Istruzioni Operative Generali per gli Autorizzati al Trattamento dei Dati Personali

SOMMARIO

1 – Scopo ……3

2 - Definizioni ……...3

3 – Premessa ……..3

4 - Istruzioni generali per le persone autorizzate al trattamento dei dati personali ……4

4.1 - Trattamenti senza l'ausilio di strumenti elettronici ……...6

4.1.1 – Custodia ……...6

4.1.2 – Comunicazione ……...6

4.1.3 – Distruzione ……...6

4.1.4 - Istruzioni in caso di trattamento di categorie di dati personali particolari o giudiziari ……....6

4.2 - Trattamenti di dati personali con l'ausilio di strumenti elettronici ……..7

4.2.1 - Gestione strumenti elettronici ……..7

4.2.2 - Gestione credenziali di autenticazione……8

4.2.3 - Installazione di hardware e software……9

4.2.4 - Gestione del salvataggio dei dati ……9

4.2.5 - Gestione della cancellazione dei dati ……..9

4.2.6 - Gestione dei supporti rimovibili ……10

4.2.7 - Gestione protezione dai virus informatici ……..10

4.2.8 - Gestione posta elettronica aziendale ……..10

5 - Istruzioni di carattere generale ……11

5.1 Come comportarsi in presenza di ospiti o di personale di servizio……11

5.2 - Come usare correttamente Internet……11

5.3 - Utilizzo di servizi di produttività personale in Cloud……11

5.4 - Come comportarsi in caso di violazioni di sicurezza ……11

6 - Osservanza delle disposizioni in materia di protezione dati personali ……....12

7 - Aggiornamento e revisione ……..12

Allegato 1 - ***"Schema Avvertenza Privacy"*** **……13**

Allegato 2 – "*Politica di protezione dal malware***" ……14**

Allegato 3 – "*Gestione delle vulnerabilità tecniche***" ……15**

1 - Scopo

Il presente documento risponde alle indicazioni contenute nel Regolamento europeo sulla protezione dei dati 2016/679 ((di seguito anche solo **"GDPR"**) con particolare riferimento all'art. 28, comma 3 e all'art. 29, che richiedono che qualsiasi persona "*autorizzata al trattamento dei dati personali*" sia debitamente informata ed istruita al fine di mettere in atto comportamenti che assicurino l'adeguato livello di sicurezza e riservatezza commisurato al "valore" del dato e ai conseguenti rischi.

2 - Definizioni

Secondo l'articolo 4 del GDPR e la normativa nazionale in materia vigente, si definisce:

a) **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;
b) **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;
c) **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

Per ulteriori definizioni si rinvia al predetto articolo 4 del GDPR.

3 - Premessa

Al fine di ottemperare all'esigenza di informazione ed istruzione delle persone autorizzate al trattamento di dati personali, le seguenti disposizioni si riferiscono agli aspetti generali di comportamento ed attenzione che devono essere adottate nello svolgimento delle attività di competenza di ciascuno dei dipendenti appositamente autorizzati al trattamento dei dati personali.

Le istruzioni specifiche, relative al trattamento o ai trattamenti per i quali la persona viene autorizzata e, conseguentemente, censita nel registro dei trattamenti, esulano dal presente documento e sono compito del titolare/responsabile o suo delegato impartire.

L'autorizzazione al trattamento di dati personali avviene in maniera esplicita da parte del titolare o suo delegato, indicando:

1. la persona autorizzata,
2. i trattamenti e la categoria di dati personali a cui si è autorizzati, censiti nel registro dei trattamenti,
3. l'applicazione IT (laddove esistente) e il relativo profilo di accesso, e/o l'archivio cartaceo di riferimento,
4. le istruzioni generali facendo riferimento al presente documento,
5. eventuali istruzioni specifiche.

I dipendenti ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativi a tali dati, devono ispirarsi al principio generale di liceità, diligenza, correttezza e trasparenza.

Ogni utilizzo dei dati in possesso di questa Società per la Regolamentazione dei Rifiuti Palermo Area Metropolitana S.C.p.A (d'ora innanzi solo ***"SRR"***) diverso da finalità strettamente professionali ed istituzionali, 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 patrimonio informativo e all'immagine della SRR.

4 - Istruzioni generali per le persone autorizzate al trattamento dei dati personali

In ottemperanza alle disposizioni previste dalla normativa in atto vigente in materia di protezione dei dati personali ed in relazione alle attività svolte nell'ambito di ciascuna struttura organizzativa (Area-Servizio- Settore-Ufficio) in cui opera la persona formalmente autorizzata al trattamento dei dati personali, la stessa dovrà effettuare i trattamenti di competenza attenendosi scrupolosamente alle istruzioni contenute nel presente documento e ad ogni ulteriore indicazione, fornita dal Titolare/Responsabile o da suo delegato.

I comportamenti messi in atto nell'esercizio delle funzioni/compiti di ciascun autorizzato, debbono conformarsi ai seguenti principi generali:

1. **consapevolezza e responsabilizzazione del "valore" dei dati trattati;**
2. **osservanza e obbligo dei criteri di riservatezza;**
3. **liceità e correttezza;**
4. **rispetto delle misure di sicurezza;**
5. **custodia e controllo dei dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di divulgazione o accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.**

Ciascun Autorizzato del trattamento, indipendentemente dal relativo livello di autorizzazione ricevuta, deve quindi:

a) rispettare i principi generali del GDPR e della normativa nazionale vigente ed in materia applicabile, 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, essenziali e legittimi;

b) rispettare l'obbligo di riservatezza e segretezza e, conseguentemente, il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto, qualora ciò non sia espressamente previsto da una fonte di rango legale;

c) 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 all'uopo preposti;

d) rispettare le idonee misure di sicurezza adottate dall'organizzazione, atte a salvaguardare la riservatezza e l'integrità dei dati;

e) segnalare - anche per iscritto - circa eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica) che possano migliorare lo svolgimento delle operazioni affidate;

f) accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;

g) in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;

h) mantenere riservate le proprie credenziali di autenticazione;

i) svolgere le attività previste dai trattamenti secondo le specifiche direttive impartite dal soggetto Autorizzato di livello superiore al proprio (Designato) e/o dal Referente di rispettivo riferimento o dal DPO;

j) non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione dei soggetti all'uopo preordinati;

k) rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

l) informare tempestivamente il proprio diretto superiore ed il DPO in caso di incidente di sicurezza che coinvolga dati particolari e non;

m) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli d'ufficio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

n) eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;

o) partecipare costantemente all'attività di formazione proposta dall'ente in materia di privacy e protezione dei dati personali;

p) auto-valutarsi con attenzione mediante modelli di questionari predisposti o mediante altre modalità da concordare con il DPO della SRR;

q) garantire che la(e) finalità si conformi(no) alla legge applicabile e si fondi(no) su una base legale ammissibile;

r) 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;

s) se del caso, fornire spiegazioni sufficienti ed adeguate circa l'esigenza di trattare dati particolari o giudiziari;

t) notificare le violazioni della privacy, secondo le specifiche modalità previste nell'apposita **procedura operativa aziendale di gestione del Data Breach**, non appena si venga a conoscenza di una vulnerabilità e di un rischio per gli individui;

u) alla cessazione dell'attività lavorativa non utilizzare le autorizzazioni ancora in essere e comunicare ai propri diretti responsabili le eventuali de-registrazioni da effettuare;

v) nel caso di variazioni di responsabilità, funzione o impiego è necessario informare tempestivamente i propri diretti responsabili e, ciò, qualora ci si rendesse conto che le credenziali di accesso sono ancora attive;

w) assicurare che gli asset di cui si è responsabili siano inventariati;

x) assicurare che gli asset siano appropriatamente classificati e protetti;

y) classificare asset e informazioni in base al regolamento aziendale in materia di Protezione dei Dati Personali;

z) 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.

Le principali operazioni demandate agli Autorizzati del trattamento sono:

- **l'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;
- **la verifica circa l'esattezza del dato e la corretta digitazione**: al momento della registrazione dei dati raccolti, occorre prestare particolare 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 in merito alla corretta gestione dell'anagrafica e allo svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- **l'esecuzione di ogni disposizione/istruzione prevista per l'accesso fisico ai locali**: I locali ove sono custoditi i dati personali (ed in particolare quelli di natura particolare), 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 custodire 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;
- **la limitazione della raccolta:** limitare la raccolta dei dati personali a quanto rientra nei limiti e nell'ambito della legge applicabile, nonché in ordine a quanto è strettamente necessario per dar seguito alle finalità specificate;
- **la minimizzazione dei dati**: ridurre strettamente al minimo indispensabile il trattamento di dati personali. Minimizzare, quindi, 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;
- **l'osservanza del principio di necessità**: per cui ciascuno autorizzato dovrebbe avere accesso soltanto ai dati personali necessari per lo svolgimento delle proprie mansioni istituzionali, nel quadro delle legittime finalità sottese al trattamento dei dati stessi;
- **il rispetto delle misure organizzative per favorire l'esercizio dei diritti degli interessati:** attuare con meticolosa cura ogni misura organizzativa prevista per favorire l'esercizio dei diritti ed il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità' e la completezza del riscontro fornito agli

stessi. A tal specifico riguardo si rimanda alla specifica **procedura operativa aziendale sull'esercizio dei diritti dell'interessato.**

Le misure di sicurezza previste dalle policy della SRR in relazione agli obblighi di cui all'art. 32 del GDPR, che di seguito si declinano, sono per maggior chiarezza espositiva distinte in funzione delle seguenti modalità di trattamento dei dati:

a) senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);
b) con strumenti elettronici (PC e sistemi informatici).

4.1 - Trattamenti senza l'ausilio di strumenti elettronici

Per *"trattamenti senza l'ausilio di strumenti elettronici"* si intendono tutte le operazioni di cui al precedente paragrafo 2, comma 1, lett.ra b) delle presenti istruzioni, effettuatesi per la gestione di dati personali contenuti in supporti cartacei e/o di altro tipo come ad esempio microfilm, microfiches e lucidi.

I supporti di tipo magnetico e/o ottico, contenenti dati personali, devono essere protetti dal punto di vista fisico con le misure di sicurezza analoghe a quelle previste per i supporti cartacei.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali e commisurate al valore del dato.

Il "valore del dato" è costituito da una valutazione della tipologia di dati trattati (comuni, particolari, giudiziari), dalle categorie degli interessati, dalla loro numerosità, ecc…

4.1.1 - Custodia

I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili alle persone non autorizzate al trattamento dei dati stessi (es. armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.

I documenti contenenti dati personali non devono rimanere incustoditi sulle scrivanie o tavoli di lavoro, stampante di rete ecc...

Il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro.

È severamente vietato utilizzare documenti contenenti dati personali (dati particolari - ex dati sensibili - o giudiziari) come carta da riciclo o per appunti.

4.1.2 - Comunicazione

L'utilizzo dei dati personali deve avvenire in base al principio del limite d'accesso alle sole informazioni per le quali l'utente ha necessità di accedere e, cioè, essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie attività lavorative (anche se queste persone sono a loro volta persone autorizzate al trattamento dei dati personali).

I dati non devono essere comunicati all'esterno dell'ente e comunque a soggetti terzi se non previa autorizzazione e mediante gli appositi canali istituzionali.

4.1.3 - Distruzione

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili, esclusivamente, da parte dell'autorizzato del relativo trattamento.

Per la distruzione dei documenti, qualora il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale autorizzato che avvierà al macero la documentazione di che trattasi è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido.

I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

4.1.4 - Istruzioni in caso di trattamento di categorie di dati personali particolari o giudiziari

I documenti contenenti categorie particolari di dati personali (di seguito "***dati particolari***") e dati relativi a condanne penali e reati (di seguito "***giudiziari***") - la cui individuazione è stata già preventivamente effettuata a mente dell'**ALLEGATO 1 ("Tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento")** del Regolamento aziendale in materia di Protezione dei Dati Personali - devono essere controllati e custoditi in modo che non vi accedano persone prive di autorizzazione o con un livello di autorizzazione non adeguato alla categoria del relativo trattamento. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc…, deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.

4.2 - Trattamenti di dati personali con l'ausilio di strumenti elettronici

Come principio generale, sia i dispositivi di memorizzazione dei PC che ogni unità di rete (*Stampanti, Scanner et similia*), devono contenere informazioni strettamente professionali ed istituzionali e non possono essere utilizzati per scopi diversi e di natura personale (immagini, video e documenti personali).

Di seguito sono riportate apposite indicazioni per la gestione dei diversi strumenti informatici in dotazione all'azienda ed oggetto di trattamento di dati personali, nonché per la gestione delle credenziali di autenticazione.

4.2.1 - Gestione strumenti elettronici

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (*a titolo esemplificativo: personal computer, periferiche varie, lettori di smart card, ecc…*).

Ogni autorizzato deve 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 alla SRR 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)**, è necessario che l'Autorizzato:

- si assicuri che al termine dell'orario di servizio, il PC risulti regolarmente spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- si accerti, in caso di assenza momentaneamente dalla propria postazione, che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, l'autorizzato deve chiudere la sessione di lavoro sul PC facendo logout ed avere attivo un salvaschermo (screen- saver) protetto da 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 5 minuti di inattività del PC;
  - deve essere messo in funzione manualmente ogni volta si lasci il PC incustodito ed acceso;

Per l'utilizzo dei **PC portatili** valgono le regole elencate per i PC fissi, 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 (ad es. cassaforte o armadi/cassetti con serratura);
- in caso di furto di un portatile è necessario avvertire tempestivamente il proprio diretto superiore ed il Responsabile del Servizio Informatico/Amministratore di Sistema, onde prevenire possibili intrusioni ai sistemi aziendali, oltre che denunciare tempestivamente il fatto alle autorità competenti;

- 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.

Per quanto concerne l'uso delle **Stampanti multifunzione** in dotazione alla sede istituzionale della SRR gli utenti sono tenuti a:

- a stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative ed istituzionali;
- a prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, ove possibile.

È severamente vietato l'utilizzo delle fotocopiatrici per fini personali.

Per l'utilizzo dei fotocopiatori occorre che ciascun Autorizzato inserisca l'apposito PIN per la generazione della relativa stampa.

Nel caso in cui si rendesse necessaria la stampa di informazioni riservate e per qualsivoglia motivo la procedura di stampa tramite PIN non dovesse essere applicabile, l'autorizzato dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

Maggiori istruzione saranno diramate per mezzo di specifiche direttive.

4.2.2 - Gestione credenziali di autenticazione.

L'accesso ai dispositivi e/o alle procedure informatiche che trattano dati personali è consentito alle persone autorizzate in possesso di apposite "credenziali di autenticazione" (profilo di accesso) che permettano il superamento di una procedura di autenticazione.

Le credenziali di autenticazione consistono in un codice per l'identificazione delle persone autorizzate al trattamento dei dati personali (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card, badge, tessera sanitaria, sistemi a due o più fattori, ecc..) o in una caratteristica biometrica.

L'adozione ed il corretto utilizzo delle credenziali è fondamentale per il regolare utilizzo dei dispositivi e delle applicazioni aziendali, in quanto:

a. tutela l'utilizzatore ed in generale la SRR da accessi illeciti, atti di vandalismo ed, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;

b. tutela l'Autorizzato 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;

c. è necessario per gestire correttamente gli accessi a risorse condivise.

Le persone autorizzate al trattamento dei dati personali devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

Ciascun autorizzato deve scegliere le password in base ai seguenti criteri:

- **devono essere composte da almeno otto caratteri;**
- **non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori;**
- **devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;**
- **non devono essere uguali alle precedenti.**

Per la corretta gestione della password è necessario:

- **che almeno ogni 3 mesi si provveda alla relativa rigenerazione (è obbligatorio cambiare la password);**
- **che ogni password ricevuta sia modificata immediatamente al primo utilizzo;**
- **che la password venga conservata in un luogo sicuro;**
- **che la password non sia rivelata o condivisa con i colleghi di lavoro, famigliari e amici e, ciò, soprattutto attraverso il telefono;**
- **che non venga utilizzata la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni;**
- **che le credenziali siano disattivate in caso di perdita della qualità di soggetto autorizzato al trattamento di dati personali;**
- **che le credenziali siano disattivate se inutilizzate per oltre sei mesi**.

In caso di trattamento di dati particolari o giudiziari, l'accesso ai sistemi e alle applicazioni deve avvenire tramite sistemi di autenticazione "robusta" (strong authentication). In questi casi, nonché in tutti gli altri eventuali casi in cui è prevista la strong authentication per accedere ai sistemi, oltre a quanto indicato nelle superiori istruzioni, la persona autorizzata al trattamento dei dati personali deve, altresì, attenersi alle seguenti specifiche istruzioni per quanto riguarda la gestione delle proprie credenziali e dispositivi di autenticazione:

- **i dispositivi di strong authentication (es. token, smart card, ecc…) devono essere conservati con cura, per evitare furti o smarrimenti.**
- **la persona autorizzata al trattamento dei dati personali deve segnalare prontamente ogni fatto anomalo (es. furto, smarrimento, ecc.) riguardante i propri dispositivi di autenticazione e, ciò, tramite presentazione di una dichiarazione sostitutiva di atto notorio rivolta alla SRR o mediante denuncia alle autorità competenti, qualora previsto espressamente dalla normativa.**
- **i dispositivi di strong authentication devono essere riconsegnati quando non sono più necessari per svolgere l'attività lavorativa (ad esempio per cambio mansione), oppure al termine del rapporto di lavoro.**

In caso di prolungata assenza della persona autorizzata al trattamento dei dati personali, solo per urgenti ed indifferibili necessità di lavoro che non possano essere espletate con altre modalità, il Dirigente responsabile dell'Area ove incardinato il soggetto autorizzato invierà un'apposita richiesta di reset della password del PC della persona autorizzata al trattamento dei dati personali assente, all'amministratore del sistema di autenticazione o altra funzione competente di riferimento. Eseguita l'operazione di reset password, l'amministratore del sistema di autenticazione, comunicherà la nuova password al dirigente e, al contempo, invierà una email informativa alla persona autorizzata al trattamento dei dati personali assente. Solo nei casi in cui il reset della password non possa essere applicato, le password di accesso ai PC contenenti dati personali, nonché le eventuali password per l'accesso ai singoli file contenenti tali dati, devono essere consegnate in busta chiusa al Dirigente competente per le finalità istituzionali dell'ente.

4.2.3 - Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dal personale all'uopo addetto (dipendenti del Servizio Informatico e/o Amministratore di sistema). Pertanto, si raccomanda agli Autorizzati 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/Amministratore di sistema;**
- **Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.**

4.2.4 - 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) o utilizzati a seguito di acquisizione di apposito servizio prestato da operatori economici terzi qualificati, il Servizio Informatico oppure l'Operatore economico affidatario (che rivestirà la qualifica quale soggetto "*Responsabile del Trattamento*" ex art. 28 del GDPR) 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 Autorizzato deve eseguire almeno una volta al mese la copia degli stessi (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'Autorizzato deve verificare che i supporti informatici utilizzati per il backup siano funzionali e non corrotti.

4.2.5 - Gestione della cancellazione dei dati

Occorre che l'utente cui è assegnato il PC abbia consapevolezza del "valore dei dati personali" archiviati sull'archivio locale del PC stesso come degli eventuali archivi di rete o supporti removibili.

I dati personali conservati sui PC devono essere cancellati in modo sicuro, scegliendo la modalità più idonea al valore di dati archiviati, prima di destinare i PC ad usi diversi. Questa attività deve essere assistita da un addetto con specifiche competenze e ruolo all'interno della SRR.

4.2.6 - Gestione dei supporti rimovibili

Si sconsiglia l'uso dei supporti rimovibili come le penne usb e gli hard disk esterni.

In tutti i casi non possono essere utilizzati per memorizzare dati particolari 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 alla SRR.

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 soltanto dopo essere stati formattati.

Tali operazioni vengono effettuate a cura del Servizio Informatico/Amministratore di sistema.

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.

In caso di perdita o furto occorre immediatamente segnalare il fatto al proprio diretto superiore e al DPO della SRR, per le consequenziali valutazioni del caso a norma del GDPR.

4.2.7 - Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore della SRR è 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 in cui 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 Servizio Informatico/Amministratore di sistema.

Si raccomanda, altresì, 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 esso contenuti e, soprattutto, l'integrità dei sistemi collegati al PC stesso.

4.2.8 - Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti interni ed esterni per le finalità della SRR e in stretta connessione con l'effettiva attività e mansioni del lavoratore che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza e di prevenire conseguenze legali a carico della SRR, 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;**
- **In calce al corpo del messaggio di posta deve essere presente un avviso privacy standardizzato, di cui allo schema ivi allegato (*vedi "All. 1 – Avvertenza Privacy"*), a mezzo del quale si avverta il destinatario, fra l'altro, della confidenzialità/riservatezza del messaggio.**

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare particolare 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 caso in cui si debbano trasmettere documenti contenenti dati particolari/giudiziari (ad es. Buste Paga, Certificati o Documenti contenenti dati particolari/giudiziari et similia) si deve valutare con attenzione la criptazione degli allegati da trasmettere, per esempio con pdf criptati mediante password.

5 - Istruzioni di carattere generale

5.1 Come comportarsi in presenza di ospiti/visitatori o di personale di servizio

Di seguito, alcune regole o comportamenti al fine di evitare rischi nella normale attività lavorativa con altre persone:

- **Fare attendere gli ospiti in luoghi in cui non siano presenti dati riservati o dati personali;**
- **Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo con password del PC (premendo ctrl-alt-canc);**
- **Non rivelare o fare digitare le proprie password dal personale di assistenza tecnica o da altri colleghi;**
- **Non rivelare le password al telefono - nessuno è autorizzato a chiederle - né inviarle per posta elettronica;**
- **Segnalare qualsiasi anomalia o stranezza al DPO della SRR.**
- **Non lasciare incustoditi i propri strumenti di autenticazione forte (es. Tessera sanitaria, badge, ecc.)**

5.2 - Come usare correttamente Internet

Per la gestione dei servizi internet e dei social, si faccia riferimento alle seguenti raccomandazioni:

- **Evitare di scaricare software da Internet (programmi di utilità, di office automation, file multimediali, ecc…) e, ciò, in particolare se non se ne conosce l'attendibilità della sorgente, in quanto questo può essere pericoloso per i dati e la rete aziendale. I software necessari all'attività lavorativa vanno richiesti alle competenti funzioni aziendali;**
- **Usare Internet entro i limiti consentiti dalle procedure/regolamenti dell'ente, i siti web spesso nascondono insidie per i visitatori meno esperti;**
- **Non leggere le caselle personali esterne via webmail, in quanto i provider esterni potrebbero non proteggere dai virus;**
- **Evitare l'iscrizione a gruppi o altro di cui non si conosce l'affidabilità della sorgente.**

5.3 - Utilizzo di servizi di produttività personale in Cloud

L'utilizzo di servizi in Cloud con particolare riferimento a quelli di utilità personale (agenda, contatti, repository di cartelle e file, ecc..), non regolati da uno specifico contratto fra l'ente e il fornitore dei servizi de quibus (tipicamente quelli gratuiti, es. Gdrive, Drop Box, ecc.) sono da evitare e sono vietati se il loro uso coinvolge dati personali oggetto di trattamento aziendale. Nel caso di impellenti necessità o in caso di non disponibilità di altri strumenti idonei, occorre coinvolgere nell'utilizzo di questi strumenti il Servizio Informatico/Amministratore di sistema nonché il DPO.

5.4 - Come comportarsi in caso di violazioni di sicurezza

In caso di eventi relativi a possibili violazioni di dati personali o di incidente di sicurezza (c.d. *"Data Breach"*), costituiti a titolo esemplificativo da: distruzione di dati digitali o documenti cartacei, perdita di dati conseguente a smarrimento/furto di supporti o di documentazione, rilevamento di modifica non autorizzata di dati, divulgazione di dati e documenti a soggetti terzi non legittimati, accesso non autorizzato a sistemi IT ecc…, occorre informare prontamente il proprio diretto superiore gerarchico e coinvolgere il Servizio Informatico/Amministratore di sistema nonché il DPO, al fine dell'attuazione degli adempimenti previsti in applicazione delle disposizioni di legge. **Per maggiori dettagli si rinvia all'apposita procedura operativa aziendale.**

6 - Osservanza delle disposizioni in materia di protezione dati personali

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

Il mancato rispetto o la violazione delle regole contenute nelle presenti istruzioni è perseguibile con appositi provvedimenti disciplinari nonché con eventuali ed ulteriori azioni civili e penali consentite dalle norme vigenti ed in materia applicabili.

7 - Aggiornamento e revisione

Tutti gli utenti possono proporre - qualora ritenuto necessario - apposite integrazioni o modifiche da apportare alle presenti istruzioni. Le proposte verranno esaminate dal personale specificamente competente in materia ed eventualmente accolte.

La presente procedura è soggetta a periodica revisione con frequenza annuale.

Palermo, lì 20.01.2022

Allegato 1 - ***"Schema Avvertenza Privacy"***

Avvertenze Privacy:

<<Il presente indirizzo di posta elettronica è di natura aziendale ed utilizzabile solo per le finalità istituzionali dell'ente.

I messaggi, pertanto, potranno essere oggetto di consultazione da parte di tutte le funzioni aziendali competenti.

Le informazioni trasmesse attraverso la presente e-mail ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con conseguente divieto di diffusione e/o di uso non conforme alle finalità per le quali la presente e-mail è stata inviata, salva espressa autorizzazione. Pertanto, qualunque utilizzazione, divulgazione o copia non autorizzata di questa comunicazione è rigorosamente vietata e comporta violazione delle disposizioni di Legge sulla tutela dei dati personali di cui al REGOLAMENTO EUROPEO 2016/679 e alla normativa nazionale all'uopo vigente ed applicabile.

Se la presente e-mail ed i suoi allegati sono stati ricevuti per errore, siete pregati di distruggere quanto ricevuto e di informare il mittente con lo stesso mezzo.

Grazie per la collaborazione.>>

Allegato 2 – *"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.

In tal senso, si dovrebbero considerare le seguenti linee guida:

- stabilire una politica formale che proibisca l'uso di software non autorizzato;
- attuare controlli che prevengano o individuino l'uso di software non autorizzato (per esempio whitelisting delle applicazioni);
- attuare controlli che prevengano o individuino l'uso di siti web malevoli conosciuti (per esempio blacklisting);
- 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;
- ridurre le vulnerabilità che potrebbero essere sfruttate dal malware, per esempio attraverso la gestione delle vulnerabilità tecniche;
- condurre riesami regolari del software e dei dati contenuti nei sistemi a supporto dei processi critici di gestione; la presenza di file non approvati o di aggiunte non autorizzate dovrebbe essere oggetto di indagini formali;
- 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:
    a) 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;
    b) 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;
    c) una scansione delle pagine web alla ricerca di malware;
- 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;
- 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;
- 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;
- isolare gli ambienti in cui si potrebbero concretizzare impatti catastrofici.

Allegato 3 – *"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 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 e l'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. In particolare:

- 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 (inventario asset); queste risorse informative dovrebbero essere aggiornate in base a cambiamenti nell'inventario o quando sono trovate altre risorse nuove o utili;
- dovrebbe essere definita una scala temporale per reagire alle notifiche di vulnerabilità tecniche potenzialmente pertinenti;
- 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;
- in ordine al grado d'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 o seguendo le procedure di risposta agli incidenti relativi alla sicurezza delle informazioni;
- 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;
- 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:
    a) la disattivazione dei servizi o delle funzionalità legate alla vulnerabilità;
    b) l'adattamento o l'adozione di controlli di accesso aggiuntivi, ad esempio firewall ai confini della rete;
    c) l'aumento del monitoraggio per l'individuazione di attacchi in corso;
    d) l'aumento della consapevolezza sulla vulnerabilità.
- dovrebbe essere mantenuto un log di audit di tutte le procedure intraprese per il processo di gestione delle vulnerabilità tecniche e, ciò, dovrebbe essere monitorato e valutato regolarmente per assicurare la sua efficacia ed efficienza;
- 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;
- 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.