Il Titolare del Trattamento è **BERTANI TRASPORTI S.P.A** con sede Legale in Via Europa, n. 26 – 46043 Castiglione delle Stiviere - P. Iva e C.f. 00247680200.

Il presente documento contiene le disposizioni, le misure organizzative e comportamentali che i dipendenti, i collaboratori a qualsiasi titolo dell'Azienda, sono chiamati ad osservare per contrastare i rischi informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche messe a disposizione da **Bertani Trasporti S.p.A.** deve sempre ispirarsi al principio della diligenza e correttezza, con la presente Politica aziendale sulla sicurezza informatica s'intende contribuire alla massima diffusione della cultura della sicurezza in Azienda, evitando che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici/informativi e nel trattamento dei dati.

In particolare, il documento è suddiviso nelle seguenti due parti:

1. Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da Bertani Trasporti S.p.A. per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo.
2. Norme comportamentali. Requisiti per i dipendenti, collaboratori esterni o individui con accesso a sistemi o dati.

Pubblicazione del presente documento - e dei suoi futuri aggiornamenti - viene data massima diffusione attraverso la sua pubblicazione sul portale aziendale HR, nonché sul sito www.bertanitrasporti.it.

1. Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da Bertani Trasporti S.p.A. per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo.

Premessa Principi Generali e Destinatari

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). 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.

Modalità di utilizzo della strumentazione informatica

(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;

Sicurezza e Privacy

Nell'utilizzo delle strumentazioni informatiche occorre adottare le seguenti cautele:

- mantenere segrete le proprie credenziali di autenticazione (password), sia quelle d'accesso alla strumentazione in dotazione sia quelle d'accesso ai vari programmi utilizzati nell'ambito della propria attività lavorativa, attribuite dal Responsabile del Sistema Informatico;
- non cedere, una volta autenticati nel proprio pc, l'uso della propria postazione a persone non autorizzate, in particolare per l'accesso ad internet ed ai servizi di posta elettronica;
- adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la sicurezza dei dati trattati e dei dati che possono fornire indicazioni utili ad un eventuale "hacker" (attaccante dei sistemi informativi) dell'Azienda;
- utilizzare, in caso di trattamento di dati personali, le cartelle di rete o altri supporti di memorizzazione messi a disposizione dall'Azienda al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali, grazie al sistema centralizzato di backup; e. prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server);
- non connettere alla rete interna dell'Azienda apparati esterni (come ad es. modem o router…) che possano compromettere il corretto funzionamento della rete aziendale;
- non utilizzare strumenti di messaggistica istantanea (per es. Skype, Messenger) per motivi personali;
- non introdurre o diffondere nella rete aziendale programmi illeciti (per es. virus, worm, spyware,...) ;
- non compiere azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore;
- utilizzare la posta elettronica messa a disposizione dell'ente per lo svolgimento dell'attività lavorativa, esclusivamente per le specifiche finalità della stessa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
- aver cura di non aprire allegati di posta in e-mail dal mittente e/o dall'oggetto sospetti per prevenire i rischi causati da software nocivi (per es. virus, worm, spyware, ecc.); m. limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail istituzionale su siti web pubblici (per es. forum, mailing list, ecc.);
- non rimuovere il programma antivirus installato sulla postazione di lavoro;
- nel caso in cui il software antivirus rilevi la presenza di un virus sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'evento all'Amministratore di Sistema;
- eventuali software aggiuntivi, rispetto all'installazione standard, dovranno essere richiesti con le modalità procedurali previste in Azienda;
- non lasciare incustoditi i dispositivi mobili aziendali (come ad esempio i cellulari e i tablet aziendali); s. in caso di incidente di sicurezza (come ad esempio nei casi di accesso non autorizzato o di minacce informatiche al sistema), attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi;
- nell'utilizzo della posta elettronica certificata, le credenziali (user id e password) per accedere a tale casella di posta devono essere a conoscenza unicamente dei collaboratori dell'ufficio autorizzati dal responsabile del servizio.

Controlli. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori. I controlli vengono effettuati dal Responsabile della sicurezza con l'ausilio dell'assistenza tecnica.
Principi. L'Azienda ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite azioni di sensibilizzazione e di diffusione dei principi e delle regole da osservare nell'utilizzo della strumentazione informatica, nell'adozione di specifiche soluzioni tecnologiche e di ogni altra misura ritenuta idonea a tal fine.

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.

Modalità di effettuazione dei controlli.
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.

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.

2. Norme comportamentali. Requisiti per i dipendenti, collaboratori esterni o individui con accesso a sistemi o dati.
È dovere dei dipendenti completare il corso di formazione di sulla sensibilizzazione in materia di sicurezza informatica e sostenere le policy di utilizzo accettabile. Qualora si notasse un individuo non identificato, non accompagnato o non autorizzato all'interno dell'Azienda, informare immediatamente il proprio diretto superiore. Tenere ordinata la scrivania. Per proteggere le informazioni è necessario accertarsi che i dati, in formato stampato, rientranti in questo campo di applicazione non vengano lasciati esposti o incustoditi sulle workstation. È richiesto l'uso di una password sicura su tutti i sistemi di aziendali come indicato nella policy di utilizzo delle password. Le credenziali devono essere uniche e diverse da quelle utilizzate per sistemi o servizi esterni. Al termine del contratto lavorativo, i dipendenti hanno l'obbligo di restituire qualsiasi record, in qualsivoglia formato, che contenga informazioni personali. Informare immediatamente l'amministratore di sistema in caso di smarrimento di un dispositivo (per es. telefoni cellulari, laptop, ecc...) contenente dati di tale natura. Qualsiasi dipendente sospetti che un sistema o un processo non rispetti la compliance a questa policy ha l'obbligo di informare l'amministrazione di sistema, per consentire l'adozione delle necessarie misure correttive.

Questo documento disciplina in forma sintetica i principi sanciti nel Regolamento Informatico Aziendale al quale si rimanda per completezza di informazioni.