Comune di San Giuseppe Vesuviano

Servizio Demografico e Sistemi Informativi

LE POLITICHE ADOTTATE DALL'ENTE

ISTRUZIONI PER GLI AUTORIZZATI AL TRATTAMENTO

AVVERTENZA

Tali politiche contengono le regole pratiche/istruzioni per garantire un trattamento di dati personali sicuro e conforme alle norme del Regolamento UE oltre che ai procedimenti di sicurezza ISO 27001, sono parte della formazione di tutto il personale. Il presente fascicolo quindi, va messo a disposizione del personale

1. POLITICA PROTEZIONE DEI DATI

Questa politica descrive come questi dati personali devono essere raccolti, gestiti e archiviati per soddisfare gli standard di protezione dei dati delineati dal Regolamento EU 679/2016 (GDPR).

SCOPO

Questa politica di protezione dei dati garantisce che l'organizzazione:

- Sia conforme alla legge sulla protezione dei dati e seguire le buone pratiche.
- Protegga i diritti di personale e terzi.
- Sia trasparente su come memorizza ed elabora i dati degli individui.
- Si protegga dai rischi di una violazione dei dati.

CAMPO DI APPLICAZIONE

Questa politica si applica ai dipendenti, collaboratori, consulenti, lavoratori temporanei, incluso tutto il personale affiliato a terze parti e a tutte le attrezzature di proprietà o in leasing dell'organizzazione.

MODALITÀ OPERATIVE

Il Regolamento Ue 679/2016 (GDPR)

Il Regolamento Ue 679/2016 (GDPR) descrive come le organizzazioni, incluso il presente ente locale, devono raccogliere, gestire e archiviare le informazioni personali.
Queste regole si applicano indipendentemente dal fatto che i dati siano archiviati elettronicamente, su carta o su altri materiali.
Per rispettare la legge, le informazioni personali devono essere raccolte e utilizzate correttamente, conservate in modo sicuro e non divulgate illegalmente.
Il GDPR è sostenuto da otto importanti principi. Questi dicono che i dati personali devono:

1) essere trattati in modo equo e legale;
2) essere ottenuto solo per scopi specifici, leciti;
3) essere adeguati, pertinenti e non eccessivi;
4) essere precisi e aggiornati;
5) non essere trattenuto più a lungo del necessario;
6) elaborato conformemente ai diritti degli interessati;
7) essere protetti nei modi appropriati;
8) non essere trasferiti al di fuori dello Spazio economico europeo (SEE), a meno che tale paese o territorio garantisca anche un livello adeguato di protezione, ci sia una base contrattuale o sia state delineate delle BRC (Binding Corporate Rules).

Applicazione, rischi e responsabilità

Questa politica si applica all'organizzazione nel suo intero:

- La sede centrale

- Sedi distaccate
- Tutto organico e i volontari
- Tutti gli appaltatori, i fornitori e le altre persone che lavorano per conto dell'organizzazione

Si applica a tutti i dati che l'organizzazione detiene in relazione a persone identificabili. Ciò può includere:

- Nomi di individui
- Indirizzi postali
- Indirizzi email
- Numeri di telefono
- ... più qualsiasi altra informazione relativa alle persone

Rischi

Questa politica aiuta a proteggere l'organizzazione da alcuni rischi di sicurezza dei dati personali molto reali, tra cui:

- **Violazioni di riservatezza** (le informazioni vengono distribuite in modo inappropriato)
- **Danno reputazionale**

Responsabilità

- Il **Titolare di trattamento** è in ultima analisi responsabile di garantire che l'organizzazione soddisfi i propri obblighi legali.
- Il **Responsabile della protezione dei dati** (RPD) è responsabile di:
  - Mantenere il titolare di trattamento aggiornato sulle responsabilità, i rischi e le questioni relativi alla protezione dei dati.
  - Revisione di tutte le procedure di protezione dei dati e delle relative politiche, in linea con un programma concordato.
  - Organizzare formazione e consulenza sulla protezione dei dati per le persone coperte da questa politica.
  - Gestire le domande sulla protezione dei dati da parte del personale e di chiunque altro coperto da questa politica.
  - Gestire le richieste da parte di individui per vedere i dati che l'organizzazione tiene su di loro
  - Verifica e approvazione di eventuali contratti o accordi con terze parti che possano gestire i dati personali trattati dall'ente

Linee guida generali per il personale

- Le uniche persone in grado di accedere ai dati coperti da questa politica dovrebbero essere coloro **che ne hanno bisogno per il loro lavoro.**
- I dati **non devono essere condivisi in modo informale**. Quando è richiesto l'accesso ad informazioni condivise, i dipendenti devono richiederlo al Responsabile del Servizio.
- Lo scrivente ha già fornito **formazione a tutti** i dipendenti del Settore sia attraverso la Formazione a distanza e sia attraverso interventi formativi fatti nell'Ente, per aiutarli a comprendere le loro responsabilità nella gestione dei dati.
- I dipendenti devono mantenere tutti i dati personali al sicuro, adottando precauzioni e seguendo le linee guida seguenti.
- In particolare, è necessario **utilizzare password complesse, che non devono mai essere condivise**.
- I dati personali **non devono essere divulgati** a persone non autorizzate, all'interno dell'ente o esternamente.
- I dati personali devono **essere rivisti e regolarmente aggiornati** se si ritiene che non siano aggiornati. Se non sono più necessari, devono essere eliminato e eliminato.

Conservazione dei dati

Queste regole descrivono come e dove i dati devono essere archiviati in modo sicuro. Le domande sulla memorizzazione sicura dei dati possono essere indirizzate al **Responsabile dei Sistemi Informativi**.
Quando i dati personali sono **archiviati su carta** devono essere conservati in un luogo sicuro dove le persone non autorizzate non possono vederli.
Queste linee guida si applicano anche ai dati che vengono solitamente archiviati elettronicamente ma per qualche motivo sono stati stampati:

- Se non richiesto, la carta o i file devono essere conservati in **un cassetto o in uno schedario chiuso a chiave**.
- I dipendenti devono assicurarsi che la carta e le stampe **non vengano lasciate dove persone non autorizzate potrebbero vederle**, come in una stampante.
- **Le stampe dei dati devono essere triturate e smaltite** in modo sicuro quando non sono più necessarie.

Quando i dati personali sono **archiviati elettronicamente**, devono essere protetti da accessi non autorizzati, cancellazioni accidentali e tentativi di Hacking illecito:

- I dati devono essere **protetti da password complesse** che vengono cambiate regolarmente e mai condivise tra dipendenti.
- I dati non devono essere **archiviati su un supporto rimovibile** (come un CD o un DVD o PEN Drive).
- I dati, ivi comprese le e-mail/PEC contenenti dati personali/particolari devono essere **memorizzati solo su unità e server designati (ad esempio il Server interno Primario)** e devono essere caricati solo su **servizi di cloud computing approvati (in tale ipotesi sarà cura del Responsabile del Servizio Sistemi Informativi a farne comunicazione).**
- I dati non devono **mai essere salvati direttamente su laptop o altri dispositivi mobili** come tablet o smartphone.

Utilizzo dei dati

- Quando si lavora con dati personali, i dipendenti devono assicurarsi **che gli schermi dei loro computer siano sempre bloccati quando lasciati incustoditi.**
- I dati personali **non devono essere condivisi in modo informale**. In particolare, non devono mai essere inviati via e-mail, in quanto questa forma di comunicazione non è sicura.
- I dati **devono essere crittografati prima di essere trasferiti elettronicamente**. I dipendenti del Servizio Sistemi Informativi possono spiegare come inviare dati a contatti esterni autorizzati. Si allegano le istruzioni per il criptaggio attraverso il software IZARC presente su tutte le postazioni.
- Le **chiavi di decodifica** dei file criptati devono essere trasmessi sempre su canale diverso rispetto a quelli dove vengono trasmessi i file criptati.
- I dati personali **non devono mai essere trasferiti al di fuori dello Spazio economico europeo**, senza seguire la corretta procedura.
- I dipendenti **non devono salvare copie di dati personali sui propri computer**. Sempre accedere e aggiornare la copia centrale di tutti i dati.
- I dipendenti **devono utilizzare la webmail e non scaricare la posta elettronica contenente dati personali sul PC**. Qualora la si scarichi, devono avere cura di salvare le e-mail sulla propria cartella presente sul Server e quindi di cancellare la posta scaricata.

Accuratezza dei dati

La legge richiede che l'organizzazione adotti misure ragionevoli per garantire che i dati siano mantenuti accurati e aggiornati.
Più importante è il fatto che i dati personali siano accurati, maggiore è lo sforzo che l'organizzazione dovrebbe compiere per garantirne l'accuratezza.
È responsabilità di tutti i dipendenti che lavorano con dati personali adottare misure ragionevoli per garantire che siano mantenuti il più precisi e aggiornati possibile.

- I dati verranno **conservati solo in posti assolutamente necessari**. Il personale non deve creare set di dati aggiuntivi non necessari;
- I dati devono essere **aggiornati quando vengono scoperte inesattezze**.

Per realizzare la protezione dei dati personali ci si avvale anche delle seguenti ulteriori politiche:

- politica della password;
- politica del backup;
- politica clear desk - clear screen.

2. POLITICA DELLA PASSWORD

SCOPO

Tutti i dipendenti ed il personale che ha accesso ai computer dell'organizzazione devono rispettare i criteri di password definiti nella seguente politica, al fine di proteggere

- la sicurezza della rete
- l'integrità dei dati
- i sistemi informatici.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutte le persone che hanno un account che richiede una password su un computer collegato alla rete. (Es. account di dominio etc.).

MODALITÀ OPERATIVE

Questa politica è stata definita per proteggere le risorse organizzative della rete mediante la richiesta di password complesse unitamente alla protezione di queste password e nello stabilire un tempo minimo tra le modifiche delle password.

Protezione della Password

a) Non annotare mai la password.

b) Non inviare mai una password tramite e-mail.

c) Non includere una password nel documento archiviato non-crittografato.

d) Non dire mai a nessuno la tua password.

e) Non rivelare la tua password al telefono.

f) Non accennare mai al formato della password.

g) Non rivelare o suggerire la tua password in un modulo in internet.

h) Non utilizzare mai l'opzione "ricorda password", di programmi come internet explorer, di posta elettronica, o qualsiasi altro programma.

i) Non utilizzare mai la password personale o di rete per un account internet, che non dispone di un accesso protetto (dove l'indirizzo browser web inizia con https:// invece di http:/).

j) Se qualcuno ti chiede la password, indirizzali al reparto/incaricato della sicurezza.

k) Non usare acronimi comuni come parte della password.

l) Non usare parole comuni o invertire l'ortografia delle parole come parte della password.

m) Non utilizzare nomi di persone o luoghi, come parte della password.

n) Non utilizzare una parte del tuo nome utente per la tua password.

o) Non utilizzare parti di numeri facili da ricordare, come numeri di telefono, numeri di indirizzo o altro di similare.

p) Stare attenti a lasciare che qualcuno veda la digitazione della password.

Requisiti di Password (soggetto a variazioni)

Coloro che fissano i requisiti di password devono ricordare che rendere queste regole troppo difficili può effettivamente diminuire la sicurezza: gli utenti possono decidere che sono impossibili da soddisfare o, se le password sono cambiate troppo spesso, gli utenti tendono ad annotarle o rendere la loro nuova password una variante di una vecchia, cosa che la renderebbe più vulnerabile ad un attacco. I seguenti requisiti di password verranno impostati a livello di dominio ovvero fanno riferimento alle credenziali di accesso al PC. Si raccomanda di utilizzare i seguenti criteri anche per i software di gestione in uso presso i Servizi Demografici e Sistemi Informativi.

- Lunghezza Minima → 8 caratteri
- Minimo livello di complessità → Nessuna parola del dizionario. Ciascuna password deve includere tre o quattro dei seguenti tipi di caratteri:
  - Minuscole
  - Maiuscole
  - Numeri
  - caratteri Speciali, ad esempio !@#$%^&*(){}[]
- le Password differenziano tra maiuscole e minuscole, mentre il nome utente o l'ID di accesso no.
- Ripetizione Password → numero min. di password prima che una vecchia password possa essere riutilizzata: questo numero non deve essere inferiore a 10;
- Validità Massima password → 90 giorni.
- Uno Screen saver protetto da Password dovrebbe essere attivato e dovrebbe proteggere il computer entro 10 minuti di inattività dell'utente. Il computer non dovrebbe essere lasciato incustodito mentre è connesso (logged-on) e senza aver attivato uno screen saver protetto da password. Gli utenti dovrebbero avere l'abitudine di non lasciare i loro computer sbloccati; per facilitarne il compito si può impostare una combinazione rapida di tasti (es. CTRL-ALT-CANC e selezionare "Blocca Computer").

Per le credenziali di accesso al PC sono previsti anche ulteriori criteri ovvero:

- Validità Minima password → 1 giorni.
- Soglia di blocco degli Account → 5 tentativi di login falliti.
- Reset blocco account → Il tempo che intercorre tra tentativi di accesso non valido e la possibilità

di ritentare: il valore raccomandato è di 20 minuti. Questo significa che se ci sono 5 tentativi non validi in 20 minuti, l'account verrà bloccato.

Scelta della Password

In primo luogo bisogna essere sicuri che la password soddisfi i requisiti minimi delle linee guida sopra citate, di seguito sono elencati alcuni suggerimenti per la creazione di una nuova password:

- Incorpora una parola o parte di una parola all'interno di un altra. ***Es.*** Mare + sabbia. Password: "Marebbia".
- Sbaglia volontariamente l'ortografia di una parola, soprattutto se si usa una sola parola come parte della vostra password. ***Es.*** Cioccolato. Password: "Ciocolatto".
- Utilizzare una frase che è personale e usa il primo, il secondo o il terzo carattere di ogni parola nella frase. Ci possono essere diverse varianti di questo approccio:
  - Utilizzare una frase che ha un numero alla fine.
    Es. Il mio numero preferito è 333. Password: "IMNPE333"
  - Dopo la creazione della password, combinare i numeri e caratteri in modo che da poterli ricordare.
    Es. Quanto darò oggi? Il 100%. Password: "qdo?I100%"
  - Usa lettere maiuscole e lettere minuscole in modo insolito.
    Es. Non rimandare a domani ciò che puoi fare oggi! Password: "NraDccpfO!"
  - Utilizzare una rappresentazione numerica delle lettere dell'alfabeto per parte della frase o parte di una parola. Per esempio A è 1, B 2, C 3, etc.
    Es. Il nome di mia nonna è Gina. Password: "IndMnè79121".
  - Utilizzare i segni di punteggiatura o caratteri speciali.
    Es. Preferisci mare o montagna? Mare. Password: "Pm/m?111165"
  - In molti di esempi sopra citato, è facile inserire punteggiatura come "?" quando parte della vostra frase è una domanda. Se la tua frase coinvolge numeri $, %, # può essere di facilitarne l'uso. Se la tua frase si usa la parola "e" o "o", è possibile sostituire "&" o "|". Inoltre, è possibile dividere le vostre password con "/" o "\".

3. POLITICA DEL BACKUP

SCOPO

Questa politica definisce i criteri di backup per i computer all'interno dell'Ente che necessitano del backup dei dati. Questi sistemi sono in genere i server (file server, server di posta e il server web) ma non sono necessariamente limitati a questi.
Questa politica ha il fine di proteggere i dati dell'organizzazione garantendo che non vadano persi e possano essere recuperati in caso di un guasto delle apparecchiature, una distruzione di dati intenzionale, o un'emergenza.

CAMPO DI APPLICAZIONE

Questa politica si applica al salvataggio dei server virtuali presenti nel data center.

MODALITÀ OPERATIVE

Definizioni

Backup → Il salvataggio di file su supporto di memorizzazione off-line (disconnesso dalla rete) con lo scopo di prevenire la perdita dei dati in caso di guasto o distruzione delle apparecchiature.

Archivio → Il salvataggio di vecchi o inutilizzati file off-line al fine di catalogarli e alleggerire il sistema.

Ripristina → Il processo di riportare dati conservati off-line, in un sistema di archiviazione online come un file server.

Tempi

Attualmente sono attive 10 istanze virtuali che vengono eseguite sul cluster di server VMWARE. Di seguito l'elenco della varie istanze con indicazione del dispositivo/spazio utilizzato per la copia/replica.

	NAS2-Rack-A (Sito A)	NAS3-Rack-B (Sito B)	Cloud
Archiviazione ottica	✓	✓	
Server applicativi	✓	✓	✓
Server PBX Report	✓	✓	
Server Primario	✓	✓	✓
Server Update	✓	✓	

SrvAppProtocollo	✓	✓	✓
SrvBDMS	✓	✓	✓
SrvDemografici	✓	✓	✓
SrvFrontEnd	✓	✓	✓
SrvIMS-Alfresco	✓	✓	✓

Nello spazio cloud vengono effettuati i backup solo dei sistemi principali.

Le operazioni di backup vengono eseguite in automatico secondo il seguente schema

- Copie giornaliere
  - Backup primario verso NAS3-Rack-B (Sito B):
    - tra le 20:00 e le 00:00
    - 10 VM come da tabella precedente
    - Punti di ripristino: 8
  - Backup in Cloud:
    - A partire dalle 3:00
    - 7 VM come da tabella precedente
    - Punti di ripristino: 3

- Copie settimanali
  - Backup verso NAS1-Rack-C (Sito A):
    - A partire dalle 4:00 di ogni domenica
    - 7 VM come da tabella precedente
    - Punti d ripristino: 4

- Copie mensili
  - Backup verso NAS2-Rack-A (Sito A):
    - Ogni 28 giorni a partire dalle 5:00
    - 10 VM come da tabella precedente
    - Punti di ripristino: 2

Responsabilità

Il backup dei server centralizzati è a cura del Servizio Demografico e Sistemi Informativi

Test

La capacità di ripristinare i dati dal backup viene eseguito periodicamente

Dati di Backup

	NAS2-Rack-A (Sito A)	NAS3-Rack-B (Sito B)	Cloud
Archiviazione ottica	✓	✓	
Server applicativi	✓	✓	✓
Server PBX Report	✓	✓	

Server Primario (contenente le cartelle condivise)	✓	✓	✓
Server Update	✓	✓	
SrvAppProtocollo	✓	✓	✓
SrvBDMS	✓	✓	✓
SrvDemografici	✓	✓	✓
SrvFrontEnd	✓	✓	✓
SrvIMS-Alfresco	✓	✓	✓

Ripristino

Gli Utenti che hanno bisogno di file ripristinati, devono presentare una richiesta al Servizio Demografico e Sistemi Informativi, includendo informazioni circa la data di creazione del file, il nome del file, l'ultima volta che è stato cambiato, e la data e l'ora in cui è stato cancellato o distrutto.

4. POLITICA CLEAR DESK / CLEAR SCREEN

SCOPO

Per migliorare la sicurezza e la riservatezza delle informazioni, l'organizzazione ha adottato una politica "clear desk" (scrivania pulita) per documenti e supporti di archiviazione rimovibili, ed una politica "clear screen" (schermo pulito) per gli strumenti di elaborazione delle informazioni.
Questo al fine di ridurre il rischio di accessi non autorizzati, perdita e danneggiamento di informazioni durante e al di fuori del normale orario di lavoro o quando le aree non sono presidiate.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutto il personale del Servizio Demografici e Sistemi Informativi.

MODALITÀ OPERATIVE

Clear Desk

- Ove possibile, carta e supporti informatici devono essere conservati in apposite casseforti, armadi o altre forme di protezione quando non sono in uso, soprattutto al di fuori dell'orario di lavoro.
- Le porte delle aree di uffici devono essere chiuse a chiave quando non sono in uso o non sono vigilate.
- Informazioni riservate, sensibili o classificate, una volta stampate, devono essere rimosse immediatamente dalle stampanti. Ove possibile, devono essere utilizzate le stampanti con l'opzione di inserimento password per la protezione dei documenti.
- Utilizzare appositi cestini di sicurezza per eliminare fogli con informazioni sensibili o personali

di cui non si ha più bisogno.

- Notare che le informazioni lasciate sulla scrivania hanno più probabilità di essere danneggiate o distrutte in una situazione di emergenza come incendi, inondazioni o esplosioni.
- Non stampare le email per leggerle: aumenta soltanto la quantità di disordine.
- Le scrivanie degli uffici aperti al pubblico, possono essere particolarmente vulnerabili ai visitatori. Questa zona deve essere mantenuta il più "pulita" possibile in ogni momento; in particolare, le informazioni personali non devono essere alla portata/vista di chiunque possa accedere all'ufficio.
- Liberare sempre la scrivania prima di andare a casa.

Clear Screen

- Gli utenti devono SEMPRE "log-off"(disconnettersi), quando lasciato il computer incustodito.
- Impostare il Blocco schermo di Windows affinché si attivi automaticamente quando non vi è alcuna attività per un breve predeterminato periodo di tempo.
- Il Blocco schermo di Windows deve essere protetto da password per la riattivazione.
- Le password non devono essere annotate su/sotto al computer o in qualsiasi altra posizione accessibile.

Modalità di monitoraggio e revisione

Tutto il personale è responsabile nel monitorare il proprio rispetto dei principi/procedure descritti in questa politica. Questa politica sarà soggetta a revisione periodica durante il Riesame da parte del Titolare del trattamento o dal designato.
Una revisione eccezionale può essere giustificata se si verifica una delle seguenti situazioni:

- In base ai risultati/effetti di incidenti critici;
- Per ogni altra pertinente ragione.