CREMONA SOLIDALE

AZIENDA SPECIALE COMUNALE PER I SERVIZI ALLA PERSONA

Sede Legale: Via Brescia, 207 – 26100 Cremona

24/07/2024 - 11.12
A.S.C. Cremona Solidale
CREMONA
U.O. SISTEMI INFORMATIVI
Protocollo N°: **00003483/00** rif: **CBA|3314125**
Data Movimento: **24/07/2024 - 11.12**

Deliberazione n. 42

VERBALE DELLA DELIBERAZIONE

adottata dal Consiglio di Amministrazione nella adunanza
del 23 Luglio 2024

OGGETTO: Adozione del Regolamento Informatico Aziendale coerentemente alle disposizioni del Regolamento UE 2016/679 e del D.Lgs. n. 231/2001.

L'anno duemilaventiquattro il giorno ventitré del mese di luglio alle ore diciassette e trenta, nella sala destinata alle Adunanze, convocato ai sensi del vigente Statuto, si è riunito il Consiglio di Amministrazione sotto la presidenza del Dott. Emilio Arcaini.

Sono presenti i Consiglieri Dott.ssa Luisa Guglielmi e Dott. Andrea Barzanti, mentre il Dott. Sergio Morandi è collegato da remoto.

La Dott.ssa Marialuisa Rocca è assente giustificata.

Partecipano i Revisori Dott.ssa Elisabetta Pasquali, Dott. Andrea Gamba e Dott. Giovanni Costa.

Partecipa la Dott.ssa Simona Gentile in qualità di Direttore Sanitario e Direttore Generale facente funzioni.

Ai sensi dell'art. 18 comma 3 del vigente Statuto assiste, con funzioni di Segretario, il Dirigente U.O. Affari Generali, Relazioni Istituzionali, Rapporti con il Terzo Settore, Dott.ssa Francesca Cerati.

IL PRESIDENTE

dopo aver constatato che gli intervenuti costituiscono il numero legale, dichiara aperta la seduta.

IL CONSIGLIO DI AMMINISTRAZIONE

RICHIAMATO Il Regolamento Europeo (UE) 2016/679: "Regolamento Generale Sulla Protezione dei Dati" (GDPR);

PREMESSO CHE il GDPR non prevede in capo agli Enti/Aziende l'obbligo di adottare un Regolamento Informatico, in quanto fondato sul *Principio di Accountability*;

DATO ATTO CHE in ragione del *Principio di accountability* il Titolare ha la possibilità di definire le misure tecniche ed organizzative di cui dotarsi, al fine di rispettare gli adempimenti richiesti in materia di protezione dei dati e garantire un livello di sicurezza adeguato al rischio;

CONSIDERATO CHE il GDPR prevede l'adozione di misure organizzative di sicurezza (art.32), l'istruzione degli operatori (art.29) e l'adozione di politiche di sensibilizzazione e di formazione del personale (art.39);

EVIDENZIATO CHE il *Regolamento Informatico* per l'utilizzo degli strumenti informatici aziendali, conformemente al GDPR, si configura come uno strumento funzionale alla tutela dell'organizzazione aziendale nei confronti delle minacce derivanti dalla rete informatica e per la formazione e sensibilizzazione del personale in materia di protezione dei dati personali;

RICHIAMATI:

- Artt. 2104 e 2105 Codice Civile che affrontano il tema della Diligenza del prestatore di lavoro e dell'obbligo di fedeltà;
- Art.4 Statuto dei Lavoratori che disciplina la gestione degli strumenti lavorativi forniti al personale dipendente;
- *Linee Guida del Garante della Privacy,* adottate con Delibera n. 13 del 1° marzo 2007, relative *all'utilizzo della posta elettronica e della rete internet nel rapporto di lavoro*;

CONSIDERATO CHE le suddette Linee Guida prevedono che il Datore di lavoro assicuri la funzionalità e il corretto impiego degli strumenti aziendali, inclusa la posta elettronica e l'utilizzo di internet, adottando misure di sicurezza idonee e funzionali ad assicurare la disponibilità e l'integrità dei sistemi informatici e dei dati, prevenendo quindi utilizzi indebiti;

RITENUTO opportuno dotare l'Azienda di un Regolamento Informatico finalizzato a regolamentare l'utilizzo dei sistemi informativi aziendali e a disciplinare le modalità di lavoro con strumenti informatici funzionali alle attività e processi aziendali;

ACQUISITA la proposta di Regolamento Informatico, prot. n. 00003459 del 23/07/2024, redatto dall'Amministratore di Sistema dell'ASC Cremona Solidale e validato dal DPO aziendale, fondata sui seguenti principi:

- la responsabilità del personale verso gli strumenti di lavoro;
- le modalità di utilizzo degli strumenti informatici di lavoro;
- la conservazione delle credenziali e password da parte degli operatori in modo responsabile e sicuro, trattandosi di dati personali e particolari;
- la regolamentazione dell'installazione di software esterni sui dispositivi aziendali che espongono l'azienda a malware e a responsabilità in caso di violazione di licenze o in materia di diritto d'autore;
- la disciplina della navigazione internet e della gestione della posta elettronica;

RICHIAMATO Il D.Lgs. 8 giugno 2001 n. 231 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000 n. 300*";

VISTO il *Modello di Organizzazione, Gestione e Controllo (MOGC) aziendale*, adottato con Delibera n. 40 del 23/07/2024, in particolare l'allegato 5 "*Catalogo dei reati presupposti*" che prevede la fattispecie dei Delitti informatici e trattamento illecito di dati (art. 24-bis, D.Lgs. n.231);

DATO ATTO CHE in attuazione del suddetto MOGC è stato redatto il Protocollo preventivo n.08 "*Sicurezza Informatica e Trattamento dei dati*", prot. n. 00003457;

Tutto ciò premesso e considerato, ad unanimità dei voti legalmente espressi

DELIBERA

1. approvare, per le motivazioni esplicitate in premessa, *il Regolamento Informatico* ALL. A) dell'ASC Cremona Solidale, acquisito agli atti con prot. n. 00003459 del 23/07/2024, redatto in ottemperanza alle disposizioni normative del GDPR e del D.Lgs. n.231/2001, quale parte integrante e sostanziale del presente atto;

2. di demandare all'Amministratore di Sistema aziendale gli adempimenti conseguenti all'adozione del presente atto;

3. di pubblicare, ai sensi e per gli effetti del D.Lgs. n. 33/2013, il presente provvedimento sul sito aziendale nella sezione *"Amministrazione Trasparente";*

4. di trasmettere copia del presente atto al Comune di Cremona entro i quindici giorni successivi alla data odierna.

Letto, confermato e sottoscritto.

IL PRESIDENTE
Dr. Emilio Arcaini

IL SEGRETARIO VERBALIZZANTE
Dr.ssa Francesca Cerati

CREMONA SOLIDALE

AZIENDA SPECIALE COMUNALE PER I SERVIZI ALLA PERSONA

REGOLAMENTO INFORMATICO

Approvato con Delibera del Consiglio di Amministrazione n 42 del 23/07/2024

Approvato dal Titolare del Trattamento in data 23/07/2024.

INDICE

Premessa

L'utilizzo delle risorse informatiche e telematiche dell'azienda deve sempre ispirarsi ai principi di diligenza e correttezza. La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare l'utilizzo delle e-mail aziendali e l'accesso alla rete Internet, espone l'azienda ai rischi di coinvolgimento sia patrimoniale sia penale, creando potenziali problemi alla sicurezza e all'immagine dell'Azienda stessa.
Si ritiene perciò opportuno adottare regole interne di comportamento comune, tese a prevenire comportamenti inconsapevoli o involontari così come scoraggiare ogni atto o comportamento non conforme a detti principi al fine di garantire la sicurezza informatica di tutta l'azienda e un adeguata protezione di tutti i dati personali dei quali l'azienda è Titolare del Trattamento.
Tali regole sono applicate a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, stagista, fornitore di prestazione occasionale, ecc.) e impongono un utilizzo degli strumenti informatici, degli applicativi e dei portali solo ed esclusiviste negli orari di lavoro, ovvero al di fuori degli stessi solamente se autorizzati.
Tutti gli utenti sono tenuti a segnalare eventuali anomalie al Titolare del trattamento.

Definizione di "Soggetti autorizzati"

Il Regolamento Europeo 2016/679 definisce come Soggetti autorizzati "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".
Il soggetto autorizzato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Titolare del Trattamento o al Responsabile. Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

1. Dati personali: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
2. Categorie di dati particolari: l'Art. 9 del Reg. UE 2016/679 definisce in tale modo i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
3. Dati giudiziari: tali sono considerati informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
4. Dati che presentano rischi specifici: si tratta di dati che, pur non essendo così delicati come quelli particolari e giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare: in considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, prescritti dal Garante a garanzia dei soggetti interessati. In questa categoria di dati possono ricadere ad esempio le informazioni relative alla capacità di solvibilità del debito, dati biometrici, dati di geolocalizzazione, immagini riprese da impianti di videosorveglianza, ecc.

1. Utilizzo degli strumenti aziendali

Tutti i dispositivi aziendali (PC desktop, PC portatili, Tablet, cellulari, ecc.) ed i relativi programmi e/o applicazioni affidati al dipendente/consulente/collaboratore sono di proprietà dell'azienda e sono esclusivamente strumenti di lavoro; ogni utilizzo non inerente all'attività lavorativa, ovvero svolto al di fuori della stessa senza autorizzazione, può contribuire ad innescare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza.

Pertanto:

- tali strumenti vanno custoditi in modo appropriato e utilizzati con cura e possono essere utilizzati solo per fini lavorativi (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali;
- debbono essere prontamente segnalati al Titolare il furto, il malfunzionamento, il danneggiamento o lo smarrimento di tali strumenti;
- non è consentito utilizzare programmi e/o applicazioni aggiuntive alla dotazione aziendale (anche gratuiti, o che non richiedono installazione), per evitare il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni del computer;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare o disattivare le configurazioni software impostate, salvo autorizzazione esplicita da parte dell'Amministratore di Sistema; in particolare, è espressamente vietato modificare le impostazioni antivirus, firewall e proxy;
- non è consentita la visualizzazione di video ed immagini, se non a fini prettamente lavorativi;
- non è consentito collegare dispositivi hardware ai pc (chiavette USB, Cellulari, ecc.) senza la previa autorizzazione dell'Amministratore di Sistema; anche in caso di necessità di ricarica elettrica di cellulari personali è fatto divieto collegarli ai PC aziendali;
- non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema;
- non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'azienda;
- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
- le informazioni archiviate digitalmente devono essere esclusivamente quelle necessarie all'attività lavorativa; è espressamente vietato memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria di carattere sessuale, religioso e razziale;
- non è consentita la riproduzione o la duplicazione di programmi informatici;
- il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate;
- il Personal Computer utilizzati h24 vanno riavviati almeno una volta a al giorno;
- la tutela della gestione locale di dati memorizzati su personal computer è demandata all'utente che dovrà posizionare/salvare i propri dati in apposite cartelle personali e/o condivise, predisposte nella rete e non sul PC locale;
- si deve provvedere alla pulizia periodica (almeno ogni tre mesi) degli archivi e delle e-mail, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei file: è infatti assolutamente da evitare un'archiviazione ridondante. Soprattutto nelle cartelle comuni. E' compito degli utilizzatori coordinarsi per la corretta gestione della risorsa. L'amministratore di sistema si riserva di fornire un elenco di file obsoleti e/o duplicati da far bonificare;
- il Titolare del Trattamento, attraverso tecnici autorizzati e l'Amministratore di Sistema, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia del PC degli incaricati che delle unità di rete.
- non è consentito copiare e portare/trasportare fuori dalla sede di lavoro dati e file inerenti la propria attività lavorativa o comunque qualsiasi dato del quale l'azienda è Titolare (ad esempio su chiavette usb); non è altrettanto consentito inviare/trasferire fuori dalla sede di lavoro dati e file con strumenti elettronici quali e-mail o software di trasferimento (come, ad esempio, WeTransfer o ftp) se non previa specifica autorizzazione da parte del Titolare o dell'Amministratore di Sistema.
- non è consentito utilizzare ambienti cloud esterni per scopi personali sui dispositivi aziendali (come ad esempio Dropbox, OneDrive, Google Drive, iCloud ecc.) né tanto meno depositare/salvare/copiare in ambienti cloud esterni dati o file se non previa specifica autorizzazione da parte del Titolare o dell'Amministratore di Sistema.
- Parimenti non è consentito accede agli applicativi ed ai portali ad uso lavorativo con il proprio dispositivo

mobile se non in orario di lavoro, ovvero al di fuori solo se autorizzato.

- Non è consentito attivare/aprire un collegamento di teleassistenza da remoto (TeamViewer, AnyDesk, LiveLet, Bomgard, ecc.) per eventuali assistenze tecniche sul PC aziendale senza prima aver avuto l'autorizzazione del Titolare del trattamento o dell'Amministratore di Sistema; prima di attivare/aprire il collegamento è necessario chiudere tutti i programmi (email, software gestionali ecc.) e tutti i file che contengono dati personali non strettamente necessari ai fini dell'attività di teleassistenza; il collegamento dovrà sempre essere presidiato e controllato dall'utente che dovrà aver cura di disattivare il collegamento al termine dell'attività di teleassistenza prima di ricominciare le consuete attività lavorative; non è consentito configurare collegamenti di teleassistenza con modalità di accesso remoto non presidiato che non necessita del consenso utente di attivazione/apertura.
- Non è possibile creare applicativi e script (anche all'interno di software della suite office) e non si possono gestire base dati esterne come access. Tutte le esigenze che richiedono questa attività devono essere inoltrate all'amministratore di sistema

2. Utilizzo della rete aziendale

L'accesso alle risorse sulla lan aziendale deve avvenire mediante le proprie credenziali di accesso personali o, dove previsto, utilizzando le credenziali specifiche; è assolutamente proibito entrare nella rete e nei programmi con nomi utente e password di un altro soggetto.
Le unità di rete 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 dette unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte dell'Amministratore di Sistema. Quest'ultimo ha facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema, ovvero acquisiti o installati in violazione del presente regolamento.
È fatto divieto:

- connettere in rete nuovi computer se non dietro esplicita e formale autorizzazione dell'Amministratore di Sistema;
- monitorare o tracciare ciò che transita in rete.

3. Password e Credenziali di Accesso

L'accesso ai dispositivi aziendali è regolamentato da due differenti tipologie di autenticazione in relazione all'utilizzo destinato:

1. Per i PC/Tablet utilizzati l'accesso viene effettuato mediante credenziali comuni agli utenti abilitati mentre l'accesso agli applicativi di pertinenza dei singoli operatori avviene mediante credenziali personali. Particolare attenzione deve essere posta nel posizionare su desktop e cartelle comuni solo i file contenenti dati utilizzati da tutti gli operatori abilitati in quanto tali file verranno visualizzati da tutti gli utenti che utilizzano quelle stesse credenziali di accesso.
2. Per i PC affidati ad uso esclusivo di un solo utente le credenziali di accesso sono personali.

- Le credenziali di accesso e la relativa Password non devono essere divulgate, garantendo la massima riservatezza. Inoltre, non devono essere utilizzati come password nomi facilmente identificabili e riconducibili all'utilizzatore. Per questo si rimanda all'allegata Best Practice Password che deve essere rispettata
- Le credenziali vengono comunicate dall'Amministratore di Sistema al caposervizio.
- L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione;

- La password ha una validità di tre mesi nel caso di accesso a dati personali, al termine del quale dovrà essere modificata (Privacy by Default);
- Se il PC viene lasciato incustodito per un periodo superiore a 10 minuti, è opportuno bloccare la sessione di lavoro, uscendo prima dagli applicativi e dai programmi gestionali;
- Nel caso si sospetti che la password abbia perso di efficacia o si sospetti che sia stata diffusa o violata, la stessa deve essere immediatamente modificata dall'utente, dando comunicazione all'Amministratore di Sistema del sospetto di violazione della password; qualora l'utente venisse a conoscenza della password di altri soggetti, è tenuto a darne immediata notizia all'Amministratore di Sistema;
- È fatto divieto di conservare le password in modo non adeguato, come ad esempio in modalità cartacea non sicura. Per questo si rimanda all'allegata Best Practice Password che deve essere rispettata;
- Tutte le password vanno correttamente conservate attraverso un software (ad esempio Keepass) in cui vengono salvate e protette da credenziali d'accesso; il database va salvato nelle unità di rete condivise sul server e sottoposte a backup.

L'utente è responsabile di eventuali danni effettuati dall'uso improprio delle credenziali di accesso a lui assegnate qualora ci fosse stata incuria e non rispetto di quanto previsto dal presente articolo.

4. Utilizzo di supporti di memorizzazione rimovibili

- È vietato scaricare/copiare dati e file supporti rimovibili;
- È vietato collegare ai dispositivi aziendali supporti di memorizzazione esterni (dischi esterni, chiavette USB, cellulari personali ecc.) per operazioni non inerenti la propria attività lavorativa;
- Tutti i dispositivi mobili di provenienza incerta o comunque esterna, necessari all'attività lavorativa, prima di essere collegati ai dispositivi aziendali devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'Amministratore di Sistema e comunque è sempre necessario operare una scansione dei dispositivi mediante antivirus;
- Nel caso si renda necessaria l'utilizzo di dispositivi USB per la propria attività lavorativa, l'utente dovrà richiedere all'Amministratore di Sistema una chiavetta USB aziendale che sarà fornita dallo stesso già protetta da password all'accesso e crittografata, e che dovrà essere conservata e custodita dall'utente in modo tale da impedirne lo smarrimento o furto. Per poter riutilizzare tali supporti per finalità successive e diverse, è necessario cancellare completamente i dati in esso contenuti, mediante formattazione. A fine utilizzo il dispositivo usb aziendale dovrà essere riconsegnato all'Amministratore di Sistema;
- Non è consentita la copia di archivi aziendali di qualsiasi genere o specie su dispositivi asportabili (CD, chiavi USB e simili) né su dispositivi di memorizzazione esterni all'Azienda (ad esempio in server accessibili mediante Internet, aree dati in Cloud come ad esempio WeTransfer, Dropbox, ecc.) se non su esplicita autorizzazione del Titolare del Trattamento.

5. Utilizzo PC Portatili (notebook)

Ai computer portatili si applicano le regole di utilizzo previste per i computer fissi (desktop). L'utente è responsabile del PC portatile assegnatogli dall'azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

- I PC portatili utilizzati all'esterno (convegni, visite in azienda…), in caso di allontanamento, devono essere custoditi in un luogo protetto; in particolare essi non devono mai essere lasciati incustoditi nell'autovettura neppure nel bagagliaio;
- Non è consentito in nessun caso concedere l'utilizzo anche temporaneamente del pc portatile, come di ogni altra dotazione tecnologica aziendale mobile, a un utente non autorizzato come ad esempio famigliari, amici, colleghi ecc.
- È buona norma collegarsi periodicamente alla rete interna per consentire il caricamento

dell'aggiornamento dell'antivirus;

- È fatto obbligo disconnettere eventuali connessioni VPN/RDP se non utilizzate, anche per brevi periodi;
- In caso di furto, smarrimento o danneggiamento del PC portatile, come di ogni altra dotazione tecnologica aziendale mobile (ad esempio cellulare, Tablet, ecc.), deve essere effettuata immediata comunicazione al proprio responsabile ed al Titolare stesso al fine di prendere il prima possibile tutte le contromisure necessarie per limitare la violazione o potenziale violazione dei dati personali, fare eventuale denuncia alle autorità competenti ed effettuare una valutazione in merito alla necessità di comunicazione Data Breach al Garante della Privacy e comunicazione agli interessati.
- Il Titolare si riserva in qualsiasi momento di chiedere all'utente la riconsegna del PC aziendale, come di ogni altra dotazione tecnologica aziendale mobile.

6. Accesso agli strumenti aziendali/e-mail e ai dati in essi contenuti

Il titolare ha adottato tutte le misure necessarie (condivisione cartelle, regolamento e istruzioni ecc.) per evitare di dover accedere al profilo utente e all'email aziendale assegnata all'utente in assenza del dipendente/collaboratore; tuttavia, si riserva la possibilità di accedere alla postazione e all'email aziendale nel caso di assenza dell'utente per interventi di assistenza tecnica o qualora sia necessario per garantire la continuità lavorativa.

Le modalità e la procedura di accesso sono le seguenti:

- Il responsabile di settore o il Titolare richiederà all'Amministratore di Sistema di modificare/resettare la password di accesso dell'account personale o alla casella e-mail dell'assente;
- L'Amministratore di Sistema modificherà la password dell'utente per accedere temporaneamente ai dati ed effettuerà l'accesso al PC o alla casella e-mail;
- Verrà inviata apposita e preventiva comunicazione al Titolare del Trattamento, a mezzo e-mail, recante richiesta di autorizzazione all'intervento con la data e i motivi sottesi alla forzatura dell'account nel l'ottica del rispetto del principio di trasparenza;
- La nuova password verrà comunicata all'utente al momento del rientro sul posto di lavoro, il quale dovrà cambiarla con nuove credenziali di accesso aventi le caratteristiche previste dall'art.3 del presente regolamento.

In ogni caso l'accesso ai dati dovrà rispettare il principio di necessità per il quale verranno visionati unicamente le sole informazioni indicate nella motivazione che ha portato alla forzatura dell'account personale, fermo restando il rispetto dei principi etici di riservatezza ai quali è tenuto l'Amministratore di Sistema.
Il Titolare si riserva la facoltà di poter fare richiesta all'Amministratore di Sistema accesso al PC/e-mail aziendale/cellulare aziendale affidato all'utente nel caso in cui ritenga necessario effettuare verifiche sulla sua attività lavorativa per il solo fine di prevenire o evitare danni o pregiudizi al Titolare, agli utenti o a terzi.

7. Utilizzo della rete internet e dei relativi servizi

Internet rappresenta uno strumento di lavoro molto utile, ma al contempo costituisce anche un rischio elevato per la sicurezza dei sistemi informatici aziendali.

Ribadiamo comunque che:

- Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line/e-commerce e simili, salvo casi direttamente autorizzati dal Titolare;
- Non è consentito lo scarico di software gratuiti (sia freeware che shareware) prelevati da siti internet, se non espressamente autorizzati all'Amministratore di Sistema;
- Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;

- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- Non è permessa la partecipazione, per motivi non professionali a Forum, a social networks, a chat, a bacheche elettroniche e a Guestbook anche utilizzando pseudonimi;
- Non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo definita "*sensibile*" quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
- L'accesso a internet può essere revocato dall'azienda in qualsiasi momento.

I sistemi aziendali registrano gli accessi e la navigazione effettuata in appositi registri (file di log e statistiche) che potranno essere consultati dal titolare e dall'Amministratore di Sistema nei casi previsti dalla legge per effettuare controlli difensivi, per verificare il corretto funzionamento delle rete, per prevenire danni o usi impropri degli strumenti, per redigere statistiche o analisi sull'impiego degli strumenti forniti e per soddisfare le richieste pervenute dalle forze dell'ordine. Il trattamento dei dati sarà effettuato nel rispetto dei principi di pertinenza e non eccedenza.

8. Posta elettronica

La posta elettronica costituisce uno strumento aziendale a disposizione del lavoratore solo per consentirgli di svolgere la propria funzione aziendale e pertanto resta nella completa disponibilità del Titolare.

8.1 Posta elettronica

La posta elettronica è uno strumento di lavoro e le persone assegnatarie delle caselle di posta sono responsabili del corretto utilizzo delle stesse.
Si ritiene utile segnalare che:

- Non è consentito utilizzare la posta elettronica (interna od esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- Non è consentito utilizzare caselle di posta elettronica private per corrispondenza inerente le attività aziendali salvo esplicita autorizzazione del titolare;
- Non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria di carattere sessuale, religioso e razziale;
- La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro "*Strettamente Riservati*" o contenenti dati personali senza aver provveduto all'adozione di sistemi di protezione;
- Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, social o mail-list salvo diversa ed esplicita autorizzazione;
- Va prestata particolare attenzione agli allegati contenuti nei messaggi ricevuti (dall'interno o dall'esterno). Nel caso in cui non si sia più che certi del contenuto dell'allegato è necessario richiedere all'Amministratore di Sistema un esame del contenuto stesso prima di aprire l'allegato, onde evitare la propagazione di virus od altri programmi elaborati al fine di danneggiare o violare il contenuto della rete aziendale;
- Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli.
- Nel caso di messaggi contenenti allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti;
- Nel caso in cui si debba inviare un documento all'esterno dell'azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf);
- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti; l'utilizzo della stessa è consentito esclusivamente come strumento di comunicazione, l'archiviazione sistematica di file allegati è pertanto impropria e non autorizzata; la casella di posta non è un archivio di file: i file allegati per i quali è necessaria la conservazione dovranno essere salvati nelle apposite unità di rete;
- È vietato fare invii massivi di mail (invii di mail a una pluralità di destinatari) al fine di evitare che i server dell'azienda siano annoverati tra gli indirizzi IP dei mittenti indesiderati ("*spam*"). Nel caso sia necessario

effettuare invii massivi rivolgersi all'Amministratore di Sistema che metterà a disposizione gli idonei strumenti;

- In caso di necessità di inviare una e-mail a più soggetti destinatari che non sono tenuti a conoscere l'identità degli altri è obbligatorio utilizzare sempre lo strumenti CCN (*copia conoscenza nascosta*).
- I messaggi che necessitano di tracciabilità e opponibilità a terzi dovranno essere inviati attraverso gli indirizzi PEC a disposizione dell'azienda;
- Le regole e istruzioni sopra valgono anche per l'utilizzo della casella PEC che è anch'essa soggetto all'arrivo di e-mail fasulle contenenti virus.

L'accesso alle caselle e-mail è consentito solamente all'Amministratore di Sistema per effettuare controlli difensivi, per verificare il corretto funzionamento del sistema di posta elettronica, prevenire danni o usi impropri degli strumenti, per redigere statistiche o analisi sull'impiego degli strumenti forniti e per soddisfare le richieste pervenute dal titolare o dalle forze dell'ordine. Il trattamento dei dati avverrà sempre nel rispetto dei principi di pertinenza e non eccedenza seguendo la procedura descritta al punto 6.
Le credenziali di accesso alla PEC sono nella disponibilità del Titolare del trattamento, il quale potrà sempre accedervi per verifica e controlla, anche laddove sia stato incarico uno specifico utente.

8.2 E-mail, PEC phishing e virus

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore. Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima.

Cosa fare:

- Non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- Limitarsi a fornire informazioni a interlocutori noti nei limiti dei contenuti afferenti all'ambito lavorativo assegnato;
- Diffidare di messaggi provenienti da fonte non conosciuta contenenti allegati o link;
- Non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- Non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche, agenzia delle entrate) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- In caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con l'Amministratore di Sistema.

8.3 Assenza del lavoratore e procedura accesso e-mail

Il Titolare si riserva la facoltà di poter fare richiesta all'Amministratore di Sistema di accedere alla posta elettronica aziendale affidata dell'utente nel caso in cui ritenga necessario effettuare verifiche sull'attività lavorativa dell'utente al solo fine di prevenire o evitare danni o pregiudizi agli interessi del Titolare, di terzi o degli stessi utenti. Verrà in ogni modo rispettata la procedura sopra descritta al paragrafo 6

9. Protezione Antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'azienda meditante virus.

Pertanto:

- È vietato disattivare la protezione antivirus ed annullare le scansioni programmate dall'Amministratore di Sistema;
- Ogni dispositivo di provenienza esterna dovrà essere verificato mediante programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, il dispositivo infetto non dovrà essere utilizzato;
- Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e staccare subito il cavo di rete/disconnettere il wi-fi per isolare subito l'infezione ed evitare che si propaghi agli altri PC e ai server, segnalando senza indugio l'accaduto all'Amministratore di Sistema;
- Utilizzare soltanto programmi provenienti da fonti fidate autorizzate preventivamente dal Titolare o dall'Amministratore di Sistema. Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma nuovo, prima dell'installazione, deve essere sottoposto all'autorizzazione dell'Amministratore di Sistema;
- Non utilizzare programmi non autorizzati, con particolare riferimento alle applicazioni di gioco, che sono spesso utilizzate per veicolare virus e per questo motivo ne è vietato l'utilizzo.

10. Aggiornamenti

I sistemi informatici richiedono una continua e costante manutenzione del sistema operativo, per questo motivo ogni postazione è configurata per l'esecuzione automatica degli aggiornamenti rilasciati da Microsoft. È buona pratica spegnere il computer almeno una volta al giorno anche per le postazioni utilizzate in modo continuativo nell'arco delle 24 ore così da consentirne l'effettivo aggiornamento.
Eventuali anomalie vengono comunque monitorate all'Amministratore di Sistema.

11. Impianto elettrico e assenza di corrente

Le "ciabatte elettriche" o altri dispositivi a presa multipla devono essere correttamente installati, tenendo conto della portata di carico e della strumentazione ad essa collegata. Il collegamento di tali strumenti deve essere predisposto dall'Amministratore di Sistema.

12. Backup

La copia di backup dei dati costituisce uno degli elementi fondamentali per la sicurezza informatica, per questo l'azienda ha adottato un sistema di backup a più livelli.
In particolare:

- I dati presenti nei database dell'azienda, gli archivi comuni (cartelle condivise) e la posta elettronica
- Vengono copiati con cadenza giornaliera;
- I dati/i file devono essere salvati nell'apposita cartella di rete assegnata all'utente o al gruppo e non nella cartella documenti in locale o sul desktop; il rispetto di questa procedura è necessaria in quanto in caso di guasto inaspettato del PC non sarà possibile recuperare i dati/file presenti sul PC stesso; tali dati/file andranno così persi esponendo l'azienda al rischio Data Breach nonché a gravi conseguenze per l'attività lavorativa;
- La tutela dei dati/file locali presenti su eventuali PC portatili, sul dispositivo mobile/cellulare è demandata all'utente che dovrà approntare con l'Amministratore di Sistema una procedura appropriata per il salvataggio.

13. Centralino telefonico

Il telefono costituisce uno strumento aziendale a disposizione del lavoratore/collaboratore solo per consentirgli di svolgere la propria funziona aziendale e pertanto resta nella completa disponibilità dell'azienda.
In caso di installazione di centralino digitale, ogni numero interno è abbinato/abbinabile un profilo di abilitazione alle chiamate secondo lo schema seguente:

- Solo chiamate interne;
- Chiamate interne e esterne;

Si ricorda che non è consentito effettuare telefonate non inerenti all'attività lavorativa.
In caso di ricezione di telefonate di tipo commerciale o a fini statistici è vietato rispondere a domande che possano riguardare l'azienda o l'attività lavorativa da essa svolta; in particolare è vietato fornire informazioni a soggetti non autorizzati in merito al personale dell'azienda, ai fornitori e collaboratori dell'azienda, in merito ai programmi e alla struttura informatica dell'azienda.

14. Cellulari e dispositivi di connessione in mobilità

I telefoni cellulari *smartphone,* e in generale ogni altro dispositivo mobile, costituiscono uno strumento aziendale a disposizione del lavoratore/collaboratore solo per consentire il corretto svolgimento delle funzioni attribuite e pertanto restano nella completa disponibilità dell'azienda esattamente come avviene per i PC. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza.

Pertanto, tali strumenti:

- Vanno custoditi con cura e in modo appropriato;
- Possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate);
- Non possono essere oggetto di installazione applicazioni fatto salvo previa autorizzazione dell'Amministratore di Sistema per evitare il grave pericolo di introdurre virus informatici e di alterare la stabilità del dispositivo.
- Non possono essere utilizzati per nessun motivo da persone non incaricate (famigliari, amici, colleghi ecc.)

L'utente deve prontamente segnalare al Titolare il furto, lo smarrimento, il malfunzionamento e il danneggiamento di tali strumenti. In caso di furto/smarrimento verranno attuate dall'Amministratore di Sistema le procedure di localizzazione e di blocco da remoto del dispositivo mobile, al fine di evitare l'accesso non autorizzato ai dati in esso contenuti.
Il Titolare potrà richiedere al fornitore del servizio la visione in chiaro dei tabulati telefoni per effettuare controlli difensivi, per prevenire danni o usi impropri degli strumenti, o per soddisfare le richieste pervenute dalle forze dell'ordine. I dati saranno tratti nel rispetto dei principi di pertinenza e non eccedenza.

15. Interruzione rapporto di lavoro

Ribadiamo che l'account personale, i dati e i file contenuti sul pc, il numero di telefono (fisso o cellulare) e l'indirizzo di posta elettronica sono strumenti di lavoro pertanto restano nella completa disponibilità dell'azienda.
Nel caso di interruzione del rapporto di lavoro:

- I dispositivi informatici mobili in dotazione dovranno essere riconsegnati al titolare;
- Le credenziali di accesso alla rete e la possibilità di invio di mail dall'indirizzo di posta aziendale verranno disabilitate dall'ufficio preposto alla cessazione del rapporto di lavoro;
- Eventuali mail ricevute nei 6 mesi successivi alla data di cessazione del rapporto di lavoro all'indirizzo di posta elettronica aziendale saranno automaticamente inoltrate ad altro indirizzo aziendale per

consentirne una corretta gestione da parte del personale dell'azienda e per prevenire eventuali danni o pregiudizi agli interessi del Titolare.

- Trascorso un anno le mail verranno eliminate.

16. Revoca delle credenziali

L'azienda si riserva la possibilità di revocare in qualsiasi momento le credenziali di accesso e l'indirizzo di posta elettronica, dandone comunicazione all'utente assegnatario, nel caso di violazione grave del presente regolamento o in caso di comportamento etico/morale che possa provocare danno all'azienda.

17. Formazione

Il Titolare è tenuto ad erogare specifica formazione in materia di Privacy con test finale che ne attesti l'apprendimento da parte degli utenti.
In particolare, relativamente a:

- Profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività e conseguenti responsabilità che ne derivano;
- Rischi che incombono sui dati;
- Misure disponibili per prevenire eventi dannosi;
- Modalità per aggiornarsi sulle misure di sicurezza adottate dal titolare.

18. Gestione e conservazione dei dati cartacei

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessario e ritirare prontamente i documenti stampati dai vassoi delle stampanti. In caso di rottamazione, distruggere i documenti con un tritacarte o quantomeno romperli in piccoli pezzi.
È sempre vietato portare/trasportare all'esterno della sede di lavoro qualsiasi tipo di documento cartaceo inerente all'attività lavorativa se non previa autorizzazione da parte del Titolare.
Per il trattamento dei documenti cartacei è necessario rispettare sempre le indicazioni del Titolare in merito agli archivi a cui poter accedere: non trattare nessun documento al di fuori delle proprie mansioni o non inerenti la propria attività lavorativa.
Una volta presi in consegna o presi in carico atti o documenti contenenti dati personali, è necessario non lasciarli incustoditi e senza controllo per un tempo indefinito, ma occorre provvedere in qualche modo a riporli in luogo protetto e custodirli, per poi restituirli al termine delle operazioni affidate.
In caso di affidamento di atti e documenti contenenti dati particolari o giudiziari, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario riporre in cassetti e armadi con serratura i documenti contenenti dati particolari o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente.
L'accesso a tali archivi è consentito solo alle sole persone autorizzate da specifico e scritto profilo di autorizzazione con dovere di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

19. Social Networks

L'avvento e la crescente diffusione dei servizi di social network segnalano un cambiamento radicale nell'accessibilità pubblica a dati ed informazioni, secondo modalità e misure sinora sconosciute.
Assimilando i mezzi di diffusione del pensiero dei social network (Facebook, Twitter, LinkedIn, WhatsApp, Blog, Chat ed altro), alle dichiarazioni rese dall'incaricato a mezzo degli strumenti tradizionali di comunicazione pubblica

(giornali, radio, televisione) si ricorda che il diritto di manifestazione del pensiero e di critica in costanza del rapporto di lavoro soggiace a determinati limiti, esplicitazioni dei doveri di fedeltà, di riservatezza ed adesione ai valori dell'Azienda, che incombono sull'incaricato in quanto deducibili nella prestazione lavorativa medesima, in particolare attinenti a:

- Continenza verbale;
- Continenza sostanziale: verità dei fatti e del ruolo ricoperto all'interno dell'Azienda;
- Divulgazione di qualsiasi tipo di dato o informazione relativo e attinente all'attività dell'incaricato all'interno dell'Azienda.

Allorché il "profilo privacy" scelto e adottato dall'incaricato consente la visualizzazione dei suoi "*post*", commenti, video e foto, anche ad una cerchia di utenti aperta e sostanzialmente indeterminabile, l'incaricato soggiace a valutazioni e ad azioni di responsabilità disciplinari quando integri una lesione del rapporto fiduciario che lega l'incaricato all'Azienda, con evidenti profili di violazione della riservatezza e danno dell'immagine, alla continuità e alla regolarità dell'attività.

L'azienda si è dotata di una "SOCIAL MEDIA POLICY INTERNA" che qui si richiama interamente.

20. Inosservanza della policy aziendale

Il Titolare si riserva di verificare, nei limiti consentiti dalle norme legali e contrattuali, il rispetto da parte del dipendente/collaboratore delle regole sancite nel presente regolamento.
In caso di violazione del presente regolamento verranno applicate le sanzioni previste dal CCNL (Contratto Collettivo Nazionale di Lavoro) di riferimento.

21. Entrata in vigore

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Copia del regolamento sarà affisso nelle bacheche aziendali e reso disponibile sul server aziendale.

22. Revisione e Aggiornamento

Il presente regolamento potrà essere aggiornato a discrezione dell'azienda, la quale è tenuta a darne tempestiva comunicazione a tutti i dipendenti e collaboratori.

23. Amministratore di Sistema

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Si tratta perciò di soggetti che hanno un accesso privilegiato a tutti i dati e ampio potere di modifica/controllo.
Ai fini del Provvedimento del 27 novembre 2008 del Garante della Privacy, gli Amministratori di Sistema sono designati con apposita "Lettera di Incarico" e sottoposti a una verifica annuale da parte del Titolare per prevenire abusi di potere e per accertare che il loro operato rispetti sempre gli interessi dell'azienda.

L'Amministratore di Sistema designato è il sig. Marco Cavalli.

Presa visione da parte del dipendente

Il sottoscritto/a _____ *, dichiara di aver ricevuto, preso visione, compreso tutte le norme contenute in questo Regolamento Informatico che con la sottoscrizione accetta espressamente.*

Data _____ *Firma* _____