistema segnalerà un messaggio di avviso e nei rari casi in cui il sistema antivirus non sia in grado di rimuovere il virus.

5.7 Utilizzo dei device (smartphone, tablet)

I device affidati all’Utente sono strumenti di lavoro e la Società non ne consente un differente utilizzo.

È assolutamente vietato l'utilizzo dei device forniti per la visione, il download e il caricamento di contenuti contrari al buoncostume e rientranti quindi in ambiti pornografici e/o violenti; sono altresì vietati il download, la riproduzione e la condivisione di contenuti online e multimediali ottenuti illegalmente in violazione alla normativa sul diritto d'autore e al Codice penale.

Ogni utilizzo che possa in qualche modo contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, è assolutamente vietato; qualora si riscontrassero addebiti o sanzioni derivanti da un utilizzo improprio dei device questi rimarranno a carico della persona che ha commesso l'infrazione.

L'Utente è responsabile dei device assegnati e deve custodirli con diligenza sia fuori dalla Società sia durante l'utilizzo nel luogo di lavoro. I device devono essere custoditi con cura evitando ogni possibile forma di danneggiamento o sottrazione.

5.8 Uso della rete aziendale

Per l'accesso alla rete della Società ciascun Utente deve essere in possesso della specifica "Credenziale di Autenticazione" (username e password).

È proibito entrare nella rete e nei programmi con un codice d'identificazione Utente diverso da quello assegnato. Le password d'accesso alla rete ed ai programmi sono segrete e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server della Società 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 ultime vengono svolte regolari attività di controllo, amministrazione e back up da parte dell'Amministratore di Sistema.

Tutti i dischi o altre unità di memorizzazione locali (ad esempio il disco C interno al proprio Pc) non sono soggetti a salvataggio da parte dell'Amministratore di sistema. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.

È vietato connettere in rete stazioni di lavoro o altri dispositivi hardware, sia personali sia di fornitori, senza autorizzazione della Società. È vietato monitorare, attraverso qualsiasi dispositivo hardware o software, ciò che transita in rete. È vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonica per l'accesso a banche dati esterne o interne all'Azienda.

L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza o non consoni all'attività lavorativa sia sui device degli Utenti sia sulle unità di rete.

È opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun Utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo necessario evitare un'archiviazione ridondante.

5.9 Uso della rete Internet

La rete Internet è ormai divenuta uno strumento operativo di comunicazione imprescindibile e costituisce a tutti gli effetti uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.

Un suo utilizzo indiscriminato, però, può rendere la Società vulnerabile sotto il profilo della sicurezza ed è quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

L'Utente deve utilizzare Internet in modo da non rivelare o diffondere al pubblico informazioni di tipo confidenziale o di proprietà dell'Azienda (ade esempio: informazioni finanziarie, nuovi progetti di business e produzione, piani e strategie di marketing, database e informazioni in essi contenute, liste di clienti, informazioni tecniche di prodotto, software, codici di accesso ai computer e alla rete, dati e informazioni personali e relazioni di lavoro).

Alla luce di ciò, la Società ha adottato alcune misure ritenute opportune per proteggere i propri sistemi elettronici dall'eventuale utilizzo non accorto della navigazione su Internet da parte dei lavoratori.

In particolar modo gli utenti non possono utilizzare strumenti privati per il collegamento alla rete. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare Internet per:

- l’upload o il download di software gratuiti (freeware) e shareware, nonché l’utilizzo di documenti provenienti da siti web, se non strettamente attinenti all’attività lavorativa (filmati e musica) e previa verifica dell’attendibilità dei siti in questione;
- l’effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Società;
- 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 line (esclusi gli strumenti autorizzati), di bacheche elettroniche come i social network e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dalla Società;
- l’accesso, tramite Internet, a caselle webmail di posta elettronica personale.

Al fine di evitare la navigazione in siti non pertinenti (a rischio) all’attività lavorativa, la Società rende nota l’adozione di uno specifico sistema di blocco che previene determinate operazioni quali l’upload o l’accesso a siti ad alta rischiosità inseriti in una black list.

I blocchi sopraindicati limitano l’accesso ai siti Internet che presentano i seguenti contenuti:

- illegali o non etici;
- materiale per adulti, pornografia;
- giochi, scommesse, intermediazione e trading, download software;
- social network, radio e tv, Internet;
- peer to peer;
- malware, spyware, hacking, bypass proxy, phishing.

Gli eventuali controlli, compiuti dalla Società potranno avvenire mediante “file di log” della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell’Azienda.

5.10 Uso della posta elettronica

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. È vietato utilizzare tutte le caselle di posta elettronica, comprese info@acquevenete.it o quelle condivise tra più utenti, 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 di allegati contenenti filmati o brani musicali (es.mp3) 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 o mailing-list se non legati all’attività lavorativa;
- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, lo si dovrà comunicare immediatamente all’Amministratore di Sistema. Non si dovrà in alcun caso procedere all’apertura degli allegati a tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Nel caso di mittenti sconosciuti o messaggi insoliti, identificati come potenziali tecniche intrusive di spamming e phishing, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli.

Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe, .scr, .bat, ecc.), oppure file che abbiamo nomi simili a documenti che hanno estensione ZIP o diano parvenza di archivio compresso, non devono essere aperti. È obbligatorio quindi porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Le caselle di posta elettronica personali devono essere consultate esclusivamente dagli Utenti intestatari.

Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere il seguente avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.

Pertanto, nei messaggi inviati tramite posta elettronica aziendale verrà automaticamente inserito il seguente testo:

"Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Chiunque ricevesse questo messaggio per errore o comunque lo leggesse senza esserne legittimato, è informato che trattenerlo, copiarlo, divulgarlo, distribuirlo a persone diverse dal destinatario è severamente proibito, ed è pregato di rinviarlo al mittente distruggendone l'eventuale copia cartacea e la copia in formato elettronico."

5.11 Uso stampanti

Per quanto concerne l'utilizzo delle stampanti, gli Utenti sono tenuti a:

- stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
- spegnere le stampanti locali ogni sera prima di lasciare gli uffici o in caso di loro inutilizzo.

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà avere cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

5.12 Social Network

L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, Linkedin™, Instagram™, Yammer, blog e forum, anche professionali – verrà gestito e organizzato esclusivamente dalla Società attraverso specifiche direttive e istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti. Fermo restando il pieno e inderogabile diritto della persona alla libertà di espressione e al libero scambio di idee ed opinioni, la Società ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine e il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro.

La policy qui dettata deve essere seguita dagli Utenti sia che utilizzino dispositivi messi a disposizione dalla Società, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti della stessa Azienda.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dalla Società riservate e in genere, a titolo esemplificativo e non

esaustivo, sulle informazioni finanziarie e economiche, commerciali, sui piani organizzativi, sui clienti, sui fornitori e altri partners della Società stessa.

Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione da parte della Direzione aziendale.

L'Utente deve garantire la tutela della privacy delle persone; non potrà quindi comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso della Direzione della Società.

L'Utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso la Società, i colleghi, i clienti e i fornitori, attività che possano essere penalmente o civilmente rilevanti. A titolo esemplificativo, sono vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. E' vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione in cui essa avviene possa essere collegata all'ambito aziendale.

Infine, in via generale e ove non autorizzato in senso diverso dalla Direzione, l'Utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Azienda, in particolare in forum professionali, l'Utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Azienda.

5.13 Misure organizzative

Si conferma l'obbligatorietà del salvataggio dei dati sulle apposite unità di rete messe a disposizione degli Utenti al fine di evitare perdite dati e agevolare le operazioni di backup degli stessi.

5.14 Richieste e assistenza informatica

La Società mette a disposizione degli Utenti un sistema di ticketing con il quale è possibile gestire le richieste informatiche, nonché le segnalazioni di guasti e malfunzionamenti dei sistemi.
Tale sistema è accessibile tramite:

- sito internet: http://assistenza.acquevenete.it (link "Richiedi ASSISTENZA" su desktop);
- mail dedicata: supporto.tecnico@acquevenete.it.

6. MONITORAGGI E CONTROLLI DELLE SOCIETA'

6.1 Accesso ai dati dell'Utente

L'Amministratore di Sistema o i suoi delegati possono accedere ai dati trattati dall'Utente (posta elettronica, controlli di rete, ecc.) esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad esempio: contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, ecc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio: aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware).

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, ad esempio mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.
Il sistema informativo fornisce una serie di informazioni inerenti all'utilizzo dei software e/o dell'hardware di ciascuna postazione di lavoro. In via esemplificativa e non esaustiva il sistema informativo fornisce log di:

- accesso a Internet;
- posta elettronica e servizi mail to fax;
- accesso alle banche dati e agli applicativi;
- telefonia;
- attività di sistema;
- attività di accesso (accensione, spegnimento);
- stampa.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni, inerenti alla sicurezza e alla manutenzione del sistema informatico.
I file di Log vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'Azienda, fatti salvi in ogni caso specifici obblighi di legge.
Il sistema di registrazione dei log è configurato per cancellare periodicamente e automaticamente (attraverso procedure di sovrascrittura) i dati personali degli Utenti relativi agli accessi internet e al traffico telematico.
L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'Utente all'Azienda per cessazione del rapporto, sostituzione delle apparecchiature, ecc.
Sarà cura dell'Utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.
In ogni caso, la Società garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione e eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

6.2 Controlli

La Società ha l'obbligo di salvaguardare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori, pertanto, si riserva il diritto di effettuare controlli per verificare il rispetto del presente Regolamento.
A tale proposito si sottolinea che le risorse informatiche sono di proprietà della Società in quanto mezzo di lavoro: è pertanto fatto divieto di utilizzo delle stesse e dell'accesso alla rete Internet per fini ed interessi non strettamente coincidenti con quelli della Società stessa. Con riferimento a tali controlli il presente Regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti e collaboratori.

Le verifiche sugli strumenti informatici saranno eseguite dalla Società, o suoi delegati, nel pieno rispetto dei diritti e delle libertà fondamentali degli Utenti e del presente Regolamento, secondo i principi di pertinenza e non eccedenza.
La Società, pertanto, si riserva il diritto di controllare, anche in maniera occasionale e/o discontinua, il corretto utilizzo degli strumenti di lavoro, implementando ogni misura tecnologica volta a minimizzare il più possibile l'uso di dati identificativi dei lavoratori, nei modi e nei limiti esplicitati di seguito e nel successivo paragrafo denominato "Graduazione dei controlli".
In nessun caso tali controlli verranno impiegati per un monitoraggio dell'efficienza dell'attività lavorativa del singolo individuo come prescritto dall'art. 4 dello Statuto dei lavoratori.
I controlli si svolgeranno in forma graduata:
in via preliminare la Società provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura ovvero a sue aree e dunque un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite;
in assenza di successive anomalie non si effettueranno controlli su base individuale; in caso contrario il controllo si concluderà con un avviso ai dipendenti interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Le attività di accesso ad Internet vengono automaticamente registrate in forma elettronica attraverso i c.d. "log di sistema". Questi sistemi software sono programmati e configurati in modo da cancellare periodicamente e automaticamente, attraverso procedure di sovrascrittura dei log file, i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia più necessaria.
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, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Società, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, oltre ai tabulati del traffico telefonico.

6.3 Obbligo alla riservatezza

Nell'ambito del rapporto di lavoro, potranno essere comunicate informazioni organizzative, commerciali, finanziarie, operative, amministrative riservate di esclusiva proprietà e pertinenza della Società.
Tali informazioni includeranno a titolo esemplificativo e non esaustivo dati di clienti, dati di fornitori, specifiche organizzative, clienti, campioni e altro materiale relativo a prodotti, procedimenti, nonché ogni altro tipo di informazione.
Al riguardo facciamo presente quanto segue:

- tutte le informazioni ricevute si intenderanno di natura riservata e confidenziale;
- le informazioni potranno essere utilizzate al solo scopo di prestare i servizi che formano oggetto del rapporto di lavoro sopra indicato ed è necessario impegnarsi per evitarne la diffusione;
- il mancato adempimento agli obblighi sopra indicati comporterà quello di risarcire ogni e qualsiasi danno che la Società dovesse sopportare a causa di tale inadempimento;
- in occasione della cessazione, per qualsiasi motivo, del rapporto in essere tra le parti, a fronte di semplice richiesta scritta (anche a mezzo mail) della Società, si è tenuti a restituire a quest'ultima o a distruggere tutti i documenti (anche le copie) contenenti informazioni della Società.

In particolare, nel caso di richiesta di restituzione, tali documenti, copie e materiali dovranno essere restituiti entro e non oltre 24 ore dalla ricezione della relativa richiesta.
Gli obblighi di riservatezza saranno vigenti e vincolanti anche alla cessazione del rapporto di lavoro tra le parti.

6.4 I reati informatici presupposto del Decreto Legislativo 231/2001

La Legge n. 48/2008, che ha ratificato la Convenzione di Budapest del Consiglio d'Europa sul cybercrime del 23 novembre 2001, ha apportato varie modifiche sia al Codice penale che a quello di Procedura penale, introducendo delle modifiche al D.Lgs. 231/01 per inserire i vari reati informatici, di seguito riportati:

1. falsità in un documento informatico (art. 491-bis c.p.);
2. accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.): per sistema informatico o telematico si intende un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, cioè tutto ciò che gestisce ed elabora dati in formato digitale;
3. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
4. diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
5. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
6. installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
7. danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
8. danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
9. danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
10. danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635quinquies c.p.);
11. frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.);
12. violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (Articolo 1, co. 11, D.Lgs. n. 105/2019, convertito con modificazioni dalla L. n. 133/2019);
13. Frode informatica (art. 640 ter c.p.);
14. Violazione delle norme in materia di protezione del diritto d'autore (art. 171 e seguenti L. n. 633/41).

7. MODALITA' OPERATIVE

7.1 Smart working

In generale l'Utente deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa privacy:

1. tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
2. le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
3. devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
4. in caso di utilizzo delle risorse aziendali, non usare sistemi personali di posta elettronica, ma ricorrere sempre a dispositivi forniti dall'Azienda;
5. evitare l'uso dei social network o altre applicazioni social durante lo svolgimento del proprio lavoro da casa;
6. evitare di rivelare al telefono informazioni aziendali quando si è in prossimità di altre persone.

7.2 Foto, video e immagini

L'Utente deve garantire la tutela della privacy delle persone; pertanto non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso della Direzione della Società.

7.3 Regolamento Gruppi messaggistica (tipo WhatsApp/Telegram)

L'ingresso a far parte di un Gruppo di messaggistica tipo WhatsApp/Telegram avviene esclusivamente su invito da parte di un Amministratore del Gruppo, dopo che la Società ne ha dato l'approvazione.
L'utilizzo deve rispettare le normali regole di utilizzo consono, lecito e diligente, come per tutti gli altri strumenti in uso.

Eventuali modifiche al Regolamento potranno avvenire in qualsiasi momento. Integrazioni o modifiche possono essere comunicate dall'Amministratore del Gruppo anche tramite messaggio direttamente sul Gruppo stesso e le stesse integreranno o sostituiranno le parti di Regolamento ivi pubblicate.

8. VIOLAZIONI E SANZIONI DISCIPLINARI

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 i provvedimenti disciplinari previsti dalla normativa vigente e dai regolamenti interni, nonché con le azioni civili e penali previste dalla normativa di riferimento.