SOMMARIO

Redazione:	Nome	Firma	Data
Consulenti			
Verifica:	**Nome**	**Firma**	**Data**
OdV			
Approvazione:	**Nome**	**Firma**	**Data**
Presidente			

Rev.	Data	Descrizione della modifica	Pag. / par. modificati
0	12.09.2018	Prima emissione	---
1	11/2025	Revisione	

1. SCOPO

La presente procedura ha lo scopo di illustrare le modalità adottate dall'azienda per assicurare l'integrità, la riservatezza e la disponibiltà dei dati informatici, e per prevenire i seguenti reati:

- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Falsità nei documenti informatici (art. 491-bis c.p.)

2. RIFERIMENTI

Modello Organizzativo D.Lgs. 231/01 – capitolo V

3. CAMPO DI APPLICAZIONE

Si applica a tutte le attività di gestione ed utilizzo della rete informatica aziendale.

4. RESPONSABILITA'

La responsabilità della sicurezza e della riservatezza generale del Sistema Informatico è del Direttore.
L'addetto IT è responsabile dell'esecuzione del backup dei dati informatici.

5. REGOLE

5.1 Gestione sicurezza informatica

Settimanalmente viene effettuato dal responsabile dell'area IT nonché amministratore di sistema un backup dei dati informatici su server dedicato interno e su hard disc esterno.
Le attività di backup vengono eseguite con modalità idonee a garantire da possibili rischi di cifratura dei backup da ransomware ovvero impossibilità di procedere al rispristino dei backup periodici.
Tutte le postazioni di lavoro sono protette da password e su di esse è installato un software antivirus costantemente aggiornato.
Tutte le operazioni da terminale sono trascritte in un file log di sistema accessibile esclusivamente dall'amministratore di rete.
Anche l'accesso alla posta elettronica, al portale di Fondimpresa ed agli altri applicativi può avvenire solo con l'inserimento delle credenziali di accesso.
Il responsabile IT genera, azzera e conserva in luogo protetto le credenziali di accesso del personale attraverso l'attuaizone deòòa policy "no password escrow", credenziali personali non condivise, reset tramite admin, log e verifiche campionarie.

Le procedure di sicurezza vengono eseguite in conformità con il regolamento GDPR vigente.

5.2 Gestione sicurezza dati

Per sicurezza dei dati si intende la protezione dei dati su supporto informatico tesa a garantire la loro integrità e/o ricostruibilità rispetto a danneggiamenti derivanti da una qualsivoglia causa esterna, nonché la protezione del sistema informatico aziendale rispetto a guasti o malfunzionamenti di varia natura tendenti a ridurre i tempi di interruzione del servizio dal sistema stesso erogato.
La politica di sicurezza della rete è garantita da un sistema di Firewall (hardware/software) che impedisce intrusioni indesiderate di utenti dall'esterno della rete e da un sistema di antivirus che blocca i virus conosciuti all'atto in cui essi tentano di installarsi sul sistema, in dotazione anche ai PC utenti.
La sicurezza dei dati è altresì garantita dal costante aggiornamento dei sistemi operativi e gestionali (browser, Office, PDF reader, gestionali)a cura dell'amministratore di rete e responsabile IT, al fine di ridurre al massimo il rischio exploit "commodity.

5.3 Gestione riservatezza

Per riservatezza si intende la protezione dei dati da accessi impropri o fraudolenti.
La politica di riservatezza della rete è garantita da:

- Una selettiva politica di accesso alle banche dati della Pubblica Amministrazione, fiscali e previdenziali, finalizzate ad impedire alterazioni dei dati fiscali dopo la comunicazione. I dipendenti autorizzati a tale accesso sono ben individuati e accedono alle comunicazioni telematiche attraverso specifiche password, per cui si risale con certezza all'autore delle singole trasmissioni. Le comunicazioni ad INPS e INAIL sono demandate a consulente esterno come intermediario.
- Una politica tendente ad impedire un inserimento improprio di dati su bonifici di pagamento e dati contabili. Tale politica è perseguita attraverso un accesso ai dati contabili protetti da password; le trasmissioni telematiche delle disposizioni di pagamento alle banche vengono effettuate tramite dispositivi specifici protetti da password; vengono effettuati, infine, controlli di quadratura sui resoconti bancari.
- Una politica di adozione del SW applicativo tendente ad eliminare il rischio di sviluppo di software che permetta la commissione di reati. Ciò viene ottenuto attraverso l'adozione e l'uso di pacchetti standard presenti sul mercato.
- Una politica tendente ad impedire alterazione dei dati contabili presenti sul sistema, attraverso un accesso controllato ai dati, protetto da password.
- Una adeguata formazione ed informazione del personale operatore di terminale sui rischi diretti ed indiretti scaturenti dall'utilizzo del sistema informatico aziendale.

6. SISTEMA SANZIONATORIO

In caso di mancata osservanza di siffatte previsioni da parte delle funzioni aziendali espressamente delegate, verranno adottate le sanzioni previste dalla Parte Generale del presente Modello organizzativo.

7. ATTIVITÀ DELL'ORGANISMO DI VIGILANZA

Con periodicità almeno annuale, o diversa periodicità ritenuta idonea all'esercizio del controllo sulla concreta attuazione del modello, l'Organismo di Vigilanza effettua controlli a campione sull'attuazione da parte del responsabile IT delle procedure codificate nel modello atte a prevenire la commissione degli specifici reati presupposto, verificando il compiuto aggiornamento delle procedure di tutela dei dati conformemente alla modifica delle mutazioni normative eventualmente intervenute.