CLUB ALPINO ITALIANO

Regolamento interno sulle modalità per un corretto utilizzo dei sistemi informatici aziendali

INDICE

CAPO I - I PRINCIPI

ART. 1 - INTRODUZIONE, DEFINIZIONI E FINALITA'

Il presente regolamento interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte:
- del personale dipendente, ovvero
- dei collaboratori, ovvero
- dei soggetti che ricoprono incarichi istituzionali

che sono pertanto assegnatari ("**Utenti")** di risorse informatiche e di connettività messe a disposizione dal Club Alpino Italiano, al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali incluse nel regolamento, pertanto, è volto a conformare l'Ente ai principi di diligenza, informazione e correttezza ai sensi del Reg. UE 679/2016 e D. Lgs. 101/2018 e nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti degli Utenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare deliberazione n. 13 del 1° marzo 2007 del Garante per la protezione dei dati personali in materia di Linee guida per posta elettronica e internet).

ART. 2 - TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali da considerarsi di esclusiva proprietà dell'Ente.
Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative e professionali affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per l'Ente), e comunque per l'esclusivo perseguimento degli obiettivi dell'Ente.

A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Ente, sarà dallo stesso considerato come avente natura aziendale e non riservata.

ART. 3 - RESPONSABILITA' PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ente nonché dei relativi dati trattati per finalità aziendali.
A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ente, è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.
Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e/o

alla Direzione, e senza ritardo, eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento interno.
Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Ente.

ART. 4 - I CONTROLLI

I principi

L'Ente, in linea con quanto prescritto dall'ordinamento giuridico italiano, esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa e professionale dell'Utente. Resta fermo, tuttavia, per il personale dipendente, il diritto dell'Ente di effettuare controlli sull'effettivo adempimento della prestazione lavorativa; tutti gli utenti potranno essere soggetti a controlli sul corretto utilizzo dei beni e servizi informatici aziendali; i controlli posti in essere, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati, nel rispetto del principio di pertinenza e non eccedenza.
L' Ente, nel riservarsi il diritto di procedere a tali controlli, informa che le modalità di effettuazione degli stessi sono ispirate al principio della "gradualità" così come di seguito più precisamente specificato.

Modalità di effettuazione dei controlli

I controlli consentono all'Ente di intervenire con verifiche qualora si riscontrino anomalie di ambito, senza arrivare al dettaglio del soggetto singolo, almeno in una prima fase.
Secondo il principio della gradualità:

- i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura ovvero a singole aree, aventi caratteristiche tali da precludere l'immediata identificazione dell'Utente.
- nel caso in cui si dovessero riscontrare violazioni del presente regolamento interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.
- in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati

In ogni caso l'Ente non può, in alcun caso, utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore o del professionista.
Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la riproduzione e la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi occulta di computer portatili affidati in uso.

CAPO II - MISURE ORGANIZZATIVE

ART. 5 - ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali, per singola postazione lavorativa.

- gli account Utenti sono personali ovvero associati univocamente alla persona assegnataria;
- l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente da coloro all'uopo autorizzati, che le generano attraverso modalità riservate;
- le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi (seppur soggetti in posizione apicale all'interno dell'Ente).
- se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password ed a segnalare la violazione alla Direzione nonché al Responsabile della protezione dei dati personali (DPO);
- ogni Utente è responsabile dell'utilizzo del proprio account Utente;
- in base a quanto previsto dal punto n. 10 del Regolamento Tecnico – Allegato B al Codice della privacy si ricorda che in caso di assenza improvvisa o prolungata dell'utente e per improrogabili necessità legate all'attività lavorativa e professionale, per le esigenze produttive aziendali o per la sicurezza ed operatività delle risorse informatiche dell' Ente, lo stesso si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento di coloro all'uopo autorizzati.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte di coloro all'uopo autorizzati, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo almeno ogni 6 mesi.

L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri, inclusi i caratteri speciali (#, %, etc.), di cui almeno uno numerico;
- la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere non alfanumerico tipo "@#§£$%...";
- evitare di includere parti del nome, cognome e/o comunque elementi allo stesso agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che scrivere la password su post-it o altri supporti se non opportunamente custoditi (ad es. in cassaforte), non è conforme alla normativa e costituisce violazione del presente regolamento interno.

Cessazione degli Account

In caso di interruzione del rapporto di lavoro (ovvero della collaborazione, ovvero del mandato istituzionale) con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 30 giorni da quella data; entro 3 (tre) mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente senza necessariamente provvedere alla distruzione dei dati (file) ad esso attribuiti.

ART. 6 - POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *devices* concesso, dall' Ente, in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici aziendali, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di disciplinare un corretto utilizzo di tali beni, l'Ente ha adottato le regole tecniche, che di seguito si riportano:

- ogni PC, notebook (accessori e periferiche incluse), e altro dispositivo, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ente, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- è dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente, professionalmente e con la massima cura;
- il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, è necessaria espressa richiesta scritta dell'Utente indirizzata al proprio Responsabile di riferimento e/ alla Direzione, che ne valuterà i requisiti tecnici e l'aderenza alle policy interne ed al ruolo ricoperto nell'Ente;
- le postazioni di lavoro non devono essere lasciate incustodite con le sessioni Utente attive;
- quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- l'Utente deve segnalare con la massima tempestività a coloro espressamente incaricati ovvero al proprio Responsabile di riferimento e/o alla Direzione, eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi se non previa specifica autorizzazione del proprio Responsabile di riferimento e/o della Direzione;
- l'Ente si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, tablet, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, etc., **non potranno** essere collegati ai computer o alle reti informatiche aziendali riservate agli uffici, salvo preventiva autorizzazione scritta dell'Ente.

CAPO III - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

ART. 7 - PERSONAL COMPUTER E COMPUTER PORTATILI

Gli Utenti utilizzano per l'espletamento delle proprie mansioni dispositivi di proprietà dell'Ente; ne consegue che gli stessi sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione dell'Ente che la esegue per mezzo di coloro espressamente incaricati;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Ente;
- è onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce *virus* o altri malfunzionamenti, segnalando prontamente l'accaduto a coloro espressamente incaricati;
- è onere dell'Utente spegnere il proprio PC o computer portatile al termine del lavoro. Per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali *files* elaborati prima della sua riconsegna.

Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli Utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione. L'Ente non garantisce la riservatezza dei dati personali impropriamente non rimossi dai dispositivi da parte degli Utenti prima della riconsegna.

ART. 8 - SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli Utenti dovranno ottenere espressa autorizzazione dell'Ente per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").

L'Ente richiama l'attenzione di ogni utente su alcuni aspetti fondamentali che lo stesso è tenuto ad osservare per un corretto utilizzo del software nell'Ente:

- l'Ente acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli Utenti, quindi, tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza.
- non è consentito fare né il download né l'upload tramite internet di software non autorizzato.
- l'Ente, sulla base di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.
- l'Ente non tollererà la duplicazione illegale del software.

ART. 9 - DISPOSITIVI MOBILI DI CONNESSIONE A INTERNET

Agli assegnatari di computer portatili, possono essere dati in dotazione anche dispositivi per la connessione alla rete aziendale tramite internet, volta a facilitare lo svolgimento delle mansioni lavorative anche da remoto.

I suddetti dispositivi devono essere utilizzati esclusivamente sui computer forniti in dotazione dall'Ente e non è consentito concederne l'utilizzo a soggetti terzi.

Specifiche relative ai limiti entro cui l'Utente potrà utilizzare questa tipologia di dispositivi sono riportate nella scheda tecnica consegnata all'Utente unitamente al dispositivo di cui sopra. L'Utente dovrà attenersi ai suddetti limiti, potendo in caso contrario l'Ente richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

ART. 10 - DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, dischi rigidi esterni, etc.

L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'Ente; è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto.

Si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'Ente, i dispositivi saranno soggetti (ove compatibili) al presente regolamento interno.

ART. 11 - STAMPANTI, FOTOCOPIATRICI E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Ente. E' richiesta una particolare attenzione quando si inviano su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede, quindi, di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare e non è consentito tra le Pubbliche Amministrazioni. Nei casi in cui

questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.
L'utente è, comunque, tenuto ad individuare una soluzione alternativa all'utilizzo del fax e ad invitare l'eventuale interlocutore ad adottare analoghe modalità.

ART. 12 - STRUMENTI DI TELEFONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

L'Ente può mettere a disposizione, a seconda del ruolo o della funzione del singolo Utente, impianti di telefonia fissa e mobile, nonché dispositivi - quali smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonia tramite rete cellulare.
Specifiche relative ai limiti entro cui l'Utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata all'Utente unitamente ai dispositivi di cui sopra.
L'Utente dovrà attenersi ai suddetti limiti, potendo in caso contrario l'Ente richiedere il rimborso dei costi sostenuti per il superamento degli stessi.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale che è dato in uso per scopi esclusivamente lavorativi e professionali. E', tuttavia, concesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la c.d. "*diligenza del buon padre di famiglia*" e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.
A tal fine si informano gli utilizzatori dei servizi di fonia aziendale, che l'Ente eserciterà i diritti di cui all'art. 124 D. Lgs. 101/2018 (cd. *fatturazione dettagliata*), richiedendo ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo.
I controlli saranno eseguiti secondo le modalità descritte all'art. 4 del presente regolamento interno.
L'Ente si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla SIM in carico all'Utente per il periodo interessato. L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano:

- ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione;
- i dispositivi devono avere il sistema di autenticazione attivo che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza delle eventuali credenziali di accesso e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a modificarle dandone, comunque, comunicazione all'Ente;
- in caso di furto, danneggiamento o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà darne immediato avviso all'Ente; ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
- in caso di furto o smarrimento l'Ente si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili. Non è consentito all'Utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione;
- non è consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi se non per esplicito incarico dell'Ente;
- l'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'Utente le spese che l'Ente dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata;
- salvo diversi specifici accordi, al momento della consegna del tablet o smartphone l'Utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile

sugli smartphone e tablet, consapevole che, in caso contrario, l'Ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e, di conseguenza, del suo assegnatario.

ART. 13 – SISTEMI DI VIDEOCONFERENZA

L'Ente mette a disposizione, a seconda del ruolo o della funzione del singolo Utente, sistemi di videoconferenza per organizzare riunioni a distanza.
Tali sistemi non possono essere utilizzati per scopi diversi da quelli lavorativi.

CAPO IV - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

ART. 14 - GESTIONE UTILIZZO DELLA RETE INTRANET AZIENDALE

La rete interna, istituita appositamente per permettere collegamenti funzionali tra Utenti che prestano servizio all'interno della struttura aziendale, non può esser utilizzata per scopi diversi da quelli lavorativi o professionali.
Deve essere premura di ciascun Utente preservare dati, notizie ed informazioni aziendali dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

ART. 15 - GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dall'Ente, alla navigazione Internet tramite la rete aziendale.
Col presente regolamento interno si richiamano gli Utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'Ente.
Internet è uno strumento messo a disposizione degli Utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.
Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a) l'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
b) non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall' Ente;
   è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
c) non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames);
d) non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
e) è consentito l'utilizzo di soluzioni di Instant Messanger, chat e social networking esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'Ente;
f) non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;
g) non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

È, altresì, rigorosamente proibito qualsiasi uso del Web e dei social networks che non trasmetta un'immagine positiva o che possa in qualunque modo risultare nocivo all'immagine dell'Ente. La

registrazione di informazioni relative al traffico Internet, in ogni caso, avverrà in forma anonima o tale da precludere l'immediata identificazione di Utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*).
In caso di abusi singoli o reiterati – *cfr*. sul punto l'art. 4 del presente Regolamento interno – verranno inoltrati preventivi avvisi collettivi di richiamo al rispetto delle regole. Qualora, nonostante i rischiami generalizzati, perduri un indebito utilizzo della rete internet l'Ente procederà all'invio di avvisi più circoscritti, e – solo se a seguito della gradualità dei controlli emergano fondati sospetti – verranno allora effettuati controlli nominativi o su singoli dispositivi e postazioni.
Per facilitare il rispetto delle predette regole, l'Ente si riserva, per mezzo di coloro all'uopo incaricati, la facoltà di configurare specifici filtri che inibiscono l'accesso a siti o contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).
L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza. Ogni Utente settimanalmente provvede a cancellare i dati relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

ART. 16 - GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

Principi guida

L'Ente provvede ad assegnare una casella di posta elettronica individuale ad ogni utente. I servizi di posta elettronica devono essere utilizzati a scopo professionale: si ricorda a tutti gli utenti che la casella di posta elettronica è uno strumento di proprietà dell'Ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative e professionali affidate personalmente al soggetto.
Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri Utenti. Tali caselle devono essere utilizzate esclusivamente per la ricezione dei messaggi, mentre per le risposte o gli invii, si deve sempre utilizzare la personale casella di posta elettronica assegnata.
L'Ente valuterà caso per caso e previa richiesta dell'Utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso individuale.
Attraverso l'indirizzo di posta elettronica aziendale, gli Utenti rappresentano pubblicamente l'Ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine aziendale.
Gli Utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:

- conservare le credenziali di accesso nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file. Gli allegati provenienti da mittenti sconosciuti devono essere aperti solo dopo verifica antivirus in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi;
- inviare preferibilmente *files* in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
- non aprire e/o rispondere a messaggi di posta elettronica di dubbia affidabilità;
- cancellare preventivamente ogni messaggio di posta elettronica di palese inaffidabilità;
- collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

Non è consentito agli Utenti, al contrario:

- diffondere il proprio indirizzo di posta elettronica aziendale attraverso la rete internet;
- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (es: presentazioni o materiali video aziendali).

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli Utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".
Alla posta elettronica certificata dell'Ente si applicano, ove compatibili, le medesime sopracitate disposizioni.

Accesso alla casella di posta elettronica dell'utente assente

In caso di assenze programmate l'utente è tenuto ad attivare il sistema di invio di messaggi di risposta automatica ai messaggi in ingresso, che contengano i riferimenti di altro soggetto cui trasmettere le comunicazioni di contenuto lavorativo tramite posta elettronica o altre utili modalità di contatto in caso di assenza.
In caso di eventuali assenze non programmate (ad es., per malattia), qualora il dipendente non possa attivare la procedura sopra descritta (anche avvalendosi di servizi *webmail*), l'Ente, perdurando l'assenza oltre il limite temporale pari a due giorni, provvederà lecitamente, sempre che sia indifferibile e tramite personale appositamente incaricato, all'attivazione della risposta automatica o del re-indirizzamento, anche previa modifica delle credenziali di accesso, avvertendone il dipendente assente.
L'Ente procederà analogamente, tramite personale di volta in volta appositamente incaricato, qualora necessiti di conoscere, per improrogabili necessità legate all'attività lavorativa, il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise.

Cessazione dell'indirizzo di posta elettronica aziendale

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; entro 3 (tre) mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

CAPO V - GESTIONE DEI DOCUMENTI INFORMATICI

ART. 17 - ARCHIVIAZIONE IN CLOUD

I documenti informatici (definiti in art. 1 D. Lgs 82/2005, CAD) inerenti l'attività lavorativa o professionale, sono di proprietà dell'Ente e devono essere memorizzati esclusivamente su sistemi di memorizzazione approvati e gestiti dall'Ente ("Drive condivisi" di Google Workspace).

CAPO VI - DISPOSIZIONI FINALI

ART. 18 - SANZIONI

L'eventuale violazione di quanto previsto dal presente regolamento interno potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dal Codice disciplinare del personale dipendente non dirigente dell'Ente in vigore.
L'Ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni e/o addebiti formali, le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.
Si precisa, infine, che in caso di violazione accertata da parte degli Utenti delle regole e degli obblighi esposti in questo regolamento, l'Ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni, dati e strumenti informatici.

ART. 19 - INFORMATIVA AGLI UTENTI

EX ART. 13 REGOLAMENTO UE 2016/679 e SUCCESSIVA
REGOLAMENTAZIONE D. LGS. 101/2018

Il presente regolamento interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali, e relativamente ai trattamenti di dati personali svolti dall'Ente e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018, così come disposta dal punto 3.3 delle Linee Guida del Garante Privacy del 1° marzo 2007.

ART. 20 - COMUNICAZIONI

Il presente regolamento interno è messo a disposizione degli Utenti, per la consultazione, al momento dell'assegnazione di un account Utente o di un indirizzo di posta elettronica. Sulla intranet aziendale, ovvero presso la bacheca aziendale è pubblicata la versione più aggiornata dello stesso allo scopo di facilitarne la conoscibilità a tutti gli interessati.
Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulla bacheca aziendale e tramite l'invio di apposito messaggio di posta elettronica. Tutti gli Utenti sono tenuti a conformarsi alla versione più aggiornata del presente regolamento.
Le autorizzazioni e/o concessioni richieste dal presente regolamento ovvero poste nella facoltà degli Utenti potranno essere comunicate all'Ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es: posta elettronica).

ART. 21 - APPROVAZIONE DEL REGOLAMENTO

Il presente regolamento interno è stato adottato dal Direttore dell'Ente in data 26 novembre 2019 ed è stato modificato con atto del CDC n. 199 del 27 luglio 2022.

Milano, 27 luglio 2022
Club Alpino Italiano, in persona del Datore di Lavoro dott.ssa Andreina Maggiore

f.to dott.ssa Andreina Maggiore