REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

Ediz.	*Descrizione e riferimenti*	*Approvato*	*Data*
00	Emissione con CDS 25/2021	Con delibera CDA 01/2021 del 10.02.21	23/02/2021
01	Revisione articoli	Con delibera CDA 07/2021 del 02.09.21	09/09/2021
02			
03			
04			

SOMMARIO

DISPOSIZIONI GENERALI

ART. 1 - OGGETTO E PRINCIPI GENERALI

Le disposizioni del presente Regolamento disciplinano le modalità d'uso delle risorse informatiche e telematiche di Navigazione Lago d'Iseo s.r.l. da parte del personale dipendente e degli altri utenti abilitati ad accedere a dette risorse, nonché i controlli che la stessa Navigazione Lago d'Iseo s.r.l. può effettuare in merito a tale uso, in conformità a quanto previsto dall'articolo 4 della Legge n. 300/1970, tenuto conto delle seguenti finalità e principi:

- occorre promuovere la consapevolezza che l'uso delle tecnologie informatiche e telematiche, può dare origine a numerose problematiche con possibili gravi implicazioni in termini di sicurezza, disponibilità ed integrità dei sistemi informatici dell'azienda;
- occorre prevenire comportamenti, consapevoli e inconsapevoli, che possano innescare problemi o minacce alla sicurezza dei sistemi aziendali e nel trattamento dei dati;
- gli strumenti informatici e telematici, i computer, gli applicativi per la gestione delle diverse attività, i telefoni aziendali e gli altri mezzi forniti dall'Azienda sono da considerarsi esclusivamente strumenti di lavoro la cui utilizzazione personale è preclusa;
- l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai doveri di diligenza, fedeltà e correttezza, obblighi che sono sempre dovuti nell'ambito del rapporto di lavoro;
- è necessario porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte degli operatori nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 1.3.2007) e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'Azienda stessa a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile;
- i controlli sull'uso degli strumenti informatici e telefonici devono garantire sia il diritto dell'Azienda di proteggere la propria organizzazione ed i propri beni (materiali ed immateriali) sia il diritto del lavoratore a non vedere invasa la propria sfera personale, il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e dal Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003) nonché dal Regolamento europeo in materia (Reg. (CE) 27.4.2016, n. 2016/679/UE);
- è necessario sensibilizzare gli interessati al rispetto della normativa sulla tutela legale del software;
- l'utilizzo delle risorse e dei servizi informatici e di rete è subordinato al pieno rispetto da parte degli operatori delle norme aziendali (regolamenti, modello di organizzazione e gestione, codice di comportamento, codice etico, ecc.) delle norme civili, penali e amministrative applicabili;
- l'uso improprio delle risorse informatiche e telematiche aziendali ed il mancato rispetto delle norme e delle procedure del presente regolamento può esporre i trasgressori a sanzioni disciplinari o contrattuali, nonché a responsabilità civile o penale nei confronti della Società o di terzi;
- a fronte dei gravi rischi possibili, le violazioni alle norme del presente Regolamento saranno valutate con estremo rigore.

ART. 2 - CAMPO DI APPLICAZIONE

Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, e collaboratori dell'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto, nonché a tutti i soggetti comunque autorizzati ad operare sulle risorse informatiche e telematiche di Navigazione Lago d'Iseo s.r.l. (a titolo esemplificativo: consulenti, professionisti, incaricati di società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda, ecc.).

ART. 3 - DEFINIZIONI

Ai fini del presente regolamento si intende per:

a) **Utente**: è la persona autorizzata ad accedere alla rete informatica aziendale, ad internet e alla posta elettronica, agli applicativi aziendali e alle altre risorse informatiche e telematiche a ciò autorizzato;
b) **Autorizzato al trattamento**: è la persona fisica autorizzata a compiere operazioni di trattamento dal titolare;
c) **Dati particolari**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
d) **RSI**: acronimo di "Responsabile dei Sistemi Informati", figura responsabile di tutto il sistema informatico e dello sviluppo tecnologico dell'azienda;
e) **E-mail**: indica la funzione di posta elettronica per lo scambio di messaggio e di documenti;
f) **Download** (in italiano scaricamento): è l'azione di ricevere o prelevare dalla rete informatica un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente;
g) **Upload** (in italiano, caricamento): è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica;
h) **Freeware**: è un software che viene distribuito in modo gratuito;
i) **Shareware**: è un software che può essere liberamente ridistribuito, e può essere utilizzato per un periodo di tempo di prova variabile scaduto il quale per continuare ad utilizzare il software è necessario registrarlo presso la casa produttrice, pagandone l'importo;
j) **Malware**: tipo di software dannoso sviluppato con l'obiettivo di infettare computer o dispositivi mobili;
k) **Ransomware**: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in inglese) da pagare per rimuovere la limitazione;
l) **Virus**: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto;
m) **Spyware:** software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato.
n) **BIOS**: insieme di routine software che forniscono una serie di funzioni di base per l'accesso all'hardware del computer e alle periferiche integrate sulla scheda madre da parte del sistema operativo e dei programmi.

ART. 4 - GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

L'abilitazione attraverso le credenziali di autenticazione per l'accesso alla rete informatica viene eseguita dal Responsabile dei Sistemi Informativi (da ora RSI), e deve essere preceduta da regolare richiesta del responsabile di funzione/unità organizzativa, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Lo stesso responsabile è tenuto a dare repentina comunicazione nel caso di revoca e/o trasferimento degli utenti della propria funzione/unità organizzativa.

Nel caso di collaboratori la preventiva richiesta verrà inoltrata direttamente dal responsabile del servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'RSI, associato ad una parola chiave (password) riservata, che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione al BIOS, senza preventiva autorizzazione da parte dell'RSI.

La parola chiave, formata da lettere maiuscole e minuscole, numeri e caratteri speciali, in combinazione fra loro, deve essere composta da almeno nove caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

Al primo utilizzo della rete informatica aziendale verrà chiesto obbligatoriamente di sostituire la parola chiave rilasciata dall'RSI, sarà poi il sistema a chiedere la sostituzione della stessa ogni sei mesi.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, il responsabile di funzione/unità operativa dovrà richiedere una nuova password di accesso all'RSI.

Soggetto preposto alla custodia delle credenziali di autenticazione alla rete informatica è l'RSI. Ciascun utente deve fornire copia delle credenziali di accesso all'RSI, tramite busta chiusa, onde assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato stesso in presenza di circostanze che rendano indispensabile e indifferibile l'intervento per esclusive necessità di operatività e di sicurezza del sistema.

DISPOSIZIONI PER L'UTILIZZO DEI SISTEMI INFORMATICI

ART. 5 - UTILIZZO DELLA RETE INFORMATICA AZIENDALE

Per l'accesso alla rete informatica dell'Azienda ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

È proibito entrare nella rete informatica e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete informatica ed ai programmi sono personali e vanno tenute segrete.

Le cartelle utenti presenti nei server dell'Azienda 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 temporaneamente, in queste unità. Sulle predette cartelle vengono svolte regolari attività di controllo, amministrazione e back-up da parte del RSI.

L'Azienda si riserva di procedere in qualunque momento allo spostamento, messa in quarantena e/o rimozione di ogni file o applicazione non conforme al presente regolamento o potenzialmente pericoloso per la sicurezza del sistema sia nei personal computer degli utenti sia nelle unità di rete.

È vietata l'installazione non autorizzata di modem o altri dispositivi o servizi atti a trasmettere o ricevere dati che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'Azienda.

È compito di ciascun utente, per quanto di propria competenza e secondo i canoni della diligenza, preservare i dati, le notizie e le informazioni aziendali che circolano nella rete informatica dalla conoscibilità di terzi soggetti non espressamente autorizzati ad averne notizia.

I sistemi di teleassistenza remota sono permessi solo tramite VPN, preventivamente autorizzata dall'RSI. Altre modalità potranno essere valutate per i singoli casi.

È vietato per tutti gli utenti monitorare con software apposito ciò che transita nella rete informatica dell'Azienda.

ART. 6 - UTILIZZO DI PERSONAL COMPUTER

Il personal computer aziendale è uno strumento di lavoro.

Ogni utilizzo non inerente all'attività lavorativa è vietato. È vietato ogni utilizzo a fini privati.

Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il personal computer permette l'accesso alla rete informatica dell'Azienda solo attraverso specifiche credenziali di autenticazione come descritto negli articoli successivi.

L'Azienda si riserva di eliminare qualsiasi elemento hardware e software la cui installazione sia avvenuta senza formale richiesta da parte del responsabile di funzione/unità operativa e autorizzazione esplicita da parte dell'Ufficio Sistemi Informativi.

Costituisce buona regola la pulizia periodica (almeno una volta ogni sei mesi) delle cartelle, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati evitando l'archiviazione ridondante, specialmente sulle unità o cartelle di rete condivise, se presenti.

L'archiviazione nei dischi locali del personal computer di dati personali dell'utente non è permessa. Tali dati dovranno essere archiviati, per i soli utenti della Direzione di Esercizio e del Cantiere navale di Costa Volpino, nelle unità di rete aziendali disponibili per singolo utente.

Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato nel personal computer o in rete.

L'Azienda è autorizzata a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, per ulteriori motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.) nonché per garantire la corretta applicazione del presente regolamento. Detti interventi potranno comportare l'accesso in qualunque

momento ai dati trattati da ciascun utente, ivi compresi gli archivi di posta elettronica, nonché alla verifica dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. Analogamente, ai fini di sicurezza del sistema e per garantire la corretta operatività delle attività aziendali, si procede in caso di assenza prolungata od impedimento dell'utente.

L'RSI è autorizzato a collegarsi e visualizzare in remoto, previa comunicazione all'utente, il desktop delle singole postazioni di personal computer al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, e simili. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, fatta salva l'urgenza di procedere per non pregiudicare l'efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito il collegamento mediante dispositivi non aziendali alla rete informatica aziendale salvo specifica richiesta da parte del responsabile di funzione/unità operativa e conferma dell'RSI. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'RSI per conto dell'Azienda, né è consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, a fronte del grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza della precedente disposizione espone sia l'Azienda sia l'utente a gravi responsabilità civili; inoltre 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 non protetto dal diritto d'autore, sono sanzionate penalmente.

Salvo preventiva espressa autorizzazione dell'RSI, non è consentito all'utente modificare le caratteristiche impostate sul personal computer né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (a titolo esemplificativo masterizzatori, modem, dispositivi di memorizzazione, ecc.).

È autorizzato il solo uso di dispositivi esterni forniti dall'Azienda. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'RSI nel caso in cui siano rilevati virus ed adottando quanto previsto dai successivi articoli del presente Regolamento relativamente alle procedure di protezione antivirus.

Il personal computer deve essere spento: ogni sera prima di lasciare la sede di lavoro ed in caso di inutilizzo per un periodo prevedibilmente prolungato, salvo indicazioni contrarie da parte dei responsabili del servizio stesso o del servizio di assistenza ai Sistemi Informativi.

Il Personal Computer non va lasciato incustodito e per evitare l'utilizzo improprio da parte di altri soggetti è necessario attivare il blocco con la richiesta password.

Nel personal computer non devono essere presenti file personali, quali ad esempio fotografie, file musicali, file video, file di attività extra lavorative. L'Azienda può monitorare la tipologia di file presenti e procedere, senza nessun preavviso, allo spostamento, alla messa in quarantena e/o alla rimozione degli stessi. Durante le operazioni di cambio / sostituzione del personal computer (ammodernamento del parco macchine), l'RSI rimuoverà, se presenti, tutti i file non inerenti all'attività lavorativa.

Non sono consentiti spostamenti di postazioni di lavoro, salvo formale richiesta da parte del responsabile di funzione/unità operativa e autorizzazione esplicita da parte dell'RSI.

ART. 7 - UTILIZZO DI PERSONAL COMPUTER PORTATILI

Ai personal computer portatili si applicano integralmente le norme di cui all'articolo precedente con esclusione del solo ultimo comma.

L'utente è responsabile del personal computer portatile assegnatogli dall'RSI e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

I personal computer portatili utilizzati all'esterno devono essere custoditi con la massima diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare accessi ai dati da parte di soggetti non autorizzati, danni o sottrazioni.

II portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.

I personal computer portatili devono essere restituiti all'RSI al termine del rapporto.

In caso di smarrimento o furto, è necessario effettuare denuncia presso le forze dell'ordine consegnando una copia della stessa alla Direzione.

ART. 8 - UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

Tutti i supporti magnetici rimovibili forniti dall'Azienda (dischetti, CD e DVD riscrivibili, supporti USB, SSD ecc.), contenenti dati particolari nonché informazioni costituenti patrimonio aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici e digitali rimovibili contenenti dati particolari, ciascun utente dovrà contattare l'RSI e seguire le istruzioni da questo impartite.

In ogni caso, i supporti magnetici e digitali contenenti dati particolari devono essere dagli utenti adeguatamente custoditi in armadi chiusi a chiave.

È vietato l'utilizzo di supporti rimovibili personali, salvo i casi espressamente autorizzati dall'RSI

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

ART. 9 - UTILIZZO DEGLI APPLICATIVI INFORMATICI

Gli applicativi informatici per la gestione informatizzata delle attività aziendali sono strumenti di lavoro.

Il loro utilizzo è consentito previa autenticazione personalizzata e profilazione per le funzioni allo specifico applicativo aziendale.

È vietato ogni utilizzo non inerente all'attività lavorativa con la correlata responsabilità dell'utente in ogni caso di violazione.

ART. 10 - UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.

L'utente assegnatario è responsabile del corretto utilizzo della propria casella di posta elettronica.

Eventuali controlli a campione sui contenuti delle e-mail potranno essere effettuati dall'Azienda, adottando il principio di liceità e necessità come stabilito dal Garante per la protezione dei dati personali (deliberazione del n.13 del 1.3.2007).

L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del responsabile di funzione/unità organizzativa. Lo stesso responsabile è tenuto a dare tempestiva comunicazione nel caso di revoca e/o trasferimento degli utenti della propria funzione/unità organizzativa.

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. A titolo esemplificativo l'utente non può utilizzare la posta elettronica per:

- invio e/o il ricevimento di allegati contenenti filmati o brani musicali (mp3) non legati all'attività lavorativa;
- invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- inviare o memorizzare messaggi (interni ed esterni) con contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita o non conforme ai doveri di correttezza e buona fede.
- invio e/o il ricevimento di qualsiasi Informazione o materiale che sia offensivo, abusivo, indecente, osceno, ovvero costituisca minaccia o violi la privacy, il diritto d'autore o altri diritti legalmente tutelati;
- partecipazione a catene telematiche (o di Sant'Antonio);

Se si dovessero peraltro ricevere messaggi di tale tipo, si deve darne comunicazione immediatamente all'RSI; 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 in particolare gli allegati ingombranti.

La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, conseguentemente, non deve essere utilizzata per inviare documenti o dati di lavoro contenenti dati particolari.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus o ransomware, è obbligatorio cancellare i messaggi senza aprirli avvisando l'RSI.

È obbligatorio controllare e porre la massima attenzione nell'aprire i file allegati ai messaggi di posta elettronica prima del loro utilizzo. Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .cab, .exe, .scr, .pif, .bat, .cmd, altro) o collegamenti a siti web o ftp per lo scarico di file, questi ultimi non devono essere aperti e i messaggi devono essere cancellati.

Per la trasmissione di file è opportuno utilizzare le cartelle condivise; è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono mai superare i 50 MB, anche facendo ricorso ai più comuni formati compressi (*.zip, *.rar).

È fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal dovere di riservatezza cui sono tenuti i dipendenti e collaboratori in ottemperanza agli obblighi di diligenza, fedeltà e correttezza. È obbligatorio mantenere la firma impostata dall'RSI per ogni utente, inclusa la clausola di riservatezza delle informazioni che si riporta integralmente:

Informativa Privacy - Ai sensi del Reg. UE 679/16 in tema di Privacy si precisa che le informazioni contenute in questo messaggio sono riservate e ad uso esclusivo del destinatario. Qualora il messaggio in parola Le fosse pervenuto per errore, La preghiamo di eliminarlo senza copiarlo e di non inoltrarlo a terzi, dandocene gentilmente comunicazione. Grazie.
I messaggi inviati e ricevuti alla presente casella di posta hanno natura non personale e possono essere conosciuti dall'organizzazione di appartenenza (Navigazione Lago d'Iseo S.r.l.) ai sensi del proprio Regolamento per l'utilizzo dei sistemi informatici aziendali disponibile all'interno del sito www.navigazionelagoiseo.it nella sezione "Società Trasparente"

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, il sistema, in caso di assenze programmate (ferie, permessi, attività di lavoro fuori sede dell'assegnatario della casella) può inviare automaticamente messaggi 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.

Sarà comunque consentito al responsabile della funzione/unità organizzativa dell'utente, preventivamente sentito quest'ultimo, o comunque a persona individuata dall'Azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

L'RSI o altro personale esterno a ciò incaricato, al fine di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le finalità indicate nel presente Regolamento o dalla legge.

L'Azienda potrà avere accesso alla posta elettronica dell'utente in conformità agli articoli 15 e 16 del presente Regolamento.

ART. 11 - UTILIZZO DELLA RETE INTERNET

È vietata la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

L'utente è direttamente e pienamente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine Internet ai quali abbia stabilito un collegamento tramite link.

A titolo 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 o http, se non strettamente attinenti all'attività lavorativa;
- 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 dal responsabile della funzione/unità organizzativa e/o dall'Ufficio Sistemi Informativi e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum o Social Network non professionali e l'utilizzo di chat line (esclusi gli strumenti autorizzati);
- inviare, ricevere, caricare, scaricare, utilizzare ovvero riutilizzare qualsiasi Informazione o materiale che sia offensivo, abusivo, indecente, osceno, ovvero costituisca minaccia o violi la privacy, il diritto d'autore o altri diritti legalmente tutelati.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda adotta uno specifico sistema di blocco o filtro automatico per prevenire determinate operazioni quali l'accesso a determinati siti inseriti in una black list.

I controlli effettuati dall'Azienda anche a mezzo dell'RSI potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi, e comunque per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

ART. 12 - UTILIZZO DI TELEFONI, FAX, SCANNER E FOTOCOPIATRICI AZIENDALI

Il telefono aziendale o palmare in dotazione all'utente è uno strumento di lavoro.

Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono aziendale a disposizione.

Qualora venisse assegnato un palmare o un telefono aziendale all'utente, previa autorizzazione rilasciata dalla Direzione, l'utente stesso sarà responsabile del suo utilizzo e della sua custodia.

Ai dispositivi sopra menzionati si applicano le medesime regole dell'art. 11 per l'utilizzo della rete Internet.

È vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere telefonate o messaggi di natura personale o comunque non pertinenti allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta.

È vietato l'utilizzo dei fax aziendali per fini personali sia per spedire sia per ricevere documentazione, salva diversa esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.

È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.

In caso di smarrimento o furto dei telefoni aziendali, è necessario effettuare denuncia presso le forze dell'ordine consegnando una copia della stessa alla Direzione.

ART. 13 - PROTEZIONE ANTIVIRUS

Il sistema informatico dell'Azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque verificare la presenza dell'antivirus nei propri dispositivi e tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, spegnere il personal computer e segnalare prontamente, attraverso gli opportuni canali, l'accaduto al Responsabile dei Sistemi Informativi.

Ogni dispositivo magnetico e digitale di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'RSI.

ART. 14 - OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

Tutti i soggetti a cui si applica il presente Regolamento devono osservare le disposizioni in materia di protezione dei dati personali e le misure minime per la sicurezza ai sensi del Codice della Privacy (D.Lgs. 30.6.2003, n. 196) e del Regolamento (CE) 27.4.2016 n. 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

ART. 15 - ACCESSO AI DATI TRATTATI DALL'UTENTE

È facoltà dell'Azienda accedere, nel rispetto della normativa sulla privacy, a tutti gli strumenti aziendali ed alle informazioni ed ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico, per esigenze produttive, organizzative e di sicurezza, in particolare per garantire la massima sicurezza del sistema, per garantire la costante e corretta operatività delle attività aziendali, per eseguire le attività e gli adempimenti necessari alla instaurazione, gestione e cessazione del rapporto di lavoro o di collaborazione; per controllare il rispetto della normativa (in particolare nei seguenti ambiti: tutela dei dati personali; tutela ambientale, responsabilità penale delle imprese – d.lgs. n. 231/2001), esercitare diritti in sede giudiziaria (con riferimento a contenziosi in atto o a situazioni precontenziose).

L'accesso è consentito per motivi di sicurezza e gestione del sistema informatico e telematico, per motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, altro, per finalità di controllo e programmazione dei costi aziendali (quali verifica dei costi di connessione ad Internet, traffico telefonico, ecc.), di continuità del servizio.

L'accesso è inoltre consentito nell'ambito del sistema di controlli di cui all'articolo seguente.

I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il titolare del trattamento è la Società NAVIGAZIONE LAGO D'ISEO S.R.L. avente sede legale a Costa Volpino (BG) in via Nazionale n. 16, telefono 035971483 ed e-mail info@navigazionelagoiseo.it.

ART. 16 - SISTEMA DI CONTROLLI GRADUALI

I controlli sono finalizzati a prevenire e ricercare rischi e fonti di danno alla sicurezza aziendale, mantenere la continuità del servizio, per eseguire le attività e gli adempimenti necessari alla instaurazione, gestione e cessazione del rapporto di lavoro o di collaborazione; verificare e garantire il rispetto della normativa (in particolare nei seguenti ambiti: tutela dei dati personali; tutela ambientale, responsabilità penale delle imprese – d.lgs. n. 231/2001), esercitare diritti in sede giudiziaria (con riferimento a contenziosi in atto o a situazioni precontenziose), controllare l´effettivo adempimento della prestazione lavorativa, controllare il corretto utilizzo degli strumenti di lavoro, esercitare procedimenti disciplinari e comminare le eventuali sanzioni, verificare e garantire il rispetto del presente Regolamento.

In caso di anomalie il Responsabile dei Sistemi Informativi effettuerà controlli anonimi, che si concluderanno con avvisi generalizzati diretti agli operatori dell'area o del settore in cui è stata rilevata l'anomalia e nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali con invito agli interessati di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti dall'Azienda solo in caso di successive ulteriori anomalie. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

L'Azienda potrà effettuare controlli mirati in caso di specifiche segnalazioni ed in ogni caso in cui vi siano elementi che possano far sospettare abusi o gravi violazioni al presente Regolamento ed agli obblighi di diligenza, fedeltà e correttezza.

ART. 17 – SANZIONI

È fatto obbligo a tutti gli utenti di osservare le disposizioni del presente Regolamento.

Il mancato rispetto o la violazione delle disposizioni regolamentari è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari applicabili conformemente alla normativa di legge ed alla contrattazione collettiva.

L'azienda si riserva la facoltà di agire tramite tutte le azioni civili e penali consentite.

A titolo esemplificativo si richiama l'attenzione sulle seguenti norme del codice penale: art. 595, artt. 600-ter e segg., art. 615-ter, art. 615-quarter, art. 615-quinques, art. 617-quarter, art. 617- quinquies, art. 617-sexies, art. 635-bis, art. 635-ter, art. 635- quarter, art. 635-quinquies, art. 640 ed art. 640 ter) e sulla conseguente gravità delle conseguenze che possono derivare dalla violazione del presente Regolamento.

NORME FINALI

ART. 18 - NORMA DI RINVIO

Per tutto quanto non previsto dal presente Regolamento si rinvia alla normativa in vigore.

ART. 19 - ENTRATA IN VIGORE

Il regolamento entrerà in vigore il 23/02/2021, salvo successive modifiche ed integrazioni. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Il presente Regolamento è affisso nella bacheca aziendale in Direzione di Esercizio.

Il presente Regolamento viene consegnato ad ogni utente, che provvederà a rilascerà apposita ricevuta, e potrà essere consultato da ciascun interessato all'interno del portale Aziendale nella sezione "11-Regolamenti e procedure".