BERSANETTI GIOVANNI

VIALE NAVIGAZIONE INTERNA 15
35129 PADOVA (PD)
Tel: 049 7800207
P.IVA 00685880288

ELENCO DELLE MISURE DI SICUREZZA ADOTTATE

Sono sotto riportate le misure di sicurezza implementate ai sensi dell'art.32 del Reg.to UE 2016/679.

Misure di sicurezza adottate a livello logico ed organizzativo

Verifica dei Back-up.	E' stato predisposto un piano di verifica periodica del corretto funzionamento delle copie di Back-Up.
Consegna istruzioni dettagliate agli addetti.	Ad ogni addetto sono state consegnate istruzioni dettagliate e complete riguardanti il trattamento dei dati personali, a seconda dei suoi compiti e dei dati trattati. ► Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. Istruzioni per assicurare la segretezza della componente riservata della credenziale (es. password) e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. ► Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. Sono impartite istruzioni agli incaricati per non lasciare incostudito e accessibile lo strumento elettronico durante una sessione di trattamento. ► Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei. Gli incaricati hanno ricevuto istruzioni scritte sul comportamento da tenere per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento.
Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile	Il Registro dei Trattamenti e documento cogente e contiene la lista dei trattamenti effettuati eventuali comunicazioni degli stessi all'esterno e relative misure di sicurezza attuate.
Redazione documento Privacy by Design e By Default	Redazione Piano di Privacy by Design e By Default per documentare per tutti i trattamenti l'attuazione delle necessarie misure di sicurezza ex. Art. 32 in grado di garantire un rischio residuale basso
Implementazione Procedura di Nomina a Responsabile del trattamento	Implementazione Procedura di Nomina a Responsabile del trattamento per tutte le strutture esterne che trattano dati per conto del Titolare
Implementazione procedura di verifica per i Responsabile del trattamento	Implementazione procedura di verifica affinché i trattamenti effettuati da esterni abbiano adeguate garanzie di rischio residuale basso

Misure di sicurezza adottate per trattamento

- **Acquisti**

Dati Comuni trattati :	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative
Unità di archiviazione utilizzate per il trattamento	• ARMADIO AMMINISTRAZIONE (sede: Sede principale azienda) • ARMADIO COMMERCIALE (sede: Sede principale azienda) • SERVER (sede: Sede principale azienda)

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Gruppo di continuità	Gruppo di continuità
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10 Sistema Operativo Windows 10
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.

Gestione Personale

Dati Comuni trattati :	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • dati relativi alla famiglia e a situazioni personali • lavoro • istruzione e cultura
Unità di archiviazione utilizzate per il trattamento	• ARMADIO AMMINISTRAZIONE (sede: Sede principale azienda) • SERVER (sede: Sede principale azienda)

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.

Estintori	Installazione Estintori e verifica periodica degli stessi.
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Gruppo di continuità	Gruppo di continuità
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10 Sistema Operativo Windows 10
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.

● Nominativi del personale

Gestione dei nominativi per PL

Dati Comuni trattati :	• nominativo, indirizzo o altri elementi di identificazione personale

Posta elettronica

Dati Comuni trattati :	• nominativo, indirizzo o altri elementi di identificazione personale
Unità di archiviazione utilizzate per il trattamento	• BERSANETTI-HP (sede: Sede principale azienda) • BERS-ENTRATA (sede: Sede principale azienda) • LAUNDRY-HP (sede: Sede principale azienda)

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.
Gruppo di continuità	Gruppo di continuità
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.

Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10 Sistema Operativo Windows 10 ► Windows 8 Sistema Operativo Windows 8
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).

• Sito Internet

Dati Comuni trattati :	• cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie)

• Social Network

Dati Comuni trattati :	• nominativo, indirizzo o altri elementi di identificazione personale

• Vendite

Dati Comuni trattati :	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative
Unità di archiviazione utilizzate per il trattamento	• ARMADIO AMMINISTRAZIONE (sede: Sede principale azienda) • ARMADIO COMMERCIALE (sede: Sede principale azienda) • SERVER (sede: Sede principale azienda)

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.

Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Gruppo di continuità	Gruppo di continuità
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10 Sistema Operativo Windows 10
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.

• Videosorveglianza

Dati Comuni trattati :	• registrazione Filmati VideoSorveglianza

Misure di sicurezza adottate per archivio

• ARMADIO AMMINISTRAZIONE

Trattamenti:	• Vendite • Gestione Personale • Acquisti
Tipo di archivio	• Archivio cartaceo
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.

• ARMADIO COMMERCIALE

Trattamenti:	• Vendite • Acquisti
Tipo di archivio	• Archivio cartaceo
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.

• BERSANETTI-HP

Trattamenti:	• Posta elettronica
Tipo di archivio	• Archivio digitale su rete pubblica
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.
Gruppo di continuità	Gruppo di continuità
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. ► Disattivazione delle vecchie credenziali. ► Disposizioni scritte per la disponibilità dei dati.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).

• BERS-ENTRATA

Trattamenti:	• Posta elettronica
Tipo di archivio	• Archivio digitale su rete pubblica
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.
Gruppo di continuità	Gruppo di continuità
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. ► Disattivazione delle vecchie credenziali. ► Disposizioni scritte per la disponibilità dei dati.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 8
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).

• LAUNDRY-HP

Trattamenti:	• Posta elettronica
Tipo di archivio	• Archivio digitale su rete pubblica
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.
Gruppo di continuità	Gruppo di continuità
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. ► Disattivazione delle vecchie credenziali. ► Disposizioni scritte per la disponibilità dei dati.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).

• SERVER

Trattamenti:	• Vendite • Gestione Personale • Acquisti
Tipo di archivio	• Archivio digitale su rete pubblica
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Contratto con Agenzia di Sorveglianza	Contratto con Agenzia di Sorveglianza
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware.
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio
Installazione impianto Videosorveglianza	Installazione impianto Videosorveglianza
Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Dotazione serrature ufficio.	Se sono presenti dati particolari o giudiziari in archivi cartacei, è consigliata una chiusura a chiave o dell'ufficio o dell'archivio.
Estintori	Installazione Estintori e verifica periodica degli stessi.
Gruppo di continuità	Gruppo di continuità
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. ► Disattivazione delle vecchie credenziali. ► Disposizioni scritte per la disponibilità dei dati.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Windows 10

Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.