Regolamento Informatico

Bertani Trasporti S.p.A.

"And the only way to do great work is to love what you do"

-Steve Jobs-

1. PRINCIPI GENERALI

Il presente regolamento ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori ecc.) al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre la società a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.
A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1 marzo 2007).

Copia del presente Regolamento viene pubblicata sul portale aziendale e consegnata a ciascun dipendente/collaboratore all'atto dell'assunzione e dell'instaurazione del rapporto contrattuale. L'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per il soggetto autorizzato al trattamento dei dati personali e per la Società, per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

La Società riconosce il valore fondamentale dell'utilizzo di strumenti di comunicazione sia nella comunicazione interna che con l'utenza esterna, anche al fine di ridurre i tempi di risposta e di migliorare pertanto l'efficienza del proprio operato.

2. CAMPO DI APPLICAZIONE

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative della società.
Per **utente** pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.
Per **ente** si intende, invece, la società, l'organizzazione e in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza. Ferme restando le disposizioni normative in materia, e tutte le prescrizioni previste per il trattamento di categorie particolari di dati personali ai sensi dell'art. 9, GDPR o di personali giudiziari *ex* art. 10, GDPR, il contenuto del presente Regolamento costituisce disposizione di servizio. I beni e le risorse informatiche, i servizi IT e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'ente. Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti attività svolte per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi aziendali. A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura aziendale e non riservata. Sono esentati dall'applicazione del presente Regolamento, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, eventuali soggetti nominati Amministratori di Sistema. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione autentica delle disposizioni contenute nel presente Regolamento, è possibile rivolgersi al personale IT compilando apposito quesito o inviando una segnalazione all'indirizzo di posta [postmaster@bertanitrasporti.it.] ponendo sempre per conoscenza "l'Amministratore di Sistema" Dott. Cesare Bertani.

3. RIFERIMENTI NORMATIVI E DEFINIZIONI

Ai sensi dell'art. 4, GDPR e del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 intitolato *"misure e accorgimenti prescritti ai Titolari dei trattamento effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*, come letto e interpretato in base a quanto stabilito dal GDPR, si intende per:

1) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) "limitazione di trattamento": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5) "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) "archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
8) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9) "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
10) "terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) "violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
13) "dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
14) "impresa": la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
15) "gruppo imprenditoriale": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
16) "autorità di controllo": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51, GDPR;
17) "amministratore di sistema", la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi di software complessi, nella misura in cui consentano di intervenire sui dati personali; soggetti che, pur non essendo preposti ordinariamente a operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali; vanno considerati a tutti gli effetti alla stregua di trattamenti di dati personali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware, anche quando non consultati "in chiaro" dall'amministratore.
18) "risorse informatiche": i server; le *workstation*; i personal computer; i notebook; i tablet, smartphone e qualsiasi altra tipologia di elaboratore elettronico; le stampanti; i plotter; i fotocopiatori e i fax; tutti gli strumenti informatici interconnessi con la rete aziendale ivi compresi i telefoni cellulari; gli apparati di rete; tutti i software e i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati; file di qualsiasi natura, archivi di dati anche non strutturati e applicazioni informatiche.

4. RESPONSABILITA' PERSONALE DELL'UTENTE

Di seguito vengono descritte le norme a cui gli Utenti 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, la Società ha provveduto a nominare ciascun Utente quale soggetto autorizzato al trattamento ai sensi dell'art. 29, GDPR; all'interno di tale atto di nomina il soggetto autorizzato (di seguito, l'"Incaricato") si è impegnato ad 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:

(i) Gli strumenti assegnati devono essere utilizzati SOLO per finalità lavorative; Non possono essere scaricati programmi o applicazioni non preventivamente autorizzate dalla Direzione (Il traffico dati originato dal download di musica, video, foto e quant'altro incide sulle prestazioni di rete, causando rallentamenti con conseguente perdita di produttività aziendale);

(ii) E' vietato collegare al PC chiavette USB o telefoni che potrebbero rappresentare veicolo di infezione; E' vietato scaricare o semplicemente visualizzare o ascoltare tramite il PC musica o filmati; E' vietato utilizzare il PC per scaricare, inviare, distribuire fotografie personali o altro materiale personale;

(iii) Si raccomanda di mantenere sempre la scrivania ed il desktop puliti come da normativa vigente in materia di Sicurezza delle Informazioni e nel rispetto delle Direttive Aziendali;

(iv) 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 commerciale o d'ufficio, i dati ritenuti obsoleti dovranno essere rimossi quanto prima;

(v) le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita e/o distruzione, che 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;

(vi) 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 o automatizzato;

(vii) non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile o necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;

(viii) deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

(ix) I supporti di memorizzazione (es. chiavette USB, qualsiasi apparecchiatura contenente supporti di memorizzazione) alla fine del loro utilizzo devono essere regolarmente ripuliti e/o formattati per non permettere la visione del loro contenuto ad altre persone non autorizzate. Per maggiori chiarimenti contattare gli Amministratori di Sistema.

(x) Il trasporto di supporti fisici che contengono informazioni deve essere effettuato con imballaggio adatto a proteggere il contenuto da qualunque tipo di danneggiamento, e deve essere affidato al solo personale interno qualificato.

Non sarà possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza. Tutti gli Utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale e ad operare a tutela della sicurezza informatica aziendale, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente.

5 ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

5.1 CREAZIONE E GESTIONE DEGLI ACCOUNT

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali per singola postazione lavorativa. Gli account utenti vengono creati dagli amministratori di sistema e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", solitamente username e password, comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.
Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'ente.
Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al responsabile privacy di riferimento.
In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza e operatività delle risorse informatiche, l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento dell'amministratore di sistema.
I beni e la strumentazione informatica oggetto del presente regolamento rimangono di esclusivo dominio dell'ente, che in conseguenza dei rapporti instaurati con gli utenti ne disciplina l'assegnazione.

In caso di instaurazione di rapporto di lavoro con l'utente, le credenziali di autenticazione verranno gestite come da Istruzione "**I040 Istruzione Gestione profili utente"** e Moduli collegati.

5.2 GESTIONE DELLE PASSWORD

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo anche nel caso di trattamento di categorie particolari di dati personali (art. 9 GDPR) o relativi a condanne penali o reati (art. 10 GDPR), almeno ogni 3 mesi.
L'utente, nel definire il valore della password, deve rispettare le seguenti regole:
• Utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, ecc.), di cui almeno uno numerico;
• La password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#$£$%...";
• Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
• Evitare l'utilizzo di password comuni o prevedibili;
• Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;
Scrivere la password su post-it o altri supporti non è conforme alla normativa, compromette in maniera pressoché totale le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

5.2.1 Autenticazione a più fattori

E' stata implementata la sicurezza per i collegamenti dall'esterno (VPN) con l'attivazione della Multi Factor Autentication (MFA).

5.3 – CESSAZIONE DEGLI ACCOUNT

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno gestite come da Istruzione "**I040 Istruzione Gestione profili utente"** e Moduli collegati.

6. ANTIVIRUS

I Personal Computer (PC) 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:

- controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;
- chiudere correttamente i programmi in uso;
- prima di aprire un allegato ricevuto via e-mail verificare che l'indirizzo mittente sia conosciuto;
- non aprire, se si lavora in rete, *file* sospetti o di dubbia provenienza;
- non scaricare e/o installare applicazioni/software che non siano state preventivamente approvate e autorizzate dal personale IT della Società;
- non installare sulla strumentazione in uso, hardware fisso o removibile (ad esempio chiavette USB, telefoni cellulari aziendali e personali, tablet ecc), qualora ciò non risulti espressamente richiesto ed autorizzato dalla Società.
- verificare con l'ausilio del programma antivirus in dotazione ogni supporto esterno contenente dati (DVD-ROM, USB KEY), prima dell'esecuzione dei file in esso contenuti;
- non utilizzare DVD-ROM, USB KEY o altri supporti elettronici di provenienza incerta;
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;
- non modificare le configurazioni pre-impostate sul proprio PC;
- spegnere il PC al termine della giornata di lavoro;
- in caso di malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'Incaricato /Utente sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto, spenga tempestivamente il pc e contatti immediatamente l'Area Sistemi Informatici.

7. SALVATAGGIO DEI DATI

Al termine della giornata lavorativa, tutti i dati vanno salvati sul server aziendale. A tale riguardo, qualora vi sia la necessità e non si sia già provveduto a fare ciò, l'Incaricato / Utente può richiedere all'Area Sistemi Informatici la creazione sul server di una cartella a lui intestata o, in alternativa, di una cartella condivisa dal gruppo di lavoro cui fa riferimento l'Incaricato / Utente stesso.

8. PROTEZIONE DEI PC PORTATILI

L'Utente è responsabile dell'integrità del PC portatile affidatogli dalla Società e dei dati ivi contenuti. L'Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti all'esterno. Ai PC portatili si applicano le regole di utilizzo previste per i personal computer.

Nel caso di utilizzo comune con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati. Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. In casi particolari i dischi dovranno essere criptati al fine di evitare, in caso di furto o di smarrimento, l'accesso a dati riservati e/o personali da parte di soggetti non autorizzati.

Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda;
- avvertire tempestivamente l'Area Sistemi Informatici, che darà le opportune indicazioni, in caso di furto di un PC portatile;

- essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto al PC fisso;
- operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

Istruzione "I040 Istruzione Gestione profili utente".

8.1 Connessioni remote e Telelavoro

Nei casi in cui il dipendente si trovi a lavorare fuori dalla propria sede lavorativa, dopo essersi collegato alla VPN, deve rispettare quanto sotto riportato:

- Utilizzare esclusivamente PC Aziendali;
- NON utilizzare chiavette USB e/o dispositivi esterni non preventivamente autorizzati dalla Direzione;
- Fare riferimento alla Procedura P500 Infrastruttura Informatica.

9. STRUMENTI DI FONIA MOBILE O DI CONNETTIVITÀ IN MOBILITÀ

A seconda del ruolo o della funzione del singolo utente, l'ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi. È tuttavia permesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la "diligenza del buon padre di famiglia" prevista dalla normativa e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.
I controlli saranno eseguiti secondo criteri e modalità descritte nel presente regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.
L'utilizzo dei dispositivi mobili risponde alle seguenti regole:
Ciascun utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione; è fatto espresso divieto di estrarre la carta SIM di cui è dotato l'apparto al momento della consegna ed inserirla in altri apparati non aziendali.

I dispositivi devono essere dotati di password di sicurezza, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che: o il codice PIN dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione;

Istruzione "I040 Istruzione Gestione profili utente ".

10. INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno alla Società. In particolare, l'Utente / Incaricato dovrà osservare le seguenti regole:

- è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- non è consentito scaricare software gratuiti di nessun genere prelevati da siti internet;

- non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa e, in ogni caso, previa autorizzazione della Società;
- non è consentito l'utilizzo funzioni di *instant messaging* a meno che autorizzate dalla Società
- è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro), si raccomanda di controllare sempre l'estensione dopo l'@ per essere sicuri che l'e-mail provenga da soggetti conosciuti;
- non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- è sconsigliato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;
- occorre essere consapevoli che la posta elettronica e la navigazione in internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;
- è consentito solo l'utilizzo dei programmi ufficialmente installati dall'Area Sistemi Informatici;
- è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti nonché di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dalla Società;
- è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o *connect card*), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. *switch*, *hub*, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o *connect card* ecc.), visualizzare documenti audio o video in *streaming* utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna) salvo che non sia autorizzato dalla Società con l'utilizzo di dispositivi forniti e configurati dall'Area Sistemi Informatici interna;
- va sempre prestata la massima attenzione all'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), anche se previamente autorizzati, avvertendo immediatamente l'Area Sistemi Informatici nel caso in cui siano rilevati virus;
- sono tassativamente vietati accessi a siti aventi per oggetto: -attività o argomenti illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio; -materiale per adulti, nudità, pornografia; giochi, scommesse, intermediazione e trading, download software freeware; -social network, radio e tv via Internet (salvo i casi espressamente autorizzati dalla Società);
- l'Utente / Incaricato, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 3 giornate lavorative - deve attivare l'apposita funzionalità di sistema (cd. "Fuori Sede") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.
- Si consiglia di eliminare le mail pubblicitarie, lo spam e tutto ciò che non sono mail di lavoro e procedere allo svuotamento del cestino per le mail che hanno una anzianità superiore a 3 mesi. Si ritiene inoltro opportuno ridurre al minimo la dimensione degli allegati.

In caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, la Società si riserva di accedere alla casella di posta elettronica dell'Utente / Incaricato assente.

10.1. PARTICOLARI CAUTELE NELLA PREDISPOSIZIONE DEI MESSAGGI DI POSTA ELETTRONICA

Nell'utilizzo della posta elettronica ciascun Utente / Incaricato deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti aziendali. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, nonché l'immagine e la reputazione della Società. La Società formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

(i) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti da clienti, fornitori, da responsabili o altre funzioni organizzative interne, o da altre società del gruppo societario di cui la Società fa parte;
(ii) prestare attenzione ai messaggi di posta elettronica ed ai *file*, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. 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;
(iii) 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;
(iv) l'iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica devono essere preventivamente autorizzati dalla Società e dall'Area Servizi Informatici, in particolare;
(v) in caso di errore nella spedizione o ricezione di qualsiasi informazione o dato, 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;
(vi) evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

11. TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. Quando il

dato personale deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati particolari ai sensi dell'art. 9, GDPR (ex "sensibili") occorre:

(i) prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;
(ii) per le comunicazioni inviate a mezzo fax, verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un'ulteriore verifica del numero del destinatario e della quantità di pagine inviate;
(iii) nel caso di documenti inviati per posta elettronica, accertarsi, prima di confermare l'invio, di avere allegato il file giusto e che tutti i destinatari siano quelli corretti;
(iv) in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

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.

12. RICHIESTA HARDWARE E SOFTWARE e SISTEMA di TICKETING

Quando si ravvisa la necessità di procedere per esigenze lavorative, all'implementazione di applicativi Hardware e/o Software sugli apparati concessi in uso dalla Bertani Trasporti S.p.A., l'interessato deve procedere alla compilazione dell'apposita richiesta su Service Desk Plus.
Il Sistema di Ticketing anch'esso disciplinato nella Procedura sopra riportata, permette di gestire i malfunzionamenti dei software aziendali.

13. PERSONALIZZAZIONI

La Bertani Trasporti S.p.A. pur non sviluppando software, effettua "sviluppi" intesi come personalizzazioni di software di produttività interna. È espressamente vietata qualsiasi modifica di applicativo software, le uniche modifiche e/o personalizzazioni ai software di produttività vengono fatte esclusivamente ad interfacce, campi e viste logiche.

13.1 Sicurezza nelle personalizzazioni

L'Obiettivo è la sicurezza delle informazioni progettata ed attuata, all'interno del ciclo di personalizzazione dei sistemi informativi.
I Programmatori per attuare tale obiettivo creano ambienti di test per gli applicativi di produttività personalizzabili, verificano i requisiti di sicurezza dell'ambiente nella fase di personalizzazione hanno inoltre la capacità di evitare, trovare e sanare le vulnerabilità.
Nelle attività di modifica e/o personalizzazione dei software (ove ammesse), i programmatori tengono in considerazione il rischio che possano essere compromessi controlli interni e l'integrità dei processi, la necessità eventuale di ottenere un consenso da parte del produttore, la possibilità di ottenere i cambiamenti richiesti dal produttore come aggiornamenti interni del programma, l'impatto dell'eventualità in cui l'organizzazione

dovesse divenire responsabile per la manutenzione del software a seguito cambiamenti effettuati e la compatibilità con altri software utilizzati.
Sevi fosse la necessità di apportare cambiamenti al software originale, premesso che al momento tale attività non risulta tra quelle contemplate dalla Società, esso verrebbe conservato ed i cambiamenti dovrebbero essere applicati su una copia appositamente designata. Verrebbe attuato un processo di gestione del software per garantire che le ultime patch e gli aggiornamenti applicativi siano installati su tutto il software autorizzato in modo da ottenere le informazioni sulle vulnerabilità tecniche dei sistemi informativi in modo tempestivo. L'eventuale esposizione a vulnerabilità verrebbe valutata e gestita attraverso l'adozione di misure atte ad affrontare i rischi relativi. Come in premessa tutte le attività di personalizzazione sono sottoposte a test e documentati a sistema, in modo che questi possano essere applicati nuovamente a futuri aggiornamenti del software stesso. Le personalizzazioni richieste dalla Bertani Trasporti S.p.A., essendo di modesta entità, non richiedono l'obbligo di convalida da parte di organismo di valutazione indipendente.

14. CRITTOGRAFIA

La cifratura delle informazioni costituisce un controllo di sicurezza nei confronti del rischio di perdita della riservatezza delle stesse.

Premesso che ciò che viene cifrato non è l'Asset in sé ma le informazioni che esso contiene, le informazioni che la Bertani Trasporti S.p.A. intende proteggere mediante crittografia e la metodologia utilizzata sono le seguenti:

- Comunicazioni di Posta Elettronica (TLS 1.2 Transport Layer Security)
- Connessioni da remoto mediante VPN (IPsec/IKEv2)
- Portali pubblicati all'esterno (https)
- Interscambio dati (SFTP - SOFTP2 – TLS)
- Utilizzo di Bitlocker con funzionalità di Manage Engine per la crittografia degli Endpoint.

15. ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali o dati aziendali sensibili non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

In caso di trattamento di categorie particolari di dati *ex* art. 9, GDPR (ex dati "sensibili"), 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. L'accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato dalla Società.

Lo smaltimento del materiale cartaceo contenente dati personali o dati aziendali sensibili deve essere eliminato mediante utilizzo di apposito trituratore di carta.

16. AMMINISTRATORE DI SISTEMA

L'ente conferisce all'amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche aziendali. È compito dell'amministratore di sistema:

• Gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;

• Gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;

• Monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

• Creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

• Rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

• Provvedere alla sicurezza informatica dei sistemi informativi aziendali;

• Utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (o *designato*) all'interno dell'ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
Deve essere redatto un elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, aggiornato con cadenza annuale ovvero ogni volta che si rilevino modifiche.

17. ACCESSO AI DATI DELL'UTENTE

L'Amministratore di Sistema ed i soggetti dallo stesso autorizzati possono accedere ai dati trattati dall'Utente / Incaricato tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, *malware*, intrusioni telematiche, fenomeni quali *spamming, phishing, spyware*, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware*, ecc.).

Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza, 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 ed i soggetti dallo stesso autorizzati, in caso di assenza improvvisa o prolungata dell'Utente / Incaricato o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, sono abilitati ad accedere alla posta elettronica dell'Utente / Incaricato per le strette necessità

operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'Utente / Incaricato.

L'Amministratore di Sistema e i soggetti dallo stesso autorizzati possono 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 sui file di log da parte dell'Amministratore di Sistema 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.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico. L'Amministratore di Sistema e i soggetti dallo stesso autorizzati sono altresì abilitati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'Utente / Incaricato alla Società per cessazione del rapporto, sostituzione delle apparecchiature, etc.. Sarà cura dell'Utente / Incaricato la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti. In ogni caso, la Società garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo e non esaustivo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- controlli nella durata delle connessioni ed elementi processati.

18. CONTROLLI

L'ente esclude la configurabilità di forme di controllo aziendali aventi direttamente a oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, statuto dei lavoratori). Premesso che i sistemi informatici vengono controllati mediante controlli automatizzati effettuati con software esterni adibiti a tale scopo, l'ente esclude la configurabilità di controlli che vadano ad interferire con i diritti e le libertà fondamentali dei lavoratori.

In attuazione di tale principio:
• I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
• Nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;
• In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

In caso di anomalie, la Società, 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, la Società 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.

18.1 SANZIONI

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

19. APPLICAZIONE ED INTERPRETAZIONE DEL PRESENTE REGOLAMENTO

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente Regolamento, l'Utente / Incaricato potrà rivolgersi all'Ufficio Privacy ed all'Ufficio Sistemi Informatici.

20. DISCIPLINA, DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

Qualora la Società intenda modificare il presente Regolamento, le modifiche saranno applicate dandone conoscenza immediata all'Utente / Incaricato.
Deroghe o modifiche di uno o più punti del presente Regolamento non rendono invalidi gli altri punti.
Il presente Regolamento è approvato dal Legale Rappresentante.

21. Bertani Poland Sp. Z.o.o.

Tutte le regole sopra indicate sono estese e applicate anche alla società controllata Bertani Poland Sp. z.o.o.

Indice Revisioni

Rev. 01 Prima Emissione

Rev. 02 - Par. 5.2 Gestione Password

Rev. 03 – Par. 13 Personalizzazioni - 13.1 Sicurezza nelle personalizzazioni e Par. 14 Crittografia

Rev. 04
Par. 4. RESPONSABILITA' PERSONALE DELL'UTENTE – Punto iii)
Par. 5.2.1 Autenticazione a più fattori
Par. 14. CRITTOGRAFIA - Utilizzo di Bitlocker con funzionalità di Manage Engine per la crittografia degli Endpoint.

Rev. 04
Par. 4. RESPONSABILITA' PERSONALE DELL'UTENTE – Punto iii)
Par. 5.2.1 Autenticazione a più fattori
Par. 12. RICHIESTA HARDWARE E SOFTWARE e SISTEMA di TICKETING

.