Econord S.p.A.

Bodio Lomnago (VA)

DISCIPLINARE RELATIVO AL TRATTAMENTO DEI DATI

Regole di condotta ed obblighi dei dipendenti e collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica, comprensivo di note per la gestione dei dati cartacei.

Aggiornamento: Gennaio 2025

1. AMBITO GENERALE

1.1. Definizioni

Ente/Organizzazione: ECONORD S.p.A.

P. IVA/CF: 01368180129

Indirizzo: Via Giordani, 35 - Varese

Telefono: 0332/226336 **Email:** privacy@econord.it

Tipo attività:

- Progettazione e gestione dei servizi di igiene urbana
- Progettazione, realizzazione e gestione di piattaforme e impianti
- Costruzione e gestione di impianti di trattamento e smaltimento di rifiuti solidi urbani, speciali e pericolosi
- Recupero ambientale ed energetico

Regolamento (UE) 2016/679: Regolamento UE del Parlamento europeo e del Consiglio del 27.04.2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

D. Lgs. 196/2003: Decreto Legislativo 196 del 30 Giugno 2003 e sue successive modifiche ed integrazioni "Codice in materia di protezione di dati personali".

AND: accordo di non divulgazione.

Dipendente: personale dell'Ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Titolare del trattamento dei dati: ECONORD S.p.A

Incaricato: ogni dipendente o collaboratore o fornitore che, nell'ambito dell'attività assegnatagli, tratta dati di titolarità dell'Ente (nell'accezione del capitolo seguente).

Dispositivo aziendale: PC personale (fisso o portatile) o smartphone o tablet messo a disposizione dall'Ente all'Incaricato ai soli fini dell'attività lavorativa.

1.2. Premessa

L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "**informazioni**", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del D.Lgs. 196/2003 e del Regolamento (UE) .., "**dati personali**" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Ente adotti una serie di adeguate misure tecniche e organizzative.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, o per Accordo di non Divulgazione (AND), o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, l'Ente tratta "**dati cartacei**" ovvero informazioni su supporto cartaceo e "**dati digitali**" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature informatiche.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Ente.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

L'utilizzo delle tecnologie informatiche ed in particolare l'accesso alla rete internet dai dispositivi aziendali espone l'Ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'Ente ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.
Il presente Disciplinare Interno si applica a tutti i dipendenti, collaboratori o fornitori (di seguito indicati come **Incaricati**) che si trovino ad operare con dati di titolarità dell'Ente, sia se gestiti con le risorse informatiche aziendali (es. posta elettronica, navigazione internet), sia se gestiti in modalità cartacea o altro supporto non informatico.
Per risorse informatiche aziendali si intendono cellulari, tablet, PC fissi o portatili (di seguito detti **Dispositivi**), i servizi informatici aziendali quali la posta elettronica o i gestionali (di seguito detti **account**), nonché gli accessi alla navigazione in Internet.

Una gestione di tali dati che sia difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Analoghe considerazioni valgono nel caso in cui i dati siano gestiti eccezionalmente da dispositivi o account personali ossia non aziendali.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi della normativa sulla Privacy.

1.3. Esclusione all'uso delle risorse informatiche

All'inizio del rapporto lavorativo o di consulenza, l'Ente valuta la presenza dei presupposti per l'autorizzazione all'uso delle varie risorse informatiche da parte dei dipendenti o collaboratori.

Successivamente e periodicamente l'Ente valuta la permanenza dei presupposti per l'utilizzo degli stessi.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare tutte o parte delle risorse informatiche:

1. L'utilizzo del Computer o di altri Dispositivi ;
2. L'utilizzo della posta elettronica;
3. L'accesso a internet;
4. L'assegnazione di specifici account.

Le eventuali esclusioni sono strettamente connesse alla natura dell'attività lavorativa cui è designato l'Incaricato. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli Incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.

1.4. Linee guida per il trattamento dei dati personali

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.
Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Incaricato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.
Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

1.5. Titolarità dei Dispositivi e dei dati

L'ente è esclusiva titolare e proprietaria dei Dispositivi aziendali messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa.

L'Ente è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri Dispositivi aziendali o eccezionalmente mediante Dispositivi non aziendali, nonché archiviati in modo cartaceo nei propri locali o eccezionalmente presso altri locali non aziendali.

L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei Dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, o altre tipologie di files) siano privati o personali, né può presumere che i dati in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

1.6. Finalità nell'utilizzo dei Dispositivi

I Dispositivi assegnati dall'Ente sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo, non possono quindi essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questo Ente, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.7. Restituzione dei Dispositivi e dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'Ente, della permanenza dei presupposti per l'utilizzo dei Dispositivi e/o dei dati cartacei aziendali, gli Incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei Dispositivi in uso e/o dei dati cartacei in loro possesso di titolarità dell'Ente;
2. Divieto assoluto di formattare i Dispositivi o alterare o manomettere o distruggere i Dispositivi e/o i dati cartacei assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

2. PASSWORD E ACCOUNT

2.1. La password

La password è un metodo di autenticazione assegnato dall'organizzazione all'Incaricato che, in accoppiamento ad uno username, garantisce l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'Ente nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

In qualsiasi momento l'organizzazione si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2. Regole per la corretta gestione delle password

Per una corretta e sicura gestione delle password, l'Ente prevede le seguenti procedure:

1. Le password inserite devono soddisfare le regole di formato di seguito specificate. Il rispetto di queste regole è controllato direttamente durante l'inserimento a video.
2. Le password scadono ogni 6 mesi e devono essere rinnovate. Dove il sistema lo permette, la scadenza è gestita automaticamente con relativo avviso per l'utente, altrimenti viene gestito il rinnovo manualmente a cura dell'IT.
3. In caso di smarrimento o problemi ad una password o in caso di particolare necessità, l'amministratore IT può resettare la password di un utente, previa segnalazione all'utente stesso e/o all'Ente.
4. L'amministratore IT non può leggere la password di alcun utente, ad eccezione di alcuni portali aziendali in cui, previo accordo con l'utente, la password viene gestita direttamente dall'amministratore IT.
5. L'Ente potrebbe effettuare audit periodici con gli Incaricati, informandoli preventivamente, per verificare se stanno correttamente rispettando le regole di gestione delle password.

L'Incaricato, da parte sua, deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri.
2. Non appena si abbia il dubbio che una password sia diventata poco "sicura" occorre avvertire immediatamente l'IT e cambiare la password.
3. Le password non possono essere memorizzate su alcun tipo di supporto facilmente intercettabile da terzi non autorizzati.
4. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Ente.

2.3. Regole di gestione degli account

Ai dipendenti Incaricati possono essere assegnati uno o più account specifici per una risorsa informatica utilizzata:

- account Microsoft 365 (posta elettronica, Office, cartelle cloud Sharepoint/Onedrive);
- account Windows di accesso al PC;
- account di accesso ai Portali aziendali web;
- account di accesso al Sistema gestionale dei rifiuti (WinWaste);
- account di accesso al Sistema gestionale del personale;
- account di accesso al Sistema gestionale contabile.

Ogni account è associato ad una password ed è composto da username, informazioni personali e ruolo per accedere alle risorse informatiche.

Per una corretta e sicura gestione degli account, l'Ente prevede le seguenti procedure:

1. Negli account sono memorizzate informazioni personali strettamente necessarie.
2. Gli account utente e i relativi ruoli sono definiti in base al principio del minimo privilegio, garantendo l'accesso solo alle risorse indispensabili per lo svolgimento delle mansioni lavorative. Ad esempio, gli account Microsoft 365 possono accedere solo alle cartelle personali di Onedrive e alle cartelle personali locali del PC.
3. Solo gli account dell'IT hanno ruolo di amministratore, e accedono per fini lavorativi con massimi privilegi a tutte le risorse informatiche aziendali. In particolare, gli amministratori IT possono accedere come amministratore a tutti i server, servizi, portali, PC personali e dispositivi di rete, nonché gestire gli account, le password e i ruoli.
4. Gli account inutilizzati per un periodo superiore ai sei mesi sono disattivati a cura dell'IT.

2.4. Regole per l'impostazione della password

Le password devono rispettare le seguenti regole di sicurezza:

1. Essere lunghe almeno 8 caratteri
2. Contenere almeno una lettera maiuscola e una lettera minuscola
3. Contenere almeno un carattere speciale (ad esempio: [], () ? *!$&<>) e almeno un numero;
4. Non contenere:
   - nome, cognome e loro parti;
   - lo username assegnato;
   - un indirizzo di posta elettronica (e-mail);
   - parole comuni (in Inglese e in Italiano);
   - parole banali e/o di facile intuizione;
   - ripetizioni di sequenze di caratteri (es. abcabcabc);
   - una password già impiegata.

Alcuni esempi di password assolutamente da evitare:

1. se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. il nome della moglie/marito, fidanzato/a, figli, ecc.;
3. la propria data di nascita, quella del coniuge, ecc.;
4. targa della propria auto;
5. numero di telefono proprio, del coniuge, ecc.;
6. parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);

2.5. La password nei sistemi

Ogni Incaricato può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo, oppure facendone richiesta all'Amministratore di Sistema. La password può essere sostituita dall'Amministratore di Sistema, anche qualora l'Utente l'abbia dimenticata.

3. PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.
Per postazione di lavoro si intende qualsiasi luogo in cui l'incaricato sta utilizzando un Dispositivo aziendale: la scrivania dell'ufficio, un luogo aziendale diverso dall'ufficio (ad esempio un deposito o un'officina), un mezzo mobile (ad esempio l'auto, il camion), un luogo pubblico, la propria abitazione etc.

3.1. Login e Logout (Accesso o Disconnessione)

Il "Login" è l'operazione di Accesso con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. Come già indicato, può essere necessario effettuare più login, tanti quanti sono gli account di ambienti di lavoro diversi.

Il Login ad un sistema critico con un account amministratore richiede sempre l'autenticazione a due fattori (username, password e OTP generata da app di autenticazione sullo smartphone aziendale). Invece il Login come utente generico richiede l'autenticazione a singolo fattore (username e password).

Il "Logout" o disconnessione è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni e tutte le sessioni aperte su un Dispositivo devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "Blocco " è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera, mouse e schermo disattivati) senza chiuderla.

Per effettuare lo Sblocco di una sessione di lavoro dopo il Blocco è necessario reinserire la password.

Tutte le sessioni di lavoro dopo un periodo di inattività di 10 minuti passano automaticamente in "Blocco".

3.2. Accesso semplificato

L'accesso semplificato è una modalità semplice e veloce per effettuare il Login o lo Sblocco di una sessione di lavoro in alternativa all'inserimento della password, quali l'inserimento di un PIN o di un segno o di un riconoscimento biometrico.

Per ragioni di sicurezza, l'unico accesso semplificato reso disponibile dall'Ente è lo Sblocco della schermata di accesso allo smartphone o tablet mediante modalità "segno". L'accesso al PC deve sempre avvenire con password.

3.3. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo Dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo Dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo Dispositivi.
6. Non permettere ad altri utenti (es. colleghi) di operare con i propri dati di accesso;
7. Non comunicarla mai telefonicamente o via email o via social (salvo gravi necessità).

4. USO DEL PERSONAL COMPUTER AZIENDALE

4.1. La rete aziendale

Il sistema informativo aziendale si basa su una infrastruttura totalmente cloud di server e servizi, non sono presenti server locali.

Alla infrastruttura cloud accedono i client aziendali attraverso la rete Internet oppure attraverso la rete Intranet, quest'ultima composta dalle LAN locali e dai collegamenti geografici via VPN.

I client possono essere Dispositivi aziendali oppure altri apparati di supporto alla operatività dell'Ente (ad esempio stampanti, webcam, domotica).

La **infrastruttura cloud** si compone di:

1. SERVER in hosting e housing presso la piattaforma Amazon Web Service (AWS).
   Sui Server sono residenti tutti gli applicativi aziendali:
   - il portale DigitalNord - Portale Aziendale Econord contenente tutte le informazioni relative a Clienti, Fornitori e Formulari (Econord e Terzi);
   - il portale Ecoinfo – Portale Aziendale per il Numero Verde contenente le informazioni necessarie alle prenotazioni porta a porta ed i disservizi segnalati dai comuni;
   - il portale EcoPortale – Portale aziendale di consultazione esterna ai dati statistici dei trasporti;
   - il gestionale dei rifiuti WinWaste;
   - il gestionale di contabilità aziendale;
   - il gestionale delle risorse umane;
   - applicativi/processi di servizio,
   - i DBMS e i Database;
   - i backup gestiti direttamente da IT.
2. SERVIZI di archiviazione presso la piattaforma Google, per lo storage di una seconda copia dei backup oltre a quelli archiviati su AWS.
3. SERVIZI SaaS offerti dalla piattaforma Microsoft 365, che offre la suite Office, cartelle personali e cartelle condivise (tramite SharePoint) e la funzione di amministrazione ActiveDirectory.

Tutte le piattaforme cloud sopra elencate offrono ampie garanzie di sicurezza fisica, protezione dei dati e controllo degli accessi.

Ogni **LAN** si compone di **FIREWALL** che permettono:

- di accedere alla rete aziendale da esterno solo tramite autenticazione via VPN;
- il blocco e di monitorizzare gli accessi interni ed esterni;
- di bloccare la navigazione su indirizzi internet non autorizzati;
- di gestire gli accessi internet degli utenti autorizzati attraverso differenti livelli di policy.

4.2. Corretto utilizzo del COMPUTER aziendale

I Personal Computer (PC) sia fissi che portatili in dotazione agli utenti, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.

Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole.

Il computer consegnato all'Incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Per necessità aziendali, gli amministratori di sistema utilizzando il proprio login con privilegi di amministratore potranno accedere sia ai backup che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche da remoto.

L'Incaricato deve adottare le seguenti misure di utilizzo del Computer aziendale:

1. Utilizzare per scopi lavorativi solo ed esclusivamente le cartelle soggette a salvataggio da parte delle operazioni di backup aziendale:
   - sul disco fisso locale (nel caso dei PC) nelle apposite cartelle personali dell'utente (Documenti, Immagini, Video, Download, Collegamenti) sotto la cartella OneDrive ;
   - sulle cartelle di rete previste dall'account Microsoft 365;
   - sulle cartelle di rete condivide, specifiche per uffici e competenze.
2. Eventuali file personali, ossia non collegati alle attività lavorative, possono essere archiviati sul computer aziendale solo temporaneamente, e devono essere mantenuti rigorosamente separati dai file aziendali e su cartelle diverse da quelle soggette al backup aziendale citate al punto precedente.
3. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;
4. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro, disposti dall'Ente;
5. Non collegare dispositivi USB o altro diversi da quelli disposti dall'Ente;
6. Non installare applicazioni (anche gratuite). L'installazione è permessa soltanto all'amministratore IT, direttamente o con collegamento da remoto, e deve essere espressamente autorizzata.
7. Non dare accesso al proprio computer ad altri utenti, a meno che siano Incaricati con cui si condividono l'utilizzo dello stesso PC o a meno di necessità stringenti e sotto il proprio costante controllo. L'accesso deve comunque avvenire con le credenziali personali assegnate.

4.3. Divieti espressi sull'utilizzo del COMPUTER

All'incaricato è vietato:

1. La gestione, la memorizzazione o il trattamento di file - documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative - nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere. La memorizzazione di file personali è permessa solo temporaneamente, con i vincoli indicati al par.4.2.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Ente.
4. Installare alcun software di cui l'Ente non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

4.4. ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, file-sharing, chat, via mail ecc..

L'Ente impone su tutti Dispositivi aziendali e sui Server l'utilizzo di un sistema antivirus denominato "ESET PROTECT " correttamente installato, attivato, aggiornato quotidianamente e rinnovato annualmente.

Ogni Dispositivo aggiorna automaticamente il proprio antivirus quando connesso alla rete, e comunica con una applicazione centrale aziendale ESET di amministrazione e di log degli eventi.

L'antivirus agisce in autonomia su ogni dispositivo al rilevamento di un evento di sicurezza, mettendo eventualmente in quarantena file sospetti.

Su ogni smartphone aziendale è installata un'app ESET che oltre a svolgere funzione di antivirus permette all'amministratore IT, in caso di furto o smarrimento e previa autorizzazione dell'Ente, di tracciare il dispositivo ed eventualmente bloccarlo da remoto.

L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. comunicare all'Ente ogni anomalia o malfunzionamento del sistema antivirus;
2. comunicare all'Ente eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:

1. è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;

2. è vietato ostacolare l'azione dell'antivirus aziendale;
3. è vietato tentare di disattivare l'antivirus senza l'autorizzazione espressa dell'Ente (la disattivazione non è peraltro accessibile ad un utente non amministratore) anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o che in qualche modo appaiano strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5. INTERNET

5.1. Internet è uno strumento di lavoro

La connessione alla rete internet del dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare, si vieta l'utilizzo dei social network.

5.2. Misure preventive per ridurre navigazioni illecite

L'organizzazione ha adottato idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri.

L'Ente è dotato di un sistema di sicurezza sui FIREWALL che permette la gestione degli accessi Internet degli Incaricati autorizzati attraverso policy di profilazione.

Su tutti i Dispositivi aziendali (PC, cellulari, tablet) in uso agli Incaricati sono bloccati gli accessi ai social network pubblici e ai provider di streaming, nonché ai siti elencati da IT in apposite blacklist.

Eventuali deroghe a queste restrizioni, come ad esempio la possibilità di usare WhatsApp da PC o smartphone, sono concesse da IT a determinati utenti previa autorizzazione dell'Ente.

Tutte le attività in rete da parte dei Dispositivi aziendali sono tracciate su appositi log dall'Antivirus e dai Firewall.

5.3. Divieti Espressi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi della normativa Privacy.
2. È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'Incaricato lo scarico (download) di software (anche gratuito) prelevato da siti Internet;
4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
6. È vietata la partecipazione a forum non professionali, l'utilizzo di chat online, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
9. È vietato collegare il proprio dispositivo a reti o connessioni di cui non si abbia completa garanzia di sicurezza.
10. È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'Ente stesso.
11. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'Incaricato inadempiente.

5.4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Ente per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5. Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'organizzazione

6. POSTA ELETTRONICA

6.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.
Gli Incaricati hanno in utilizzo indirizzi nominativi di posta elettronica. Per motivi di organizzazione Aziendale, la società ha creato, inoltre, indirizzi di posta elettronica generici (assistenza@econord.it, clienti@econord.it, info@econord.it, ecc.). La posta elettronica generica è consultabile da più Incaricati ai fine dello svolgimento della propria attività lavorativa.

Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. Avvisare l'IT quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.
2. Occorre sempre essere consapevoli che posta elettronica e navigazione Internet sono veicoli per l'introduzione sul proprio dispositivo (e quindi in azienda) di virus e altri elementi potenzialmente dannosi.

L'Azienda formula, inoltre, le seguenti regole di comportamento a cui gli utenti devono attenersi:

a. conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica;
b. prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti o anche apparentemente conosciuti ma inattesi, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo, con richieste di comunicare informazioni o di accedere a siti anche apparentemente corretti o di rispondere alla mail, e in generale che inducano a eseguire azioni non strettamente previste. In tali casi gli utenti devono in particolare:
    - visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio;
    - una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti;
    - cancellare il messaggio e svuotare il "cestino" della posta;
    - segnalare immediatamente l'accaduto all'Amministratore di Sistema.
c. evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;
d. in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia.

6.3. Divieti Espressi

1. È vietato utilizzare l'e-mail aziendale per inviare o ricevere e-mail personali.
2. È vietato utilizzare l'e-mail aziendale o il dominio internet dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Ente, nonché utilizzare i riferimenti dell'organizzazione per scopi personali.
3. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti adestinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer:
   «Il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'organizzazione oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente".
4. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni, se non espressamente autorizzati dall'organizzazione.

6.4. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

7. USO DEI DISPOSITIVI MOBILI

7.1. L'utilizzo del computer portatile, tablet o smartphone.

Il computer portatile, il tablet e lo smartphone (di seguito generalizzati in "dispositivi mobili") possono venire concessi in uso dall'organizzazione agli Incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.

L'Incaricato è responsabile dei dispositivi mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete indicate al par.4.2. I dispositivi mobili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Ente che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i dispositivi mobili.

All'Incaricato è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

Gli smartphone devono sempre essere protetti con PIN o segno o password e non possono essere lasciati incustoditi senza attivare il blocco.

L'Incaricato è chiamato ad informarsi preventivamente dei vincoli associati all'utilizzo della rete internet in mobilità (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli. Qualora esigenze lavorative richiedessero risorse differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'Ente.

Salvo autorizzazione dell'organizzazione, è espressamente vietata ogni connessione dei dispositivi mobili in roaming alla rete internet, e anche in caso di autorizzazione dell'organizzazione, gli utilizzi in roaming devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.2. Memorie esterne (chiavi usb, hard disk, memory card.)

Agli Incaricati può essere assegnata una memoria esterna aziendale (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

7.3. Dispositivi personali

Agli Incaricati dipendenti non sono permesse attività aziendali su Dispositivi personali (PC fissi o portatili personali, smartphone personale) o utilizzando memorie esterne personali. Eventuali deroghe per l'utilizzo di dispositivi personali a scopo lavorativo e/o per l'accesso agli account aziendali come Microsoft 365, devono essere espressamente autorizzati dall'Ente.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati dell'Ente solo se espressamente autorizzati dall'Ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali dispositivi dovranno essere preventivamente valutati dall'Ente, per la verifica della sussistenza di misure idonee di sicurezza.

7.4. Utilizzo dello smartphone personale

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l'utilizzo dello smartphone personale, ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'organizzazione si invita a non utilizzarlo per fini personali alla presenza di clienti o fornitori.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell'Ente solo se espressamente autorizzati dall'Ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dall'Ente, per la verifica della sussistenza di misure idonee di sicurezza.

7.5. Restituzione e Distruzione dei Dispositivi

Ogni Dispositivo ed ogni memoria esterna affidati agli Incaricati, (al termine del loro utilizzo dovranno essere restituiti all'Ente che provvederà a distruggerli o a ricondizionarli.

In particolare, l'Ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8. GESTIONE DEI DATI SUI SISTEMI IN CLOUD

8.1. Utilizzo di sistemi cloud

Come indicato al par. 4.1, tutti i server aziendali sono gestiti in housing o hosting sulla piattaforma in cloud AWS (Amazon Web Services). Per quanto concerne la normativa GDPR, AWS offre a clienti e partner APN (**AWS** Partner Network) informazioni utili quali report di conformità provenienti da entità di controllo di terze parti, che hanno verificato lo stato di conformità di AWS secondo diversi standard e normative di sicurezza informatica, per documentare gli elevati livelli di conformità dell'infrastruttura.

Questi report mostrano che i dati personali che decidono di elaborare in AWS sono sempre al sicuro:

1) L'infrastruttura AWS è conforme alle norme ISO/IEC 27001, 27017, 27018 e 27701. Le norme ISO 27018 e 27701, in particolare, stabiliscono linee guida e standard specifici per la corretta gestione della sicurezza e della protezione dei dati personali sui sistemi cloud.

2) AWS è inoltre conforme al codice di condotta redatto dal CISPE.

   Il CISPE è una coalizione di provider di infrastrutture cloud (Cloud Infrastructure-as-a-Service) che offrono servizi cloud ai clienti in Europa. La conformità al codice di condotta CISPE offre la garanzia ai clienti che AWS applica robusti standard per la protezione dei dati conformi al GDPR.

   Alcuni dei vantaggi del codice di condotta:

   - Chiarisce le responsabilità specifiche in relazione alla tutela dei dati, spiegando il ruolo dei provider e quello del cliente secondo il GDPR, in particolare nel contesto dei servizi infrastrutturali nel cloud.
   - Stabilisce i principi ai quali devono aderire i provider: descrive le operazioni e gli impegni che devono garantire per risultare conformi al GDPR e aiutare i propri clienti e i partner APN a soddisfare i requisiti di conformità.
   - Fornisce a clienti e partner APN informazioni relative a protezione e sicurezza dei dati necessarie per prendere decisioni relative alla conformità: richiede infatti ai fornitori trasparenza sulle misure che prendono per onorare i loro impegni di sicurezza. Queste misure prevedono l'invio di notifiche relative a violazioni alla sicurezza, eliminazione e trattamento dei dati da parte di terzi e richieste legali e da parte di autorità. I clienti e i partner APN potranno impiegare queste informazioni per acquisire una visione più completa dei livelli elevati di sicurezza forniti.

3) Infine, AWS è conforme alle regole previste dal framework CSA STAR CCM.

   Il CSA (Cloud Security Alliance) è una organizzazione internazionale no-profit che promuove best practice e certificazioni per garantire un ambiente cloud sicuro, a partire dalle regole già esistenti e ampiamenti accettati. La conformità al framework CSA STAR CCM offre la garanzia ai clienti che AWS esegue rigorosi controlli sulla effettiva, continua e completa sicurezza del cloud gestito.

   Il framework stabilisce ad esempio controlli di sicurezza sui seguenti aspetti critici:

   - analisi e politiche di gestione del rischio
   - sicurezza delle informazioni (controllo accessi, crittografia etc.)
   - sicurezza delle operazioni (problem solving, change management etc.)

- sicurezza fisica (accessi fisici, incendi etc.)
- sicurezza infrastruttura (disponibilità rete etc.)
- disaster recovery e business continuity

9. GESTIONE DATI CARTACEI

9.1. Custodia e distruzione dei dati cartacei

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli Incaricati sono invitati dall'organizzazione a trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'Ente.

Questo al fine di:

1) dare una buona impressione a clienti e fornitori che visitano la nostra organizzazione;
2) ridurre la possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) evitare che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

In particolare, gli Incaricati a fine giornata dovranno provvedere ad archiviare i documenti cartacei contenenti dati personali negli appositi armadi dotati di apposita chiusura di sicurezza.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

10. ACCESSO AMMINISTRATIVO AI DATI DELL'UTENTE

L'Amministratore IT può accedere ai dati trattati dall'utente tramite i suoi dispositivi o account aziendali esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), oppure per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio: aggiornamento, sostituzione, implementazione di programmi o manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.

Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).

L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere agli account dell'utente (ad esempio la posta elettronica) d per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'utente.

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

L'eventuale controllo da parte dell'Amministratore ITai log delle attività in rete (vedi par.5.2) o dei dispositivi aziendali degli utenti non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.

11. APPLICAZIONE E CONTROLLO

11.1. Trattamento e conservazione dei dati

Gli Incaricati, innanzitutto, devono acquisire e trattare solo i dati necessari e opportuni per lo svolgimento delle funzioni e responsabilità ricoperte.
Nel corso della "vita" e del trattamento dei dati, gli stessi devono essere protetti rispetto a coloro che non hanno diritto all'accesso seguendo le disposizioni previste nel presente Disciplinare.
L'organizzazione promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e allo scopo ha adottato gli strumenti tecnici, organizzativi e fisici ritenuti necessari per prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
I dati, qualora non rivestano più utilità per l'azienda, devono essere distrutti e resi non più accessibili.
Il tempo di conservazione dei dati, quindi, è legato alla finalità del trattamento.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e ha luogo in relazione ad esempio:

1. Ad esigenze tecniche o di sicurezza;
2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità Giudiziaria

11.2. Controllo

Con il presente capitolo portiamo all'attenzione degli Incaricati la possibilità di questa Azienda di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

L'Ente, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Si precisa, in ogni caso, che l'organizzazione non adotta apparecchiature per esclusive finalità di controllo a distanza dell'attività dei lavoratori.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà dell'Azienda in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli dell'Azienda stessa.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del Presente Regolamento.

In caso di anomalie, l'Azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.

In tali casi, il controllo si concluderà con un avviso al Responsabile della struttura dell'Area aziendale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali

affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'Azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

12. SOGGETTI AUTORIZZATI AL TRATTAMENTO

12.1. Individuazione dei Soggetti autorizzati

L'organizzazione ha designato un Responsabile del trattamento dei dati cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

I dipendenti incaricati al trattamento di dati sono sensibilizzati al corretto e diligente utilizzo dei sistemi informatici e degli strumenti cartacei mediante la consegna del presente Disciplinare, nonché la frequenza a corsi specifici.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico- gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

13. PROVVEDIMENTI DISCIPLINARI

13.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente documento da parte del personale non dirigente potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni del Contratto Collettivo Nazionale del Lavoro applicato e dello Statuto dei Lavoratori, tra cui:

1. Il biasimo inflitto verbalmente per le mancanze più lievi;
2. Lettera di richiamo inflitto per iscritto nei casi di mancanze più gravi;
3. Multa;
4. La sospensione dalla retribuzione e dal servizio;
5. Il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge.

In caso di infrazione da parte del personale dirigente l'organizzazione provvede ad assumere nei suoi confronti i provvedimenti ritenuti idonei in funzione del rilievo e della gravità delle violazioni commesse.

13.2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi dell'art. 7 del D.Lgs 196/2003 e dell'art. 15 del Regolamento (UE) 2016/679 alle informazioni che lo riguardano scrivendo al Titolare dell'organizzazione.

14. VALIDITA', AGGIORNAMENTO ED AFFISSIONE

14.1. Validità

Il presente Disciplinare ha validità a partire da: 25/05/2018

14.2. Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative.

Ogni variazione del presente Disciplinare sarà comunicata agli Incaricati.

14.3. Affissione

Il presente Disciplinare verrà portato a conoscenza di tutti gli interessati, mediante affissione in bacheca aziendale, pubblicazione sulla intranet aziendale e invio alla e-mail aziendale, nel rispetto dell'art. 7 della legge 300/70 e delle ulteriori disposizioni previste dal CCNL.

_____

Firma del Titolare o Responsabile del trattamento dei dati

Data _____