REGISTRO TRATTAMENTO SETTORE 5

ALLEGATO A - MISURE DI SICUREZZA

1. Antivirus, firewall e antispam:

tipo: prevenzione del rischio;

minaccia contrastata: azione di virus informatici o accessi internet non autorizzati; descrizione: acquisto e aggiornamento periodico antivirus. La rete è protetta da sistemi antivirus e firewall (non fisico) contro i tentativi di accesso dall'esterno non autorizzati e di intromissioni da Internet. I servizi di posta prevedono protezioni software contro la messaggistica indesiderata (spam).

2. Manutenzione periodica apparecchiature e assistenza:

tipo: mitigazione del rischio;

minaccia contrastata: malfunzionamento hardware;

descrizione: programma manutenzione ordinaria e straordinaria delle apparecchiature. Periodicità diverse a seconda del tipo di intervento. Aggiornamenti automatici.

3. Sistemi informatici:

tipo: prevenzione del rischio;

minaccia contrastata: accessi esterni non autorizzati, sabotaggio, furto, distruzione; descrizione: Le misure di sicurezza sono periodicamente riconsiderate ed adeguate ai progressi tecnici e all´evoluzione dei rischi. Il server è collegato a un gruppo di continuità che consente di prevenire la perdita di dati derivanti da sbalzi di tensione o da interruzione di corrente elettrica.

Il ripristino delle singole banche dati è possibile mediante l'apposita procedura di backup che gestisce anche il ripristino.

I computer risultano tutti sollevati da terra, in modo da evitare eventuali danneggiamenti e perdite di dati dovute ad allagamenti.

4. Sistema di autenticazione informatica:

tipo: prevenzione del rischio;

minaccia contrastata: accessi esterni non autorizzati, sabotaggio, furto, distruzione; descrizione: tutti i trattamenti di dati personali in formato elettronico svolti da Etruria P.A. sono accessibili soltanto attraverso una procedura di autenticazione.

Per poter accedere al trattamento dei dati gli Incaricati devono essere in possesso di credenziali individuali di autenticazione (le procedure di autenticazione avvengano con il riconoscimento diretto e l´identificazione certa dell´utente). Durante il trattamento avranno cura che sul video della propria postazione non siano visibili dati personali da parte di terzi non autorizzati.

Come credenziali individuali l'azienda utilizza password e codice dell'utente.

Le credenziali di identificazione sono individuali e non possono essere rilasciate a più Incaricati anche in tempi diversi. Ad ogni Incaricato possono essere assegnate più credenziali per accessi differenziati a diverse banche di dati o a software gestionali.

Le credenziali non utilizzate da almeno sei mesi devono essere disattivate.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito e non deve contenere riferimenti agevolmente riconducibili all'Incaricato.

Le password devono essere formate dalla combinazione di caratteri alfabetici e numerici e contenere almeno una lettera e un numero. Non possono essere usati più di due caratteri consecutivi identici (es: aaa…). Non possono essere utilizzate sequenze di cifre consecutive (es: 12345…). Non deve essere legata al nome dell'utente, oppure alla sua User-id, o in generale a parole a lui riconducibili (nome della moglie o dei figli, luogo e data di nascita). Non deve essere basata su parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.). Non deve essere uguale ad una delle ultime 5 già utilizzate. Non essere uguali ad una parola presente su un vocabolario, anche scritta al contrario. Le password non devono essere scritte su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, essa deve essere conservata in luogo sicuro e non deve essere confidata a nessuno per nessun motivo.

Le credenziali di accesso sono modificate periodicamente e devono essere bloccate a fronte di reiterati tentativi falliti di autenticazione.

I PC, quando non sono utilizzati, non sono lasciati incustoditi con sessioni applicative aperte o con login effettuato ("clean screen"), ma sono protetti da chiavi fisiche, password o altri tipi di blocchi/controlli.

Durante le operazioni di pulizia dei locali e in assenza degli Incaricati il sistema informatico è disattivato e comunque le procedure informatiche non sono accessibili.

Uso appropriato dei privilegi di amministratore per assicurare il corretto utilizzo delle utenze.

Sistemi e servizi di trattamento dotati di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare dati particolari o giudiziari.

Inventario dei software autorizzati e in dotazione dell'Ente.

Tutte le utenze e password sono archiviate in un database di password a chiave unica utilizzato con applicazione

5. Videosorveglianza e impianto di allarme:

tipo: contrasto del rischio;

minaccia contrastata: accessi esterni non autorizzati, sabotaggio, furto, distruzione; descrizione: videosorveglianza perimetro esterno stabilimento di produzione e aree sensibili interne. L'immobile dove è svolta l'attività della società e quindi dove vengono trattati dati personali è sorvegliato da un impianto di allarme e di videosorveglianza connesso con le forze dell'ordine al fine di impedire l'accesso a eventuali soggetti estranei al di fuori dell'orario di attività.

6. Protezione delle aree e dei locali fisici:

tipo: prevenzione del rischio;

minaccia contrastata: accessi esterni non autorizzati, sabotaggio, furto, distruzione; descrizione: Le aree contenenti dati in supporto cartaceo (mobili ed armadi contenenti documenti), le stampanti e gli apparecchi telefono e fax sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee così da impedire l'accesso a persone non autorizzate. Il personale, Incaricato del trattamento, ha ricevuto le opportune istruzioni per la tutela e la protezione dei dati in formato cartaceo e dei dispositivi informatici attraverso i quali avviene il trattamento dei dati personali.

Identificazione degli Incaricati del trattamento a cui sono state consegnate le chiavi di accesso a determinati uffici. Obbligo restituzione chiavi in caso di cessazione rapporto di lavoro. L'accesso agli Uffici comunali avviene attraverso porte dotate di propria serratura.

L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai dipendenti della società cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate.

Agli Incaricati del trattamento sono fornite istruzioni circa la chiusura degli uffici durante la loro assenza.

Eventuali soggetti ammessi ad accedere ai locali della società in cui avviene il trattamento di dati personali dopo l'orario di chiusura degli uffici sono identificabili e registrati. Autorizzazione scritta ai dipendenti dell'impresa di pulizie di permesso di accesso agli uffici con istruzioni circa il comportamento da tenere.

Dotazione di un registro degli accessi/uscite con uso di apparati di identificazione personale informatica.

7. Formazione degli "Incaricati al trattamento":

tipo: prevenzione del rischio;

minaccia contrastata: diffusione illegale dei dati e corretto trattamento;

descrizione: formazione del personale per fornire informazioni circa le procedure di sicurezza interne. La previsione di interventi formativi degli Incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

Le informative, le nomine e le correlate istruzioni per i trattamenti dei dati sono predisposte dal momento delle procedure di assunzione dei dipendenti e dei collaboratori.

8. Protezione dei supporti cartacei:

tipo: prevenzione del rischio;

minaccia contrastata: diffusione illegale dei dati e corretto trattamento;

descrizione: qualsiasi documento che tratta dati personali deve essere inserito in apposite cartelline non trasparenti. Eventuali rubriche o documenti contenenti dati personali in utilizzo su supporto cartaceo sono richiusi dopo la consultazione al fine di non rendere leggibile i dati dall'esterno. Tutti i documenti cartacei sono custoditi in idonei armadi posti in locali vigilati. Le chiavi per accedere agli armadi sono in possesso solo dei soggetti Incaricati al trattamento e al Responsabile del trattamento. Inoltre, durante le operazioni di pulizia dei locali la documentazione con dati personali risulta non accessibile.

Dotazione di apparecchi di distruggi documenti. Separazione documenti e dati in relazione alla loro natura.

9. Sistema antincendio

tipo: prevenzione del rischio;

minaccia contrastata: distruzione, danneggiamento, perdita dei dati; descrizione: dotazione di estintori/Impianto antincendio.

I locali sono dotati di sistema di aerazione adeguato.

10. Sistema organizzativo

tipo: prevenzione del rischio;

minaccia contrastata: distruzione, danneggiamento, perdita dei dati, accessi esterni non autorizzati, sabotaggio, furto, distruzione;

descrizione: dotazione di apposito software per adempimenti relativi alla normativa di cui al

G.D.P.R. e servizio di consulenza accessibile dal personale dell'Ente.

Valutazioni in ordine alla gestione del rischio.

Verifica periodica volta alla valutazione dell'efficacia delle misure di sicurezza adottate.

Procedure di ripristino in caso di data breach.