ALLEGATO 1

ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

Premessa
1. Definizioni
2. Adempimenti
3. Modalità di svolgimento delle operazioni
4. Istruzioni per l'uso degli strumenti informatici
   a) Gestione strumenti elettronici (pc fissi e portatili)
   b) Gestione username e password
   c) Installazione di hardware e software
   d) Gestione posta elettronica aziendale
   e) Gestione del salvataggio dei dati
   f) Gestione dei supporti rimovibili
   g) Gestione protezione dai virus informatici
5. Istruzioni per l'uso degli strumenti "non elettronici"
   a) distruzione delle copie cartacee
   b) Misure di sicurezza
   c) Prescrizioni per gli incaricati
6. Addetti alla manutenzione
7. Osservanza delle disposizioni in materia di Privacy.
8. Non osservanza della normativa aziendale.
9. Aggiornamento e revisione

PREMESSA

Il presente documento contiene le istruzioni operative per gli autorizzati del trattamento dei dati personali impartite dal Comune di Potenza in qualità di titolare del trattamento, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso di questa Organizzazione diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'organizzazione.

10. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

11. ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dall'organizzazione, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare anche per iscritto eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.
- Partecipare costantemente alle Formazione proposta dall'ente in materia alla privacy e alla protezione dati personali
- Autovalutarsi con attenzione mediante modelli di questionari predisposti o mediante altre modalità da concordare con il data protection officer dell'organizzazione;
- garantire che la(e) finalità si conformi(no) alla legge applicabile e si fondi(no) su una base legale ammissibile;
- comunicare all'interessato la(e) finalità prima del momento in cui le informazioni sono raccolte o utilizzate per la prima volta per una nuova finalità;
- se del caso, fornire spiegazioni sufficienti dell'esigenza di trattare dati sensibili.
- notificare violazioni della privacy ai responsabili definiti nelle procedure dell'organizzazione non appena si venga a conoscenza di una vulnerabilità e di un rischio per gli individui
- Alla cessazione dell'attività lavorativa non utilizzare le autorizzazioni ancora in essere e comunicare ai responsabili le eventuali de-registrazioni da effettuare.
- Nel caso di variazioni di responsabilità o impiego è necessario informare tempestivamente i responsabili se ci si rende conto che le credenziali di accesso sono ancora attive.
- assicurare che gli asset di cui si è responsabile siano inventariati
- assicurare che gli asset siano appropriatamente classificati e protetti
- Classificare asset e informazioni in base al regolamento dell'organizzazione
- definire, relativamente ai propri asset, appropriate regole di controllo di accesso, diritti di accesso e limitazioni per i ruoli specifici degli utenti, con un livello di dettaglio e una severità di controllo proporzionali al rischio relativo alla sicurezza delle informazioni.

12. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto, le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Limitazione della raccolta

limitare la raccolta dei dati personali a quanto rientra nei limiti della legge applicabile ed è strettamente necessario per la(e) finalità specificata(e)

- Minimizzazione dei dati

ridurre strettamente al minimo il trattamento di dati personali.
minimizzare i dati personali che sono trattati e il numero dei privacy stakeholder e delle persone alle quali i dati personali sono divulgati o che hanno accesso ad essi;
assicurare l'adozione di un principio di "necessità, per cui ciascuno dovrebbe avere accesso soltanto ai dati personali necessari per lo svolgimento delle proprie mansioni ufficiali nel quadro della finalità legittima del trattamento di dati personali.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Azienda di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

- Misure organizzative per favorire l'esercizio dei diritti degli interessati

Attuare con attenzione Misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità' e la completezza del riscontro fornito agli interessati

13. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
È obbligatorio mantenere una separazione dell'uso privato e per l'attività istituzionale o di business dei dispositivi, fino ad utilizzare del software per supportare questa separazione e per proteggere i dati su un dispositivo privato;
Se si utilizzano strumenti privati a fornitura dell'accesso alle informazioni sono dopo che gli utenti hanno sottoscritto un accordo per l'utente finale riconoscendo i loro obblighi (protezione fisica, aggiornamento del software ecc.) rinunciando alla proprietà dei dati e permettendo la

cancellazione remota dei dati da parte dell'organizzazione in caso di furto o smarrimento del dispositivo o quando non più autorizzati a utilizzare il servizio.
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

14. **Gestione strumenti elettronici** (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:
• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
    - Non deve mai essere disattivato;
    - Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
    - Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento, conviene prediligere le stampanti che hanno un pin per attivazione della stampa
Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:
• prima della riconsegna, rimuovere eventuali file ivi elaborati;
• quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

15. **Gestione username e password**

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
• tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;

• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.
Ciascun incaricato deve scegliere le password in base ai seguenti criteri:
• devono essere lunghe almeno otto caratteri;
• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
• non deve essere uguali alle precedenti.
Per la corretta gestione della password è necessario:
• Almeno ogni 3 mesi è obbligatorio cambiare la password;
• Ogni password ricevuta va modificata al primo utilizzo;
• La password venga conservata in un luogo sicuro;
• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.
• Le credenziali sono disattivate in caso di perdita della qualità
• Le credenziali sono disattivate se inutilizzate per sei mesi

16. Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto, si raccomanda agli utenti dei PC di rispettare i seguenti divieti:
• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
• Non installare sistemi per connessione esterne (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.
Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

17. Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza dell'azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:
• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
• l'indirizzo del destinatario sia stato correttamente digitato,
• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
• Nel caso in cui si debbano trasmettere documenti contenenti dati sensibili si deve valutare con attenzione la criptazione degli allegati da trasmettere per esempio con pdf criptati mediante password

18. Gestione del salvataggio dei dati

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.
Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup siano funzionali e non corrotti. Il backup deve essere eseguito mediante software sul cloud con criptazione pear to pear, backup giornaliero e data retention almeno per 120 giorni oppure con dischi magnetici esternim, CD e DVD.
Prevenire il rischio del deperimento dei supporti durante il periodo in cui i dati archiviati sono ancora necessari mediante il trasferimento dei dati su supporti nuovi prima che diventino illeggibili;

19. Gestione dei supporti rimovibili

Si sconsiglia l'uso dei supporti rimovibili come le penne usb e gli hard disk esterni. Se proprio necessario il loro utilizzo deve essere autorizzato dal centro elaborazione dati. In tutti i casi non possono essere utilizzati per memorizzare dati sensibili o dati giudiziari a meno che questi non siano crittografati.
Inoltre, questi dispositivi, diversi dalla firma digitale, devono essere monitorati con costanza e devono essere utilizzati sempre negli stessi pc.
Non è consentito lo scambio di dati mediante chiavette usb e hard disk esterni provenienti da soggetti esterni all'organizzazione.
I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del Centro Elaborazione Dati. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

20. Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

21. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un trita documenti.

c) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
• i supporti devono essere archiviati in ambiente ad accesso controllato;
• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che

avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

22. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dall'organizzazione, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

23. Telelavoro

La fornitura di accesso dovrà avvenire in modalità desktop virtuale che prevenga l'elaborazione e la memorizzazione di informazioni su dispositivi privati;
L'Incaricato dovrà attuare tutte le misure indonee a prevenire le minacce di accesso non autorizzato alle informazioni o alle risorse da parte di altri soggetti che frequentano il luogo, per esempio i famigliari e gli amici;
Conformarsi alle politiche e alle procedure per prevenire discussioni riguardo i diritti per la proprietà intellettuale sviluppatisi su dispositivi privati;
Accordare l'accesso a dispositivi privati (per verificare la sicurezza del sistema o durante un'indagine);
Adottare tutte le cautele affinché il sistema sia protetto da malware non disattivando l'antivirus fornito dall'organizzazione e mantenendolo costantemente aggiornato.

24. Trasporto di supporti fisici

Dovrebbero essere considerate le seguenti linee guida per proteggere i supporti che contengono informazioni e che devono essere trasportati:

- dovrebbe essere utilizzato un sistema di trasporto o un corriere affidabile;
- dovrebbe essere concordata con la direzione una lista dei corrieri autorizzati;
- dovrebbero essere sviluppate delle procedure per verificare l'identificazione dei corrieri;
- gli imballaggi dovrebbero essere adatti a proteggere il loro contenuto da danneggiamenti fisici che possono accadere durante il trasporto, in conformità con le specifiche del produttore, per esempio proteggendoli contro ogni fattore ambientale che può ridurre l'affidabilità dei supporti come l'esposizione al caldo, all'umidità o ai campi elettromagnetici;
- dovrebbe essere tenuto un registro che identifichi il contenuto dei supporti, la protezione applicata cosi come una traccia dei tempi del trasferimento ai custodi del transito e di ricezione a destinazione.

25. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

26. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

27. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

Il Titolare del Trattamento

Allegato A. Politica di protezione dal malware

La protezione contro il malware dovrebbe essere basata su software per l'individuazione e la rimozione del malware, sulla consapevolezza in materia di sicurezza delle informazioni e su adeguati controlli per l'accesso ai sistemi nonché per la gestione dei cambiamenti. Si dovrebbero considerare le seguenti linee guida:

12. stabilire una politica formale che proibisca l'uso di software non autorizzato
13. attuare controlli che prevengano o individuino l'uso di software non autorizzato (vedere esempio whitelisting delle applicazioni)
14. Attuare controlli che prevengano o individuino l'uso di siti web malevoli conosciuti (per esempio blacklisting);
15. stabilire una politica formale per proteggersi dai rischi relativi alla ricezione di software e file attraverso reti esterne o altri mezzi, indicando quali misure protettive dovrebbero essere intraprese;
16. ridurre le vulnerabilità che potrebbero essere sfruttate dal malware, per esempio attraverso la gestione delle vulnerabilità tecniche
17. condurre riesami regolari del software e dei dati contenuti nei sistemi a supporto dei processi critici di business; la presenza di file non approvati o di aggiunte non autorizzate dovrebbe essere oggetto di indagini formali;

18. installare e aggiornare regolarmente il software per l'individuazione del malware e per la relativa riparazione, in modo da esaminare sistemi e supporti come precauzione occasionale o su base periodica; le scansioni effettuate dovrebbero includere:
    1. una scansione per la ricerca di malware in ogni file ricevuto attraverso la rete o qualsiasi altro supporto di memorizzazione e prima del suo uso;
    2. una scansione, prima del loro uso, degli allegati di posta elettronica e dei file scaricati per la ricerca di malware; questa attività dovrebbe essere svolta in diversi punti, per esempio sui server di posta elettronica, sulle postazioni di lavoro e all'ingresso della rete dell'organizzazione;
    3. una scansione delle pagine web alla ricerca di malware;
19. definire procedure e responsabilità per: la protezione dei sistemi dal malware effettuare formazione e addestramento per il loro impiego, predisporre rapporti e ripristinare la situazione dopo un'infezione provocata dal malware;
20. predisporre adeguati piani di continuità operativa per la ripresa dopo un'infezione provocata dal malware, includendo tutti i necessari accorgimenti per il backup e per il ripristino di dati e del software
21. attuare procedure per la raccolta periodica di informazioni, come l'iscrizione a mailing list o la verifica di siti web che forniscono informazioni sui nuovi malware attuare procedure per verificare le informazioni collegate al malware e assicurare che i bollettini di avvertimento siano accurati e informativi; responsabili dell'organizzazione dovrebbero assicurarsi che vengano utilizzate fonti di informazioni qualificate come per esempio periodici di buona reputazione, siti Internet affidabili o fornitori che producono software di protezione contro il malware al fine di distinguere false segnalazioni di malware (hoax) da quelle vere; tutti gli utenti dovrebbero essere consapevoli del problema dei falsi allarmi e sapere cosa fare in caso li si riceva.
22. isolare gli ambienti in cui si potrebbero concretizzare impatti catastrofici.

<u>Altre informazioni</u>

L'uso di due o più prodotti software per la protezione contro il malware nei vari ambienti di elaborazione delle informazioni, sviluppati da produttori diversi e con differenti tecnologie può incrementare l'efficacia della protezione contro il malware

Bisognerebbe fare attenzione a proteggersi contro l'introduzione di malware durante le operazioni di manutenzione e di emergenza, che potrebbero aggirare i normali controlli di In determinate condizioni, la protezione contro il malware potrebbe causare disturbi alle attività operative

L'uso di soli software per l'individuazione del malware e la relativa riparazione come unico procedure operative che prevengano l'introduzione del malware.

Allegato B. gestione delle vulnerabilità tecniche

Obiettivo: Prevenire lo sfruttamento di vulnerabilità tecniche

Gestione delle vulnerabilità tecniche

Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati dovrebbero essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità dovrebbe essere valutata e appropriate misure dovrebbero essere intraprese per affrontare i rischi relativi

Un inventario degli asset completo e aggiornato (vedere punto 8) è un prerequisito per un'efficace gestione delle vulnerabilità tecniche. Le informazioni specifiche necessarie per supportare una gestione delle vulnerabilità tecniche comprendono il produttore del software, i numeri di versione, lo stato di distribuzione (per esempio quale software è installato su quali sistemi) e il personale responsabile per il software all'interno dell'organizzazione.

Dovrebbero essere intraprese azioni appropriate e tempestive per rispondere all'identificazione di potenziali vulnerabilità tecniche. Le seguenti linee guida dovrebbero essere seguite per stabilire un

processo di gestione efficace per le vulnerabilità tecniche organizzazione dovrebbe definire e stabilire i ruoli e le responsabilità relative alla gestione delle vulnerabilità tecniche, incluso il monitoraggio delle vulnerabilità, alla valutazione del rischio delle vulnerabilità, all'applicazione delle patch, tracciamento degli asset e ad ogni responsabilità di coordinamento richiesta;

8. le risorse informative da utilizzare per identificare vulnerabilità tecniche pertinenti e per mantenere una consapevolezza su di esse dovrebbero essere identificate per quanto riguarda il software e le altre tecnologie (basate sull'inventario degli asset, vedere punto 8.1.1); queste risorse informative dovrebbero essere aggiornate in base a cambiamenti nell'inventario o quando sono trovate altre risorse nuove o utili;
9. dovrebbe essere definita una scala temporale per reagire alle notifiche di vulnerabilità tecniche potenzialmente pertinenti;
10. una volta identificata una potenziale vulnerabilità tecnica, l'organizzazione dovrebbe identificare i rischi relativi e le azioni da intraprendere; tali azioni potrebbero includere l'applicazione delle patch ai sistemi vulnerabili o l'adozione di altri controlli;
11. seconda dell'urgenza con cui una vulnerabilità tecnica necessita di essere affrontata, le azioni intraprese dovrebbero essere portate a termine coerentemente con i controlli collegati alla gestione dei cambiamenti (vedere punto 12.1.2) o seguendo le procedure di risposta agli incidenti relativi alla sicurezza delle informazioni (vedere punto 16.1.5);
12. se una patch è resa disponibile da una sorgente legittima, i rischi legati alla sua installazione dovrebbero essere valutati rischi generati dalla vulnerabilità dovrebbero essere confrontati con il rischio dell'installazione della patch);
13. le patch dovrebbero essere sottoposte a test e valutate prima della loro installazione per assicurare che siano efficaci e non comportino effetti collaterali intollerabili; se nessuna patch fosse disponibile, altri controlli dovrebbero essere presi in considerazione quali
    1. la disattivazione dei servizi o delle funzionalità legate alla vulnerabilità;
    2. l'adattamento o l'adozione di controlli di accesso aggiuntivi, ad esempio firewall ai confini della rete (vedere punto 13.1);
    3. l'aumento del monitoraggio per l'individuazione di attacchi in corso;
    4. l'aumento della consapevolezza sulla vulnerabilità.
14. dovrebbe essere mantenuto un log di audit di tutte le procedure intraprese il processo di gestione delle vulnerabilità tecniche dovrebbe essere monitorato e valutato regolarmente per assicurare la sua efficacia ed efficienza;
15. i sistemi ad alto rischio dovrebbero essere considerati per primi;
16. un processo efficace di gestione delle vulnerabilità tecniche dovrebbe essere allineato con le attività di gestione degli incidenti per comunicare dati sulle vulnerabilità alle funzioni adibite alla risposta agli incidenti e per fornire procedure tecniche da eseguire in caso di incidente;
17. definire una procedura per indirizzare la situazione in cui una vulnerabilità sia stata identificata ma non esista una contromisura adatta. In questa situazione, l'organizzazione dovrebbe valutare i rischi collegati alla vulnerabilità conosciuta e definire appropriate azioni di individuazione e correzione

La gestione delle vulnerabilità tecniche può essere vista come una sotto-funzione della gestione dei cambiamenti e, come tale, può avvantaggiarsi dei processi e delle procedure relative

I produttori di software sono sottoposti a pressioni per rilasciare aggiornamenti non appena possibile. Esiste quindi la possibilità che una patch possa non indirizzare il problema

adeguatamente e che possa invece avere effetti collaterali negativi. In alcuni casi, inoltre, la disinstallazione di una patch installata può non essere facilmente effettuabile

Nel caso non sia possibile effettuare adeguati test delle patch, ad esempio peri costi o per la mancanza di risorse, può essere considerato un ritardo nella loro installazione per valutare i rischi relativi, basandosi sulle esperienze comunicate da altri utenti. L'impiego della ISO/NEC 27031[14] può rivelarsi utile in questo contesto