La sicurezza informatica (in inglese computer security),
è l'insieme dei mezzi, delle tecnologie e delle procedure tesi alla protezione dei sistemi informatici
in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici.

La Direzione esprime la politica aziendale, vigila sull'applicazione del Sistema di Gestione Integrato, definisce le strategie di crescita e la pianificazione di indirizzo e attua le previsioni normative in materia di Sicurezza Informatica.
La Direzione si adopera per garantire il miglioramento attraverso il rinnovamento tecnologico tutelando la sicurezza delle informazioni mediante assegnazione di ruoli definiti e responsabilità.
La presente politica e le altre politiche sulla sicurezza delle informazioni sono approvate dalla Direzione in fase di Riesame della Direzione.
La Direzione aziendale ha stabilito, adottato e diffuso ad ogni livello dell'Organizzazione la seguente Politica predisposta in osservanza della strategia e dei requisiti di business, dei regolamenti delle norme di legge applicabili, dei contratti nonché, dei rischi e delle minacce relative alla sicurezza delle informazioni attuali e previste .

La Direzione della BERTANI TRASPORTI SPA ha individuato quali elementi fondamentali del proprio Business la riservatezza che garantisce la privacy dei dati restringendo l'accesso tramite la crittografia di autenticazione, l'integrità che garantisce l'accuratezza e l'affidabilità delle informazioni e la disponibilità che garantisce che solo gli utenti autorizzati possano accedere alle informazioni. Riservatezza, integrità e disponibilità rappresentano i mezzi principali per competere sul mercato, e quindi gli elementi fondamentali della strategia aziendale, la cui Mission è: essere un anello fondamentale e strategico nella catena del valore globale del sistema Automotive attraverso il valore aggiunto dei propri servizi finalizzati alla massima soddisfazione delle esigenze del cliente.

Gli scopi principali della presente Politica sono i seguenti:
• avere una visione complessiva e centrale della sicurezza aziendale che spazia oltre il perimetro della sicurezza IT includendo anche persone e processi secondo un approccio olistico;
• disporre di strumento fondamentale per l'ottimizzazione dell'allocazione del budget indirizzandolo verso le iniziative che restituiscono un maggior ritorno in termini di riduzione del rischio;
• dimostrare la sua abilità nel fornire e servizi conformi ai requisiti dei clienti, ai requisiti degli standard di riferimento, delle leggi e dei regolamenti applicabili;
• incrementare la soddisfazione dei clienti attraverso l'efficace applicazione del SGSI e dei processi di miglioramento continuo e assicurando il rispetto dei requisiti stabiliti dalle normative cogenti e dai regolamenti applicabili.

La Politica di Sicurezza delle Informazioni è rivolta a dipendenti e collaboratori Aziendali nonché a tutti partner commerciali ed è predisposta in conformità al Regolamento UE 2016/679 GDPR, D.Lgs. 196/2003 e s.m.i, allo Standard ISO/IEC 27001 nonché, nel rispetto degli Standard richiesti dai Clienti (es. TISAX).

La Politica si divide in:

1- Sicurezza dei dati personali e GDPR
2- Sicurezza delle Informazioni

1- Sicurezza dei dati personali e GDPR

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.

Documento di proprietà della ***Bertani Trasporti S.p.A.***
Ne è vietata la riproduzione, la cessione e la divulgazione a terzi se non espressamente autorizzata dalla Direzione Aziendale.

Sicurezza e GDPR

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.

3- Sicurezza delle Informazioni

1. 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.

Documento di proprietà della ***Bertani Trasporti S.p.A.***
Ne è vietata la riproduzione, la cessione e la divulgazione a terzi se non espressamente autorizzata dalla Direzione Aziendale.

1. 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

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;

Bertani Trasporti S.p.A. ha a cuore la sicurezza delle informazioni verso i partner commerciali con cui collabora ed ha pertanto adottato una attività di Business Continuity.

L'obiettivo principale è quello di puntare al miglioramento continuo e di proteggere gli asset nei confronti degli attacchi informatici e allo stesso tempo cerca di minimizzare l'impatto nel caso di vulnerabilità che superino le difese implementate .

A tal proposito la Bertani Trasporti S.p.A. dispone di:

- ANTIVIRUS

BERTANI TRASPORTI SPA si avvale dei prodotti Antivirus in cloud per quanto riguarda la protezione da Virus e Malware.
I prodotti utilizzati sono:
VISION ONE E XDR: prodotto in cloud per la protezione dei client e dei server aggiornato in tempo reale.
LIBRAESVA: prodotto antispam per il controllo delle e-mail in entrata e uscita aggiornato ogni ora.

- BACKUP

Il backup dei dati e dei server viene effettuato con Veeam Backup che permette sia il backup completo dei server fisici e virtuali su Storage esterno che lo snapshot delle macchine virtuali che viene effettuato ogni 3 ore. E' stata attivata la funzione di Backup immutabile e backup di posta office 365.

- DISASTER RECOVERY

Il **Disaster Recovery**, o ripristino del livello di servizio a seguito di gravi anomalie, è l'insieme delle misure tecnologiche ed organizzative atte a ripristinare dati, sistemi ed infrastrutture necessarie all'erogazione di servizi IT a fronte di condizioni che rendano non erogabili i servizi dal sito principale.
Le esigenze di BERTANI TRASPORTI S.p.A. sono di dotare la propria infrastruttura IT della miglior soluzione di Disaster Recovery sulla base di valutazioni tecnologiche, procedurali, implementative ed economiche.

- ATTIVAZIONE C-SOC e MFA

Assegnazione di incarico al C-SOC gruppo Project Informatica per monitoraggio continuativo H24 del per la salvaguardia dagli attacchi informatici con intervento immediato in caso di incidente/attacco esterno.
Attivazione Multi Factor Authentication (RSA) per accesso ai Sistemi Aziendali.

Documento di proprietà della ***Bertani Trasporti S.p.A.***
Ne è vietata la riproduzione, la cessione e la divulgazione a terzi se non espressamente autorizzata dalla Direzione Aziendale.

- INTELLIGENZA ARTIFICIALE

Considerata l'importanza, ma anche la delicatezza dell'utilizzo degli strumenti di intelligenza artificiale (IA), la Direzione del Gruppo Bertani Trasporti S.p.A. ne disciplina l'utilizzo in uno specifico documento separato.

Violazioni della policy

- eventuali violazioni della presente policy, comprese le disposizioni del GDPR e del Codice etico, saranno considerate gravi infrazioni disciplinari.
- conseguenze delle violazioni e sanzioni disciplinari: per dipendenti e collaboratori, applicazione delle misure previste dal regolamento interno e dal contratto collettivo applicabile.

L'Azienda, nell'erogazione dei propri servizi, si avvale di soluzioni cloud di terze parti e monitora costantemente il rispetto delle condizioni contrattuali e i livelli di servizio (SLA).

L'Azienda ha adottato il Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/01 che "disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'Articolo 11 della Legge 300 del 29 settembre 2000".
La società ha inoltre adottato un sistema di whistleblowing che permette di gestire le segnalazioni inoltrate anche in forma anonima e/o confidenziali dal personale della società nonché, da tutti gli stakeholders (da intendersi come tali i soggetti richiamati nel d.lgs. 24/2023 es. fornitori, terze parti, consulenti ecc), le divulgazioni pubbliche e le denunce in osservanza alla direttiva UE 2019/1937, dal decreto legislativo 10 marzo 2023, n. 24 di attuazione della direttiva (UE) 2019/1937, alle linee guida ANAC, al modello di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001 di Bertani Trasporti S.p.A. (d'ora in avanti 'Bertani' o la 'società') e s.m.i..

BERTANI POLAND Sp. Z.o.o.

La presente politica si estende e si applica alla società controllata Bertani Poland Sp. z.o.o., con le seguenti eccezioni:
- ANTIVIRUS

Bertani Poland Sp. z.o.o. utilizza un prodotto antivirus per la protezione da virus e programmi dannosi. Il prodotto utilizzato è ESET NODE 32, che include la protezione dalla posta indesiderata.

- COPIE DI SICUREZZA

Le copie di sicurezza dei dati e dei server vengono effettuate mediante Veeam Backup, che consente di eseguire copie complete dei server su sistemi di archiviazione esterni.

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

Documento di proprietà della ***Bertani Trasporti S.p.A.***
Ne è vietata la riproduzione, la cessione e la divulgazione a terzi se non espressamente autorizzata dalla Direzione Aziendale.