Tizio Srl
Via_____
CAP - Città

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(in ottemperanza a quanto previsto dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. N. 196/2003)

TIZIO SRL
VIA _____
CAP – CITTA'

Data ultima revisione documento:

00/00/00

(tale documento deve essere aggiornato con cadenza almeno annuale)

Il titolare del trattamento

_____

Indice del documento.

1. Premessa

Sintetica descrizione della propria società/ente.

La composizione della TIZIO srl è la seguente:

- ✓ DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI (ex art. 19.2. del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 196/03)

NOME	FUNZIONE	DATI DI COMPETENZA
	Titolare	Clienti (dati comuni) Fornitori (dati comuni) Banche (dati comuni) Assicurazioni (dati comuni) Risorse Umane (dati comuni e sensibili)
	Impiegato amministrativo	Clienti (dati comuni) Fornitori (dati comuni) Banche (dati comuni) Assicurazioni (dati comuni) Risorse Umane (dati comuni e sensibili)
	Impiegato	Clienti (dati comuni) Fornitori (dati comuni)
	Impiegato	Clienti (dati comuni) Fornitori (dati comuni)
	Operaio	Fornitori (dati comuni)
	Autista	Clienti (dati comuni)

Tutti i soggetti sopra elencati, ad eccezione dei titolari, sono stati nominati INCARICATI DEL TRATTAMENTO. Le relative lettere di incarico sono inserite nella **Busta Allegati**.

- ✓ ELENCO DEI TRATTAMENTI DI DATI PERSONALI (ex art. 19.1. del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 196/03)

CLIENTI (dati comuni): dati amministrativi, gestione agenda, gestione anagrafica cliente, gestione contabilità, fatturazione, gestione ordini, predisposizione documenti di trasporto, contrattualistica;

FORNITORI (dati comuni): dati amministrativi, gestione agenda, gestione anagrafica fornitori, gestione contabilità, fatturazione, gestione ordini, predisposizione documenti di trasporto, contrattualistica;

BANCHE (dati comuni): dati amministrativi, rapporti con istituti di credito, operazioni bancarie on line tramite utilizzo password;

ASSICURAZIONI (dati comuni): dati amministrativi, rapporti con assicurazioni, conservazione polizze assicurative aziendali;

RISORSE UMANE (dati comuni e sensibili): dati amministrativi, gestione libro presenze/ libro matricola/libro infortuni, gestione buste paga, ricezione certificati medici, compilazione moduli assegni familiari, verifica trattenute sindacali.

- ✓ TRATTAMENTI AFFIDATI ALL'ESTERNO DELLA STRUTTURA (punto 19.7 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196)

La gestione delle paghe dei dipendenti, l'elaborazione delle buste paga, le pratiche di assunzioni e licenziamenti, gli adempimenti INPS e INAIL, sono tutti espletati internamente da personale dipendente della TIZIO srl.

Per la gestione dei dati contabili, la TIZIO si avvale dei servizi offerti dallo **STUDIO DOTT.** _____, corrente in _____. Tale consulente esterno possiede una copia dei dati contabili della TIZIO, necessari per l'espletamento della sua attività professionale.

Per la gestione del sistema informatico la TIZIO si avvale dei servizi offerti dalla _____, corrente in _____.

La TIZIO si rivolge da anni con fiducia a tali strutture esterne le quali hanno sempre garantito assoluta serietà e, nel trattamento dei dati personali, il pieno rispetto dei dettami del Codice Privacy secondo quanto previsto dalla vigente normativa e nel rispetto dell'obbligo di riservatezza e del segreto professionale.

2. Composizione del documento

Il presente documento trae la propria origine dal punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196 (CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI) il quale così dispone:

"*19. Entro il 31 Marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:*

19.1. l'elenco dei trattamenti di dati personali

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività , delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già dal momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato".

La nostra associazione considera il D. Lgs. 30 Giugno 2003, n. 196 (CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI) una conquista civile di grande importanza atta a garantire la tutela dei dati personali di ciascun individuo.

Al fine di recepire completamente lo spirito con cui è stata varata la legge, la nostra associazione ha elaborato il seguente Documento Programmatico Sulla Sicurezza (nel seguito denominato più semplicemente DPSS), che testimonia lo sforzo fatto dalla nostra realtà al fine di garantire la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Il documento procede innanzitutto dalla **Identificazione delle Risorse da proteggere**, risorse che in diverso modo operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati personali. A questo proposito, tramite **l'Analisi dei Rischi**, sono state analizzate le minacce e le vulnerabilità a cui tali risorse sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Valutati i rischi, si è redatto un **Piano di Sicurezza**, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Inoltre è stato definito un **Piano di Verifiche** delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.

Parallelamente alla stesura del Piano di Verifiche è stato redatto un **Piano di Formazione degli Incaricati** tramite il quale si renderanno edotti gli incaricati del trattamento dei rischi e dei modi per prevenire i danni.

Infine, è stato predisposto un piano di **Disaster Recovery** al fine di garantire il ripristino della disponibilità dei dati distrutti e/o danneggiati entro e non oltre sette giorni dall'evento distruttivo o dannoso.

3. Identificazione delle Risorse da Proteggere

Le risorse coinvolte nel trattamento dei dati personali sono state divise in alcune categorie:

- **Luoghi Fisici**. Sono stati analizzati tutti i luoghi ove fisicamente si svolge il trattamento dei dati o si trovano i sistemi di elaborazione o i luoghi ove si conservano i dati.
- **Risorse hardware**. Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Tra queste, particolare rilievo hanno: il server della rete locale della società, ove sono conservati i dati in formato elettronico, ed i personal computer da cui vengono eseguiti i programmi che elaborano i trattamenti.
- **Risorse dati.** Sono stati analizzati tutti gli archivi contenenti dati personali trattati dalla società, siano essi in formato elettronico che in formato cartaceo.
- **Risorse software.** Sono stati analizzati i software applicativi mediante i quali vengono effettuati i trattamenti automatizzati.

3.1 *Luoghi Fisici.*

I luoghi fisici in cui avvengono i trattamenti sono i seguenti:

SCHEDA RILEVAZIONE LUOGHI FISICI	
Città:	
Indirizzo Sede:	DESCRIZIONE SINTETICA SISTEMI DI SICUREZZA (es. portoni blindati, allarmi, vigilanza notturna, estintori)

Locali			
Descrizione e posizione	**Uso** (ufficio titolare, ufficio operativo, archivio, locale server, etc…)	**Dispositivo di protezione** (presenza di porte blindate, serrature, antifurto, etc…)	**Note**
Locale n. 1	Locale Operativo	A tale locale, posto all'ingresso dell'edificio, si può accedere dall'esterno tramite porte scorrevoli con possibilità di blocco dall'interno. Tale locale è dotato di apertura che permette di interfacciare con l'utenza ed è accessibile da una porta con chiave.	In questo locale sono conservati dai cartacei aventi natura comune concernenti clienti e fornitori. Tali dati sono conservati in cassettiere ed armadi. È presente un PC e l'apparecchiatura fax.

3.2 *Risorse hardware.*

Le risorse hardware utilizzate per trattare i dati personali sono analizzate nelle seguenti schede riepilogative:

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 01	
Codice:	PC 1
Descrizione:	Elaboratore PC
Modello:	Produttore: _____ Modello: _____ ____RAM
Sistema Operativo:	_____
Categoria:	[ ] Sistema Elaborativo Server [ ] Sistema Elaborativo Client [ ] Altro Sistema: STAND ALONE
Elaboratore in rete:	[ ] No [ ] Rete Privata [ ] Rete Disponibile al pubblico.
Dislocazione:	Locale n. 1 (v. scheda luoghi fisici)

DISPOSITIVI DI PROTEZIONE	
Presenza di Password:	[ ] No [ ] Si
Antivirus:	[ ] No [ ] Si Tipo/Prodotto: Periodicità di aggiornamento:
Altri dispositivi:	[ ] No [ ] Si

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI	
Componente	**Descrizione** (nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
1 disco fisso da ____ Gb	Nel disco sono memorizzati dati personali aventi natura comune (contabilità).

3.3 *Risorse dati.*

In base al disposto del punto 19.1. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196 si redige l'ELENCO DEI TRATTAMENTI DI DATI PERSONALI.

Gli archivi e le basi dati contenenti i dati personali trattati sono i seguenti:

- BANCA DATI CLIENTI
- BANCA DATI FORNITORI
- BANCA DATI RISORSE UMANE
- BANCA DATI ISTITUTI DI CREDITO
- BANCA DATI ASSICURAZIONI

SCHEDA RILEVAZIONE RISORSE DATI N. 01	
Codice:	BANCA01
Descrizione:	BANCA DATI CLIENTI. In questa banca dati sono conservati i dati dei clienti della società.
Tipologia risorsa:	[X] Archivio Elettronico [X] Archivio Cartaceo Nota: parte dei dati sono in formato cartaceo e sono conservati nei locali n. 1 e 2 e negli uffici n. 1 e 3 (vd. Scheda Luoghi Fisici)
Risorse Hardware su cui è ospitata: (solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)	_____

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Dato	**Natura del dato** (sensibile, comune, giudiziario)
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo	**Dato Comune**
Attività economiche, commerciali, finanziarie, etc…	**Dato Comune**

STRUMENTI E POLITICHE DI BACKUP

Dispositivo di back up:	[ ] Non esistente [X] Si, presente Tipo/Modello: _____ Frequenza di back up: _____ Note:
Incaricati del back up:	_____
Supporti di back up:	Numero di supporti: _____. Dicitura presente sull'etichetta: <<data di salvataggio>> Luoghi di conservazione: cassettiera che si trova nel Locale n.1.

SCHEDA RILEVAZIONE RISORSE DATI N. 02

Codice:	BANCA02
Descrizione:	BANCA DATI FORNITORI. In questa banca dati sono conservati i dati dei fornitori dell'azienda.
Tipologia risorsa:	[X] Archivio Elettronico [X] Archivio Cartaceo Nota: parte dei dati sono in formato cartaceo e sono conservati nei locali n. 1 e 2 e negli uffici n. 1 e 3 (vd. Scheda Luoghi Fisici)
Risorse Hardware su cui è ospitata: (solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)	_____

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Dato	**Natura del dato** (sensibile, comune, giudiziario)
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo	**Dato Comune**
Attività economiche, commerciali, finanziarie, etc…	**Dato Comune**

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di back up:	[ ] Non esistente [X] Si, presente Tipo/Modello: _____ Frequenza di back up: _____ Note:
Incaricati del back up:	_____
Supporti di back up:	Numero di supporti: _____. Dicitura presente sull'etichetta: <<data di salvataggio>> Luoghi di conservazione: cassettiera che si trova nel Locale n.1.

SCHEDA RILEVAZIONE RISORSE DATI N. 03

Codice:	BANCA03
Descrizione:	BANCA DATI RISORSE UMANE. In questa banca dati sono conservati i dati dei dipendenti dell'azienda e del titolare.
Tipologia risorsa:	[X] Archivio Elettronico [X] Archivio Cartaceo Nota: parte dei dati sono in formato cartaceo e sono conservati nel locale n. 2 e nell'ufficio n. 1 (vd. Scheda Luoghi Fisici)
Risorse Hardware su cui è ospitata: (solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)	

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO

Dato	Natura del dato (sensibile, comune, giudiziario)
Informazioni su convinzioni religiose o appartenenza a organizzazioni di carattere religioso	**Dato Sensibile**
Opinioni politiche; adesioni a partiti od organizzazioni a carattere politico	**Dato Sensibile**
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo	**Dato Comune**
Dati relativi alla famiglia ed a situazioni personali (stato civile,etc..)	**Dato Comune**
Istruzione e cultura (curriculum studi, etc..)	**Dato Comune**
Adesione a sindacati od organizzazioni sindacali	**Dato Sensibile**
Stato di salute	**Dato Sensibile**

STRUMENTI E POLITICHE DI BACKUP

Dispositivo di back up:	[ ] Non esistente

	[X] Si, presente Tipo/Modello: _____ Frequenza di back up: _____ Note:
Incaricati del back up:	_____
Supporti di back up:	Numero di supporti: _____. Dicitura presente sull'etichetta: <<data di salvataggio>> Luoghi di conservazione: cassettiera che si trova nel Locale n.1.

SCHEDA RILEVAZIONE RISORSE DATI N. 04

Codice:	BANCA04
Descrizione:	BANCA DATI ISTITUTI DI CREDITO. In questa banca dati sono conservati i dati degli istituti di credito di cui si avvale la società.
Tipologia risorsa:	[X] Archivio Elettronico [X] Archivio Cartaceo Nota: parte dei dati sono in formato cartaceo e sono conservati nel locale n. 2 e nell'ufficio n. 1 (vd. Scheda Luoghi Fisici)
Risorse Hardware su cui è ospitata: (solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)	_____

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO

Dato	Natura del dato (sensibile, comune, giudiziario)
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo,etc..	**Dato Comune**
Attività economiche, commerciali, finanziarie , etc…	**Dato Comune**

STRUMENTI E POLITICHE DI BACKUP

Dispositivo di back up:	[ ] Non esistente [X] Si, presente Tipo/Modello: _____ Frequenza di back up: _____ Note:
Incaricati del back up:	_____
Supporti di back up:	Numero di supporti: _____. Dicitura presente sull'etichetta: <<data di salvataggio>> Luoghi di conservazione: cassettiera che si trova nel Locale n.1.

SCHEDA RILEVAZIONE RISORSE DATI N. 05

Codice:	BANCA05
Descrizione:	BANCA DATI ASSICURAZIONI. In questa banca dati sono conservati i dati relativi alle assicurazioni stipulate dalla società.
Tipologia risorsa:	[X] Archivio Elettronico [X] Archivio Cartaceo Nota: parte dei dati sono in formato cartaceo e sono conservati nel locale n. 2 e nell'ufficio n. 1 (vd. Scheda Luoghi Fisici)
Risorse Hardware su cui è ospitata: (solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)	_____

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Dato	**Natura del dato** (sensibile, comune, giudiziario)
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo,etc..	**Dato Comune**
Attività economiche, commerciali, finanziarie , etc…	**Dato comune**

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di back up:	[ ] Non esistente [X] Si, presente Tipo/Modello: _____ Frequenza di back up: _____ Note:
Incaricati del back up:	_____
Supporti di back up:	Numero di supporti: _____. Dicitura presente sull'etichetta: <<data di salvataggio>> Luoghi di conservazione: cassettiera che si trova nel Locale n.1.

4. Analisi dei Rischi

Identificate le risorse coinvolte a vario titolo nelle operazioni di trattamento viene operata l'Analisi dei Rischi (punto 19.3 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196).

Per Analisi dei Rischi si intende lo studio delle minacce e delle vulnerabilità a cui sono soggette le risorse. Gli indici di rischio sono fissati mediante una scala semiqualitativa a 4 valori riportatati **nell'Allegato Uno** del precedente documento.

Opereremo l'Analisi in maniera distinta sulle categorie di beni individuati precedentemente.

4.1 *ANALISI DEI RISCHI SULLE RISORSE PROFESSIONALI*

Risorsa (tutte o una specifica)	**Elemento di Rischio**	**Soglia Individuata**	**Eventuale Motivazione**
tutte	Comportamenti errati, sleali o fraudolenti	Lieve	I dipendenti che trattano dati personali sono stati incaricati con apposita lettera scritta contenente la precisa indicazione dei compiti ai quali devono attenersi.
tutte	Organizzazione carente	Lieve	Vi è un solo impiegato amministrativo che tratta i dati personali riguardanti le risorse umane e che elabora e gestisce le buste paga dei dipendenti; questo stesso impiegato tratta altresì dati delle banche e delle assicurazioni. Gli altri impiegati gestiscono la contabilità e trattano dati comuni concernenti clienti e fornitori. Gli operai incaricati possono sottoscrivere documenti di trasporto e pertanto

			vengono a conoscenza dei dati comuni riguardanti i fornitori. Infine gli autisti che effettuano la consegna dei prodotti possono trattare dati comuni concernenti i clienti. Tale suddivisione è sottoposta a periodici controlli al fine di verificare la sua corretta applicazione.
tutte	Perdita o sottrazione credenziali	Lieve	Nella lettera di incarico è stato specificato il comportamento da attuarsi in merito all'utilizzo della propria credenziale di autenticazione (password).

4.2 ANALISI DEI RISCHI SUI LUOGHI FISICI

Risorsa (tutte o una specifica)	**Elemento di Rischio**	**Soglia Individuata**	**Eventuale Motivazione**
tutte	Possibilità di intrusione Furto	Lieve	I locali sono costantemente presidiati durante l'orario di lavoro. La sede dell'impresa è protetta da recinzione perimetrale corredata da cancelli tenuti chiusi anche durante l'attività lavorativa. La zona adiacente ai cancelli ed al parcheggio interno è protetta da videocamere a circuito chiuso con impianto di registrazione. La sede aziendale è protetta da antifurto

			di tipo volumetrico. Durante l'orario notturno l'azienda è sorvegliata dalla vigilanza privata.
tutte	Allagamenti	Lieve	Area non soggetta ad esondazioni o calamità di questo tipo.
tutte	Incendio	Lieve	Totale adeguamento alla L. n. 626/94. La sede aziendale è protetta da allarme antincendio ed è tutelata dall'evenienza di incendio dalla presenza di estintori. La sezione amministrativa è suddivisa dalla sezione produttiva e dal magazzino da porte REI 120.
tutte	Impossibilità di rilevare accessi non autorizzati	Lieve	Gli uffici ed i locali sono sempre presidiati nel periodo di svolgimento dell'attività lavorativa.

4.2 *ANALISI DEI RISCHI SULLE RISORSE HARDWARE*

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
tutte	Uso non autorizzato dell'hardware	Lieve	L'utilizzo dell'hardware è soggetto all'inserimento di password.
tutte	Manomissione/sabotaggio	Lieve	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia.

tutte	Probabilità/frequenza di guasto	Lieve	L'hardware acquistato è di qualità e storicamente non ha mai dato problemi di rilievo. Lo TIZIO si rivolge alla software house di fiducia _____ di _____ che fornisce altresì i programmi gestionali adottati per la contabilità, gestione magazzini e gestione buste paga.
tutte	Rischi connessi all'elettricità	Lieve	La società è dotata di un gruppo di continuità collegato al server che fornisce energia di buona qualità (stabilizzazione) e impedisce l'improvvisa assenza di corrente elettrica.
tutte	Virus informatici, worm e programmi maligni	Lieve	I PC sono dotati di programmi antivirus di qualità con aggiornamento automatico.

4.3 *ANALISI DEI RISCHI SULLE RISORSE DATI*

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
tutte	Accesso non autorizzato	Lieve	All'archivio cartaceo, sia storico che corrente, possono accedere solo i soggetti appositamente incaricati.
tutte	Cancellazione non autorizzata di dati/	Lieve	All'archivio cartaceo possono accedere solo

	manomissione di dati		i diretti incaricati che possiedono le chiavi del locale.
tutte	Perdita di dati	Lieve	Sono effettuate, settimanalmente, copie di back up automatico per tutti i dati presenti sui server.
tutte	Incapacità di ripristinare copie di back up	Lieve	I controlli periodici effettuati sui supporti di back up hanno sempre fornito esiti positivi.

4.4 *ANALISI DEI RISCHI SULLE RISORSE SOFTWARE*

Risorsa (tutte o una specifica)	**Elemento di Rischio**	**Soglia Individuata**	**Eventuale Motivazione**
tutte	Accesso non autorizzato alle basi dati.	Lieve	I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione (finestra di Login).
tutte	Errori software che minacciano l'integrità dei dati	Lieve	I software sono utilizzati da diversi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati
tutte	Presenza di codice non conforme alle specifiche del programma	Lieve	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni.

5. Definizione ed attuazione della Politica di Sicurezza

Al fine di assicurare l'integrità dei dati trattati ed impedirne la comunicazione e/o diffusione non autorizzata, la nostra società ha elaborato una precisa Politica di Sicurezza basata sull'adozione di misure di tipo fisico, logico ed organizzativo (sulla scorta dei punti 19.2, 19.4 e 19.5 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196). Tali misure avranno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal DISCIPLINARE TECNICO, sia un livello idoneo di sicurezza relativamente alle tipologie dei nostri dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

5.1 *MISURE DI SICUREZZA DI TIPO FISICO ADOTTATE*

Descrizione misura	Note ed indicazioni per la corretta applicazione
Custodia degli archivi cartacei	Tutti i documenti cartacei contenenti dati personali sono conservati nei locali e negli uffici, costantemente presidiati e non accessibili al pubblico, in armadi, archivi, cassettiere e schedari dotati di serratura. Gli incaricati possono prelevare i documenti necessari per il trattamento per il tempo occorrente a tale operazione dopo di che hanno il compito di riporli nel sopraccitato luogo preposto alla loro conservazione. Sarà compito dell'incaricato che preleva i documenti garantire che questi ultimi siano rinchiusi, sotto chiave, in un cassetto della propria scrivania nel periodo di temporanea assenza dal posto di lavoro.
Dispositivi antincendio	I locali della sede sono dotati di estintori per la soppressione di focolai di incendio. Totale adeguamento alla L. 626/94. La sezione amministrativa è suddivisa dalla sezione produttiva e dal magazzino da porte REI 120.
Custodia dei supporti magnetici.	I supporti magnetici utilizzati per l'attività di back up sono conservati in una cassettiera interna all'Ufficio n. 1 (vd. Scheda Luoghi Fisici).
Verifica della leggibilità dei supporti di back up (punto 19.5 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196	Periodicamente, almeno ogni 2 mesi, è verificata la leggibilità e l'integrità dei dati di back up.

5.2 *MISURE DI SICUREZZA DI TIPO LOGICO ADOTTATE*

Descrizione misura	Note ed indicazioni per la corretta applicazione
Identificazione degli incaricati preposti alle attività di trattamento	Sono stati individuati e nominati per iscritto gli incaricati preposti al trattamento. Agli incaricati, congiuntamente alla lettera di nomina, verranno indicate le norme operative e di sicurezza a cui attenersi. Le lettere di nomina sono presenti nella **Busta Allegati** del presente documento.

Indicazione dei codici identificativi e delle parole chiave agli incaricati (Punti da 1 a 10 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196)	Gli incaricati sono stati contraddistinti da codici identificativi univoci (USER ID) che neppure in futuro potranno essere associati ad altre persone. Agli incaricati sono state fornite le seguenti parole chiave: • Parola chiave del BIOS del proprio PC (stazione di lavoro). • USER ID (codice identificativo) e parola chiave per accedere alle risorse dati presenti sul server. Le parole chiave saranno composte e modificate in base a quanto previsto dal punto 5 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196. • Parola chiave dello screen saver del proprio PC (stazione di lavoro); lo screen saver, che oscura i dati eventualmente presenti a video, si attiverà dopo alcuni minuti di inattività della stazione di lavoro. La password di protezione dello screen saver consentirà all'utente la disattivazione di quest'ultimo alla ripresa dell'attività.
Assegnazione ed autorizzazione degli elaboratori su cui effettuare i trattamenti	Ad ogni incaricato è stato assegnato un elaboratore tramite il quale potrà accedere agli archivi in formato elettronico su cui operare i trattamenti.
Predisposizione ed aggiornamento degli antivirus (punto 16 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196)	Gli elaboratori connessi ad Internet sono stati protetti con programmi antivirus. Le "firme" dei virus vengono aggiornate automaticamente all'accensione del PC.

5.3 MISURE DI SICUREZZA DI TIPO ORGANIZZATIVO ADOTTATE

Descrizione misura	Note ed indicazioni per la corretta applicazione
Analisi dei Rischi e Documento Programmatico Sulla Sicurezza	Sulla base dell'analisi dei rischi è stato redatto il presente documento programmatico sulla sicurezza. Questo documento sarà divulgato a tutte le funzioni aziendali.

Piano di verifica delle misure adottate	E' stato stabilito un piano di verifica delle misure adottate. Tale piano è illustrato nel presente DPSS al capitolo 6.
Piano di formazione degli incaricati.	E' stato predisposto un piano di formazione degli incaricati. Tale piano è illustrato nel presente DPSS al capitolo 7.
Piano di Ripristino della Disponibilità dei Dati	È stato predisposto un Disaster Recovery volto a garantire la possibilità di ripristinare la disponibilità dei dati distrutti e/o danneggiati. Tale piano è illustrato nel presente DPSS al capitolo 8.
Custodia di documenti cartacei	Tutti i documenti cartacei contenenti dati personali, tranne per i periodi strettamente necessari alle operazioni di trattamento, sono custoditi in armadi all'interno di uffici e locali costantemente presidiati.

6. Piano di Verifica delle Misure Adottate

La bontà delle misure adottate deve essere periodicamente verificata.

Durante queste operazioni di verifica, da effettuarsi al più ogni sei mesi, sarà data particolare importanza a:

- Verificare la bontà delle misure di antiintrusione adottate (in particolare i cancelli automatici di ingresso, il sistema di videosorveglianza, il sistema di allarme volumetrico, i rapporti con la vigilanza privata);
- Bontà di conservazione dei documenti cartacei;
- Accertamento del livello di formazione degli incaricati. Prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta in azienda;
- Corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati. Prevedere la disattivazione dei codici di accesso non utilizzati per più di sei mesi;
- Aggiornamento dei programmi software che trattano i dati personali;
- Integrità dei dati e delle loro copie di back up;
- Accertamento della distruzione dei supporti magnetici che non possono più essere riutilizzati.

7. Piano di Formazione degli incaricati

Gli incaricati dovranno essere "*edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili delle disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare […]*" (punto 19.6 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196).

Recentemente è quindi stato indetto un incontro formativo, tenuto da personale esterno con le opportune competenze, che ha affrontato i seguenti punti:

- Analisi dettagliata del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.
- Disposizioni legislative in tema di tutela dei dati e criminalità informatica.
- Analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato
- Panoramica sugli adempimenti e sul quadro sanzionatorio.
- L'ufficio del Garante.
- Misure minime ed appropriate di sicurezza con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus e misure antihacker), contenitori di sicurezza, sistemi anti intrusione, importanza e modalità di realizzazione delle operazioni di back up, etc..

Coerentemente con l'evoluzione degli strumenti tecnici adottati dalla società e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti nuovi incontri formativi. In ogni caso, almeno una volta l'anno, verrà comunque istituito un incontro per risensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

DESCRIZIONE SINTETICA DEGLI INTERVENTI FORMATIVI	TIPOLOGIE DI INCARICATI INTERESSATI	TEMPI PREVISTI

8. Disaster Recovery

In base al punto 23 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del D. Lgs. 30 Giugno 2003, n. 196 "*sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi e degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni*".

In base a tale disposizione, è stata predisposta una procedura finalizzata alla nuova installazione dei dati persi e/o danneggiati.

- ✓ Avvertire il titolare e l'incaricato che ha in custodia i cd di back up e i cd contenenti i software;
- ✓ Rivolgersi immediatamente al manutentore di fiducia (software house) chiedendone l'intervento;
- ✓ Reinstallare i programmi eventualmente danneggiati o distrutti e provvedere a reinstallare tutti i dati contenuti nelle copie di back up;
- ✓ Provvedere all'aggiornamento dei sistemi operativi appena reinstallati;
- ✓ Seguire tutte le eventuali ulteriori istruzioni suggerite dal tecnico della software house;
- ✓ Impartire istruzioni affinché la procedura di ripristino avvenga entro e non oltre sette giorni dall'avvenuto danneggiamento o distruzione;
- ✓ Prevedere controlli periodici da parte della software house al fine di evitare rischi di distruzione o danneggiamento;
- ✓ Conservare nota cartacea dell'evento disastroso o dannoso, delle ragioni e delle procedure adottate per il ripristino.

9. Allegato 1: Soglie di Rischio

Soglia	Descrizione
Lieve	Con questa soglia viene individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
Media	Con questa soglia viene individuato un rischio superiore al precedente identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
Grave o Gravissimo	Li trattiamo insieme, perché con queste soglie vengono individuati rischi che è sicuramente inaccettabile pensare di correre. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio e contenerlo in livelli accettabili.

Il presente modello è di proprietà dell'Avv. Annalisa Macerata ed è tutelato dalle leggi italiane ed internazionali sul Diritto d'autore. Di conseguenza l'utente è tenuto ad utilizzare il modello nei limiti e per gli scopi per i quali il modello è stato fornito e non potrà in ogni caso riprodurre, copiare, fotocopiare, diffondere, pubblicare e/o divulgare il modello e comunque tutto il materiale di accompagnamento.

L'elaborazione dei testi, anche se curata con scrupolosa attenzione, non può comportare specifiche responsabilità per l'eventuale presenza di involontari errori o inesattezze; pertanto l'utente è tenuto a controllare l'esattezza e la completezza del materiale utilizzato.