REGOLAMENTO INFORMATICO

(Regolamento per l'utilizzo della strumentazione informatica e della rete Internet)

CASA DELL'IMMACOLATA
DI DON EMILIO DE ROJA
FONDAZIONE

FONDAZIONE CASA DELL'IMMACCOLATA DI DON EMILIO DE ROJA ETS
VIA CHISIMAIO, 40 - 33100 UDINE (UD), IT

STATO DELLE REVISIONI

Rev.	Data	Descrizione delle modifiche	Approvazione
00	20/09/2021	Emissione del documento	CdA
01	28/11/2023	Revisione del documento	CdA

SOMMARIO

Sommario2

Capo I – PRINCIPI4

Art. 1 – Introduzione, Definizioni e Finalità4

Art. 2 – Ambito di applicazione4

Art. 3 – Titolarità dei beni e delle risorse informatiche4

Art. 4 – Responsabilità personale dell'utente5

Art. 5 – Controlli5

Capo II — MISURE ORGANIZZATIVE6

Art. 6 – Amministratori di sistema6

Art. 7 – Assegnazione degli account e gestione delle password7

7.1 – Creazione e Gestione degli Account7

7.2 – Gestione e Utilizzo delle Password7

*7.3 – Cessazione Degli Account*8

Art. 8 – Postazioni di lavoro8

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI9

Art. 9 – Dispositivi (9999

Art. 10 – Software10

ART 11 – Dispositivi mobili di connessione (internet key e linea di backup)11

Art. 12 – Dispositivi di memoria portatili11

Art. 13 – Stampanti, fotocopiatrici e fax11

Art. 14 – Strumenti di fonia mobile o di connettività in mobilità12

Capo IV — GESTIONE DELLE COMUNICAZIONI TELEMATICHE13

Art. 15 – Gestione utilizzo della rete internet13

Art. 16 – Gestione e utilizzo della posta elettronica aziendale15

Capo V — SANZIONI, COMUNICAZIONI, APPROVAZIONE16

Art. 17 – Sanzioni16

Art. 18 – Informativa agli utenti ex art. 13 Regolamento (UE) 20161616

Art. 19 – Comunicazioni16

Art. 20 – Approvazione del Regolamento**Errore. Il segnalibro non è definito.**

CAPO I – PRINCIPI

Art. 1 – Introduzione, Definizioni e Finalità

Il presente regolamento ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori ecc.) al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre la società a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.

A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1° marzo 2007).

Art. 2 – Ambito di applicazione

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative della società.

Per **utente** pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per **ente** si intende, invece, la società, l'organizzazione, lo Studio e in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art. 3 – Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative (es. browser, pc fissi, notebook, smartphone, telefonia fissa, nas/server, account di posta elettronica, client di posta, tutti i dati e/o le informazioni ivi contenuti, e così via) costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'ente.

Ciò considerato, il loro utilizzo è consentito solo ed esclusivamente per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti all'attività svolta per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi aziendali ovvero per esigenze organizzative, produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale.

Ne consegue che è fatto espresso divieto di utilizzare tali strumenti per fini personali ovvero per fini diversi da quelli sopra indicati.

A tal fine si precisa sin d'ora che qualsivoglia dato 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. 4 – Responsabilità 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 e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale da utilizzi impropri o non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.

Ogni utente è tenuto ad operare a tutela della sicurezza informatica aziendale, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente.

Art. 5 – Controlli

L'ente esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori).

Ciononostante non si esclude che si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro. Per tali evenienze sarà onere dell'ente sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali ovvero, in assenza di queste, con la commissione interna. In difetto di accordo e su istanza dell'ente è l'ispettorato del lavoro ad indicare le modalità per l'uso di tali impianti.

Nel caso in cui gli impianti o gli strumenti dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori siano utilizzati dal lavoratore per rendere la prestazione lavorativa ovvero siano strumenti di registrazione degli accessi e delle presenza, l'Ente, secondo quanto stabilito dall'art. 4 dello Statuto dei Lavoratori, non procederà con alcuna forma di accordo sindacale ovvero altra forma di autorizzazione da parte della DTL, ma si limiterà a rendere edotto adeguatamente il lavoratore sulle modalità d'uso di tali strumenti e sulle modalità di effettuazione dei controlli, ovviamente nel rispetto del GDPR e del D.Lgs 196/2003.

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.

L'ente, riservandosi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), potrà agire in base al principio della gradualità. In attuazione di tale principio:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
- Nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, potrà

essere diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa 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 ovvero sin da subito qualora ritenuto opportuno e necessario, l'Ente procederà con verifiche più specifiche e puntuali, anche su base individuale.

L'ente titolare non può in alcun caso utilizzare sistemi costruiti esclusivamente per porre in essere forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- 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.

Capo II — MISURE ORGANIZZATIVE

Art. 6 – Amministratori di sistema

L'ente, attualmente, non ha conferito ad un amministratore di sistema esterno il compito di sovrintendere ai beni e alle risorse informatiche aziendali, compito che attualmente viene svolto direttamente dagli organi di Governance dell'Ente.

I compiti dell'amministratore di sistema ovvero degli organi di Governance dell'Ente sono i seguenti:

- Gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;
- Gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- Monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Provvedere alla sicurezza informatica dei sistemi informativi aziendali;
- Utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di necessità per motivi di lavoro.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (o *designato*) all'interno dell'ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività

indifferibili per cui è stato richiesto. Si ricorda a tal proposito che i pc dell'Ente utilizzati dai singoli lavoratori, per regolamento aziendale, sono vuoti; tutti gli utenti accedono direttamente alle cartelle condivise dai server virtuali; mentre gli account di posta non sono personali ma vengono utilizzati contemporaneamente da più utenti (o lavoratori).

Se necessario, potrà essere redatto un elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, aggiornato con cadenza annuale ovvero ogni volta che si rilevino modifiche.

Art. 7 – Assegnazione degli account e gestione delle password

7.1 – 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 vengono creati dagli amministratori di sistema o dai responsabili interni designati dell'ente e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", solitamente username e password, comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.

Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi.

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, è tenuto ad informare il Titolare e modificare successivamente la password ed a segnalare la violazione al responsabile privacy di riferimento.

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze organizzative o produttive aziendali o per la sicurezza e operatività delle risorse informatiche, per la sicurezza del lavoro o per la tutela del patrimonio aziendale, l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente.

I beni e la strumentazione informatica oggetto del presente regolamento rimangono di esclusivo dominio dell'ente, che in conseguenza dei rapporti instaurati con gli utenti ne disciplina l'assegnazione.

La validità delle credenziali di posta elettronica permane indefinitamente nel tempo, mentre, per le attività di file sharing, la scadenza e il successivo aggiornamento delle credenziali avviene ogni 3 mesi.

7.2 – Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione all'utente, la password dovrà essere modificata ogni 12 mesi.

Nel definire il valore della password, occorre rispettare le seguenti regole:

- Utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, ecc.), di cui almeno uno numerico;
- La password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#$£$%...";
- Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
- Evitare l'utilizzo di password comuni o prevedibili;
- Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;

Scrivere la password su post-it o altri supporti non è conforme alla normativa, compromette in maniera pressoché totale le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

7.3 – Cessazione Degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno disabilitate.

Art. 8 – Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (*device*) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici aziendali 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 seguenti regole tecniche:

- Ogni pc, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (*device*), 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 all'attività svolta.
- È dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente.
- 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 necessario presentare espressa richiesta al proprio responsabile di riferimento, il quale ne valuterà i requisiti tecnici, l'aderenza alle policy interne e al ruolo ricoperto in azienda.
- Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti 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 all'amministratore di sistema o al proprio responsabile di riferimento eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature ed i beni informatici aziendali a soggetti terzi.

- L'ente si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.
- Nel caso in cui il sistema rilevi la presenza di un virus sulla stazione di lavoro contattare immediatamente il personale di competenza.
- Sottoporre a scanning antivirus i supporti provenienti da terzi (ad es. floppy, CD, etc..) prima di scaricarne il contenuto sui sistemi dell'Università.
- Non disattivare o disinstallare il software antivirus mantenuto aggiornato centralmente presente sulla propria stazione di lavoro.
- Non operare modifiche alla configurazione degli strumenti informatici in dotazione senza l'autorizzazione del personale preposto.
- Conservare i dati idonei a rivelare lo stato di salute in archivi elettronici o cartacei separati da altri dati personali
- Far circolare i documenti cartacei contenenti dati personali sensibili unicamente in busta chiusa.
- Conservare i documenti ed i supporti informatici removibili in luoghi ad accesso controllato (ad es. locali ad accesso selezionato, contenitori o armadi muniti di serratura etc...) con modalità tali che vi possa accedere unicamente personale autorizzato (saranno identificati e registrati i soggetti eventualmente ammessi all'accesso negli archivi dopo l'orario di chiusura)
- Liberare le scrivanie a fine giornata e nelle pause prolungate da documenti contenenti dati sensibili o riservati
- Riprodurre i dati (creando copie degli archivi, fotocopiando documenti, etc.) per le proprie esigenze lavorative solo se è strettamente necessario e, comunque, rispettando i criteri di sicurezza validi per i dati/documenti originali
- Procedere alla cancellazione/distruzione delle copie di dati riprodotte non appena possibile al fine di evitare la proliferazione incontrollata di archivi contenenti dati personali
- Distruggere i documenti, quando non più necessari, rendendoli illeggibili, ricorrendo, ove possibile, all'utilizzo del trituratore
- Garantire adeguata custodia dei documenti e dei supporti informatici che contengono dati personali anche all'esterno dell'Ente (ad es. in viaggio, etc.).

Gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche aziendali salvo preventiva autorizzazione dell'ente.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9 – Dispositivi (*devices*): Desktop, Laptop, Tablet, Smartphone, ecc.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (*devices*) di proprietà dell'ente e sono tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio dispositivo (*device*), se non previa esplicita autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni);

- Non è consentito rimuovere, danneggiare o asportare componenti hardware;
- Non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'ente;
- È onere dell'utente, in relazione alle sue competenze lavorative, 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 all'amministratore del sistema o al proprio responsabile di riferimento;
- È onere dell'utente spegnere il proprio PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della loro riconsegna;
- Non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.
- Evitare di salvare dati personali presenti su banche dati centralizzate sul proprio disco fisso. In caso di banche dati estemporanee salvare provvisoriamente i dati sul Nas. Se si vuole per praticità utilizzare il desktop, si consiglia di creare sullo stesso dei collegamenti a files o cartelle presenti sui server virtuali.
- Qualora fosse necessario trattare i dati sul proprio disco fisso, avvisare immediatamente il Titolare.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

Art. 10 – 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 le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni) per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio *freeware* o *shareware*.

Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun utente è tenuto a osservare per un corretto utilizzo del software in azienda:

- Le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto 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 sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza.
- Non è consentito eseguire il download o l'upload di software non autorizzato.
- Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.
- La duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

ART 11 – Dispositivi mobili di connessione (internet key e linea di backup)

Agli assegnatari di computer o dispositivi portatili, in casi strettamente eccezionali, può essere concessa in dotazione anche una chiavetta per la connessione alla rete aziendale per consentire lo svolgimento delle mansioni lavorative anche da remoto.

I suddetti dispositivi mobili di connessione devono essere utilizzati esclusivamente sui computer forniti in dotazione dall'ente e non è consentito concederne l'utilizzo a soggetti terzi né utilizzarli su altri computer sia personali che di terzi.

Le specifiche relative ai limiti entro cui l'utente potrà utilizzare il servizio offerto tramite la chiavetta sono riportate nella scheda tecnica consegnata all'utente unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti; in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

In caso di mancanza della rete internet aziendale, gli utenti devono collegarsi alla linea di backup con i dispositivi hardware forniti dall'Ente. Questo permetterà il normale svolgimento dell'attività lavorativa fino al ripristino delle normali condizioni lavorative.

Art. 12 – 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: CD-ROM, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.

L'utilizzo di tali dispositivi è inibito e non autorizzato sui pc aziendali. Nei casi in cui l'utilizzo di tali supporti sia stato autorizzato, l'utente dovrà rispettare il presente regolamento e le seguenti direttive:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati dall'ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni);
- è onere dell'utente custodire i supporti contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto;
- formattare i supporti informatici removibili, quando i dati sensibili ivi salvati non sono più necessari, prima di riutilizzarli. Qualora ciò non fosse possibile distruggere fisicamente i supporti.

Art. 13 – Stampanti, fotocopiatrici e fax

L'utilizzo di tali 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.

Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Gli strumenti dotati di memoria, connessi o meno in rete, sono gestiti da ogni utente a cui sono stati affidati e che provvederanno alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

Art. 14 – Strumenti di fonia mobile o di connettività in mobilità

L'ente rende disponibile presso l'ufficio impianti di telefonia fissa e mobile che consentono, se necessario, di usufruire sia della navigazione in Internet tramite rete dati che del servizio di telefonia tramite rete mobile. L'ente non rende disponibile smartphone e tablet personali.

L'utente potrà utilizzare tali strumenti solamente presso l'ufficio in quanto tali device devono restare a disposizione di tutto il personale. Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi. Tali strumenti propri di Titolare, Soci o altro personale responsabile dell'Ente che si collegano ai client di posta aziendali e/o all'archivio centrale dei dati vanno protetti con quanto di seguito descritto.

L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

- Ciascun utente è responsabile dell'uso appropriato degli stessi, e conseguentemente, anche della loro diligente conservazione;
- I dispositivi devono essere dotati di password di sicurezza, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:

    - il codice PIN dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione;
    - il codice PIN o altri codici di accesso dovranno essere modificato con cadenza al massimo di 12 mesi;
    - ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'ente.

- In caso di furto, danneggiamento o smarrimento del dispositivo mobile si dovrà darne immediato avviso all'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso 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 cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;
- Non è consentito 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 o almeno ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo per la riparazione;
- Non è consentito all'utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano preventivamente autorizzate dall'ente.
- Informare l'interessato quando, nel corso di una conversazione, sono utilizzati dispositivi che

consentono l'ascolto della conversazione stessa da parte di altri soggetti (es. dispositivi viva-voce).

Art. 15 – Strumenti software aziendali

L'ente possiede una serie di strumenti informatici dedicati, sviluppati appositamente per implementare gli specifici processi facenti parte della propria attività. Tali strumenti sono dati a disposizione del dipendente/collaboratore secondo necessità dei rispettivi incarichi.
L'accesso a tali strumenti è regolato dalla consegna da parte dell'ente delle credenziali di accesso al dipendente, secondo natura dello strumento tali password possono essere modificate o meno. L'accesso è comunque sempre nominale e non deve essere ceduto nemmeno temporaneamente ad altri dipendenti/collaboratori né tantomeno a persone terze.

È fatto divieto di eseguire qualsiasi operazione di modifica degli strumenti consegnati, devono essere utilizzati esclusivamente secondo istruzioni ricevute.

Gli strumenti qui citati si raggruppano in due categorie: strumenti centralizzati (installati presso server di proprietà dell'ente o erogati da terzi in modalità "cloud") e strumenti locali (installati su dispositivi in dotazione al dipendente).

- Strumenti centralizzati
  L'accesso è strettamente regolato da credenziali personali (utente e password), possono essere accessibili da qualsiasi collegamento internet, oppure solo dalla rete privata dell'ente.
- Strumenti locali
  Si tratta di software che richiedono l'installazione locale sulle postazioni (fisiche o virtuali) di lavoro degli utenti, compresi eventuali dispositivi mobili (portatili, smartphone …) l'installazione verrà eseguita da personale tecnico incaricato, salvo diverse direttive dell'ente corredate da specifiche e dettagliate istruzioni operative.
  Per entrambe le categorie l'uso è consentito esclusivamente secondo istruzioni e formazione ricevuta, l'accesso ai dati o comunque informazioni aziendali tramite tali strumenti sono da intendersi sempre confidenziali e vincolate agli obblighi di riservatezza descritti nel presente documento. È espressamente fatto divieto di compiere attività di reverse-engineering e tentativi di accesso agli eventuali dati memorizzati localmente sul dispositivo dell'utente.

Capo IV — GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 15 – Gestione utilizzo della rete internet

Alcuni utenti potranno essere abilitati alla navigazione Internet e pertanto li si richiama a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'ente.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere

governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in odo da prendere ogni precauzione conseguente.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- L'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- 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;
- 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);
- Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- È consentito l'utilizzo di soluzioni di Instant Messanger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente;
- Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- Non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro.
- 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 preventivamente ed espressamente approvata.
- Accedere a Internet utilizzando solo i servizi per cui si è abilitati
- Accedere a Internet unicamente per mezzo di connessioni che si avvalgano del canale centralizzato reso disponibile dalle strutture di competenza
- Navigare in rete in modo etico e solo al fine di migliorare il proprio lavoro
- Declinare le proprie generalità in modo veritiero e non fittizio quando richiesto da siti esterni
- Rispettare la tutela del copyright anche per i programmi scaricabili gratuitamente dalla rete. Ciò deve valere anche per lo scarico di materiale mediatico (es. immagini, …)
- Non mettere a disposizione materiale a carattere inappropriato od offensivo cui è comunque vietato accedere
- Non mettere a disposizione materiale riservato o di proprietà dell'Ente se non esplicitamente autorizzati
- Osservare sempre le regole dell'Ente per tutelarsi da eventuali virus presenti sulla rete (vedi paragrafo Antivirus)
- Nessun modem o dial-up router può essere installato autonomamente dagli utenti senza il consenso del Responsabile

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'ente.

Per mezzo dell'Amministratore di Sistema o di un responsabile incaricato dall'ente e al fine di facilitare il rispetto delle predette regole l'ente si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

Art. 16 – Gestione e utilizzo della posta elettronica aziendale

I servizi di posta elettronica devono essere utilizzati a scopo professionale: l'account e-mail non è nominativo (personale), è uno strumento di proprietà dell'ente ed è conferito in uso agli utenti per l'esclusivo svolgimento delle mansioni lavorative affidate. La password di accesso è annegata nel pc con modifica ogni 12 mesi da parte dell'Amministratore del sistema o da personale incaricato.

Ogni utente ha accesso a più caselle di posta elettronica che sono condivise con altri utenti dello stesso settore aziendale. Tali caselle di posta elettronica devono essere utilizzate esclusivamente per le comunicazioni aziendali.

Attraverso le caselle e-mail aziendali 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 positivamente l'immagine aziendale.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente alle presenti regole. Ad integrazione della formazione già effettuata e degli ordini di servizio affissi in bacheca relativi a tale argomento, si ricorda che gli utenti devono:

- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- se necessario, utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- leggere ogni giorno la posta in arrivo e gestire le pratiche per quanto di competenza e segnalare eventuali mail che esulano dalla propria competenza.
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
- ransomware e malware: ad integrazione degli altri ordini si servizio esposti in bacheca, qualora una mail provenga da un indirizzo di posta elettronica conosciuto di un cliente o fornitore e sia scritta in italiano non corretto ovvero, anche se scritta in italiano corretto, sia molto breve (es. verifica allegato e conferma…) e contenga un allegato ovvero un link, non aprirla, telefonare al cliente o fornitore per sapere se sia stata da questi inviata e segnalare il fatto al responsabile.
- 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;
- rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.

Inoltre, non è consentito agli utenti:

- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video aziendali.

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".

Occorre infine che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.

Nei casi in cui l'ente si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

Capo V — SANZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 17 – Sanzioni

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori), nonché dal CCNL applicato (cfr. sopra anche cap. su registrazione accessi...).
Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.
In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti 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 o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

Art. 18 – Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento (UE) 2016/679.

Art. 19 – Comunicazioni

Contestualmente all'assegnazione di un account sul pc il presente regolamento è messo a disposizione degli utenti per la consultazione. La versione più aggiornata dello stesso è pubblicata sia in formato immateriale digitale che in formato fisico cartaceo allo scopo di facilitarne la diffusione a tutti gli interessati, ed inviata a mezzo posta elettronica.
Per ogni aggiornamento del presente regolamento sarà data comunicazione sulle bacheche aziendali e tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata.

Art. 20 – Approvazione del Regolamento

Il presente regolamento è stato approvato dal Consiglio di amministrazione dell'ente in data 18 dicembre 2023, in ottemperanza a quanto previsto dall'art. 4 dello Statuto dei Lavoratori.