Disciplinare interno per l'utilizzo dei sistemi e strumenti informatici all'interno di COMUNE DI VERZUOLO

ai sensi del Regolamento (UE) 2016/679

del Parlamento Europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Sommario

Premessa

COMUNE DI VERZUOLO (di seguito "Titolare") ha disposto che al proprio interno venga osservato il presente disciplinare tecnico.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi di **diligenza e correttezza,** comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il Titolare ha adottato un disciplinare interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i designati in attuazione del Regolamento Europeo sulla protezione dei dati (da ora in poi GDPR 2016/679), nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del GDPR 2016/679, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4, comma 3° dello Statuto dei lavoratori.

Il Titolare rende noto che PIERMARIA MONASTEROLO della **LEONARDO TEC** è stato autorizzato a compiere, direttamente o attraverso collegamento in remoto, interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.). In particolare, potrà trattare i suoi dati personali, in ottemperanza dei propri compiti, PIERMARIA MONASTEROLO, in qualità di Amministratore di Sistema per il titolare del trattamento, ai sensi del Provvedimento dell'Autorità Garante *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle*

attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008 Le medesime facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Titolare, si applicano anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, ne verrà data comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

Copia del disciplinare, oltre ad essere affisso in bacheca anche per quanto prevede l'art.7 della Legge n. 300/1970, verrà consegnato a ciascun dipendente, anche ai fini dell'art. 13 del GDPR 2016/679 e dell'art. 4, comma 3°, dello Statuto dei lavoratori, e sarà messo a disposizione di amministratori, collaboratori, consulenti, tirocinanti, od altri responsabili esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale il Titolare, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.

Campo di applicazione del disciplinare

Il presente disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti del Titolare a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori, tirocinanti, prestatori d'opera intellettuale, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile esterno del trattamento" o "terzo", ai sensi dell'art. 4 comma 10 del GDPR 2016/679, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale od a favore del Titolare stesso.

1. Utilizzo del Personal Computer

1.1. Il personal computer affidato all'utente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

1.2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Titolare solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 2 del presente disciplinare.

1.3. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone il Titolare a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico del Titolare, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

1.4. Salvo preventiva espressa autorizzazione del Titolare, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).

1.5. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare o il Responsabile del trattamento nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 7 del presente disciplinare relativo alle procedure di protezione antivirus.

1.6. Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In caso di allontanamento per breve lasso di tempo, non lasciare accessibile il personal computer: impostare un salvaschermo (screen saver) automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

2. Gestione e assegnazione delle credenziali di autenticazione

2.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Titolare o Responsabile del trattamento.
2.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà venir **custodita dal designato con la massima diligenza e non divulgata**.
2.3. La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri alfanumerici e non deve contenere riferimenti agevolmente riconducibili al designato.
2.4. È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo. Successivamente, ogni tre mesi,il sistema determina di default un termine di validità delle password: qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personale computer e/o al sistema verrà temporaneamente bloccato.

3. Utilizzo della rete informatica

3.1. Per l'accesso alla rete del Titolare ciascun utente deve utilizzare la propria credenziale di autenticazione.
3.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete.
3.3. L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.
3.4. Le cartelle utenti presenti nei server del Titolare sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale della LEONARDO TEC.
3.5. Il Titolare o Responsabile del trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei PC dei designati e delle unità di rete.
3.6. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.
3.7. Nella gestione dei sistemi informatici aziendali, la LEONARDO TEC potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate in premessa, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.
3.8. L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono impostate delle regole sul firewall che impediscono l'accesso di dispositivi non abilitati.
3.9. Il dipendente con contratto di telelavoro è tenuto al rispetto delle procedure elencate nel presente documento, ed in particolare alla cura e all'utilizzo responsabile della postazione di lavoro fornitagli dall'amministrazione, che riceve mediante comodato d'uso e dei cui danni è responsabile ai sensi dell'art. 2051 del codice civile, a meno che non provi il caso fortuito. Il telelavoratore è, altresì, tenuto al dovere di riservatezza su tutte le informazioni delle quali venga in possesso per il lavoro assegnatogli e di quelle derivanti dall'utilizzo delle apparecchiature, dei programmi e dei dati in essi contenuti nonché all'adozione di ogni accortezza tecnica e comportamentale atta a garantire la tutela ed il corretto uso dei dati trattati.
3.10. Il dipendente può essere autorizzato ad utilizzare, attraverso un programma di controllo remoto predisposto dall'Ente, attrezzature proprie come postazione di lavoro, purché compatibili dal punto di vista tecnico e di conformità alle norme di sicurezza con la prestazione da svolgere.

4. Utilizzo di altri dispositivi elettronici e supporti rimovibili

4.1. **Tutti i dispositivi elettronici e i supporti rimovibili dati in dotazione al personale devono considerarsi strumenti di lavoro,** non essendo consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative.

Fra i dispositivi in questione vanno annoverati i telefoni aziendali, PC portatili, tablet, chiavette USB, dischetti, CD e DVD riscrivibili, memorie esterne, ecc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere tramite essi alla rete del Titolare o di condividere documenti, dati e materiali ivi conservati e/o trattati.

4.2. L'utente resta responsabile nella custodia ex art 1768 cc del singolo dispositivo/supporto assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà avvisare il titolare senza ingiustificato ritardo a partire dalla scoperta fatto.

4.3. I supporti magnetici contenenti dati particolari devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

4.4. Viene severamente vietato l'utilizzo di supporti rimovibili personali.

4.5. Con riferimento ai telefoni aziendali e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile in conformità delle istruzioni al riguardo impartite dal Titolare del trattamento.

4.6. Si precisa, peraltro, che le disposizioni previste nel presente disciplinare ai punti 1, 4, 5, 6, 7 e 8 dello stesso trovano qui applicazione.

4.7. Viene infine disposto il divieto di utilizzo per fini personali di fax aziendali, per spedire o per ricevere documentazione, e/o di fotocopiatrici aziendali, salva diversa esplicita autorizzazione da parte del Titolare del trattamento.

4.8. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati particolari, ciascun utente dovrà rivolgersi al Titolare o Responsabile del trattamento e seguire le istruzioni da impartite. Nel caso di dispositivi elettronici dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordando comunque ogni opportuna azione al riguardo con il Titolare.

5. Uso della posta elettronica

5.1. **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

5.2. È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- L'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- L'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- La partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve procedere alla cancellazione e/o alla collocazione nella posta indesiderata. Nei casi ritenuti di particolare rilievo sarà cura del ricevente di comunicarlo immediatamente al Titolare o Responsabile del trattamento. In ogni caso, non si dovrà in alcun modo procedere all'apertura degli allegati a tali messaggi.

5.3. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza commerciale e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l'attività aziendale e non utili alle esigenze aziendali, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dal Titolare quale corrispondenza e documentazione lavorativa e non personale.

5.4. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

5.5. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere oggetto di trattamento esclusivo del destinatario.

5.6. Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che i messaggi ivi contenuti, avendo presuntivamente natura di corrispondenza commerciale, verranno conservati nei server aziendali a norma dell'art. 2220 del Codice civile per un periodo congruo alle finalità aziendali e non oltre ad anni 10.

5.7. È obbligatorio porre la massima attenzione nell'aprire i file attachement di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

5.8. La posta elettronica diretta all'esterno della rete informatica può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente riservati";

5.9. 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, l'utente, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) imposterà l'invio automatico messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura.

5.10. In caso di lunga assenza non programmata (ad es. per malattia) la procedura di cui al punto 5.9 - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail - verrà attivata a cura del Titolare o Responsabile del trattamento, qualora ritenuto necessario.

5.11. Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dal Titolare, di accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: assenza non programmata di cui al punto 5.9).

5.12. Il Titolare si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l'utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.

5.13. La casella di posta elettronica nominativa, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Il Titolare si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità aziendale; in tal caso:

- Avranno accesso alla casella esclusivamente dipendenti individuati dal Titolare in funzione alle mansioni lavorative assegnate;
- Verranno inviate mail ai mittenti con indicazione della diversa casella di posta elettronica aziendale cui trasmettete i messaggi.
- Viene escluso, comunque, l'invio di messaggi da tale casella di posta.

6. Navigazione in Internet

6.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**.

6.2. In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- L'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale della LEONARDO TEC);
- L'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati 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 non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati;

6.3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Titolare rende nota l'eventuale adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".

6.4. Gli eventuali controlli compiuti dal personale designato della LEONARDO TEC, 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 sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Titolare.

7. Protezione antivirus

7.1. Il sistema informatico del Titolare è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

7.2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso **senza spegnere il computer** nonché segnalare prontamente l'accaduto al Titolare del trattamento e/o ai centri assistenza informatica autorizzati con contratto vigente comunicati dal Titolare del trattamento.

7.3. Ogni dispositivo magnetico di provenienza esterna al Titolare dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale della LEONARDO TEC.

8. Partecipazioni a social media

8.1. L'utilizzo a fini promozionali e commerciali dei social media, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dal Titolare attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti.
L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare sui social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con la preventiva autorizzazione del Titolare del trattamento.

9. Osservanza delle disposizioni in materia di privacy

9.1. Gli strumenti tecnologici considerati nel presente disciplinare costituiscono strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte, anche conformemente al successivo punto 8, possono essere utilizzate per tutti i fini connessi al rapporto di lavoro, essendo stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potrebbero eventualmente essere compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

9.2. Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, il Titolare provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

10. Accesso ai dati trattati dall'utente

10.1. Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare del trattamento, tramite il personale designato o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure stabilite dal presente disciplinare, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

10.2. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

11. Sanzioni

11.1. È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

12. Aggiornamento e revisione

12.1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Disciplinare.
12.2. Il presente Regolamento è soggetto periodicamente a revisione.

Verzuolo, lì 27/09/2023

COMUNE DI VERZUOLO ★ Prov. di Cuneo ★

Il Titolare del trattamento
(timbro e firma leggibile)