SERVIZIO SANITARIO REGIONALE
BASILICATA
Azienda Sanitaria Locale di Potenza

# Procedure a supporto dello

# SMART WORKING

| Data | Preparato da | Note |
|---|---|---|
| *10.12.2020* | *Roberto Sibilani* | |

# Lista dei Contenuti

# 1 Definizioni e Acronimi

| | |
|---|---|
| Smart Working | Filosofia manageriale fondata sulla restituzione alle persone di flessibilità e autonomia nella scelta degli spazi, degli orari e degli strumenti da utilizzare a fronte di una maggiore responsabilizzazione sui risultati |
| Credenziali di dominio | Coppia di nome utente e password utilizzata per accedere al computer aziendale, alla posta elettronica, all'anagrafe sanitaria, al cloud aziendale e ad altri servizi. Il nome utente può essere espresso in tre formati:<br>• nome.cognome<br>• nome.cognome@asp.int<br>• ASP\nome.cognome |
| VPN | Una rete sicura che permette di utilizzare le procedure aziendali anche sul proprio computer di casa. Per utilizzarla bisognerà essere in possesso di credenziali regionali |
| SIA | U.O.C. Sistemi Informativi Aziendali |

## 2 Premessa

Questo documento si prefigge di semplificare e far comprendere ai dipendenti come utilizzare gli strumenti messi a disposizione dai Sistemi Informativi Aziendali dal solo punto di vista tecnico e non vuole sostituirsi alla documentazione ufficiale pubblicata dall'Azienda Sanitaria di Potenza attraverso i canali istituzionali.

Prima di utilizzare tali strumenti bisogna seguire la procedura di attivazione dello Smart Working come previsto dalla Direzione Strategica aziendale.

Nel documento vengono descritti diversi strumenti:

- La VPN aziendale: per connettersi dall'esterno alle procedure in uso
- Il Cloud aziendale: per conservare i documenti aziendali e per scambiarli con altri membri della U.O.
- Assistenza remota: per consentire attività di assistenza, da parte del personale autorizzato, alla U.O.C. SIA

## 3 Raccomandazioni

1. Bisogna tener presente che il proprio computer deve essere dotato di:
   a) Sistema operativo aggiornato (Windows 7 o Windows 10)
   b) Software di base (Microsoft Office, Libre Office) aggiornato
   c) Antivirus installato ed aggiornato
   d) Sistema di assistenza remota scaricabile dal sito aziendale
      https://get.teamviewer.com/aspbasilicata

2. L'invio di documenti o dati mediante posta elettronica deve sempre essere effettuato con le dovute cautele, quali accertarsi che il destinatario sia autorizzato a trattare i dati inviati, che l'indirizzo sia corretto, che il destinatario riceva correttamente i documenti inviati (ad es. mediante conferma di lettura)

3. Utilizzare le risorse aziendali in maniera oculata e professionale tenendo presente che verranno tracciati tutti gli accessi alla rete e ai PC aziendali, attraverso strumenti elettronici e automatici, dei quali verranno mantenuti in file di log per 60 giorni

# 4 Passi per attivare lo Smart Working

1. Il **Dirigente** attiva la modalità Smart Working per il dipendente seguendo le direttive aziendali, pubblicizzate sul sito aziendale
   http://www.aspbasilicata.it/infosalute/misure-di-contenimento-diffusione-covid-19-disposizioni-temporanee-del-direttore-generale
2. Il **Dirigente**, nel solo caso in cui verifichi che per svolgere le sue mansioni il dipendente dovrà utilizzare una o più procedure aziendali (C4H, Gupar, Anagrafe ecc.), dovrà inviare i due moduli specificati alle successive lettere a. e b. all'indirizzo mail sia@aspbasilicata.it:
   a. *Modulo richiesta credenziali per l'accesso al sistema informatico tramite VPN SSL (allegato a pag. 12)*
      Compilazione e firma a cura **del Dirigente** che dovrà inserire:
      - Nome e cognome
      - Luogo e data di nascita
      - Ufficio di cui si è responsabili (UOC, UOSD, UOS)
      - Telefono
      - Matricola aziendale

      Questo modulo dovrà essere inviato in formato PDF in un file denominato "Autorizzazione Dirigente".
   b. *Modulo richiesta accesso al sistema informatico (allegato a pag.19)*
      Compilazione e firma a cura **del Dipendente** che dovrà inserire:
      - Nome e cognome
      - Matricola
      - Utilizzo: procedure da utilizzare (Protocollo, C4H, Anagrafe, CUP, ecc.)
      - Indirizzo IP: se il dipendente dovrà raggiungere il proprio computer aziendale anche dall'esterno bisognerà inserire il suo indirizzo IP. Per tale attivazione bisognerà consultare preventivamente il proprio referente informatico che ne valuterà la necessità

      Questo modulo dovrà essere inviato in formato PDF in un file denominato "Richiesta VPN – Nome Cognome". Per esempio "Richiesta VPN – Mario Rossi".

   Il SIA, nei tempi previsti dall'ufficio, invierà le credenziali, via mail, direttamente al dipendente che potrà quindi utilizzarle (Vedi capitolo 5). L'utilizzo di tale strumento implica l'accettazione delle "Istruzioni operative Smart Working" e della "Informativa privacy Smart Working" disponibili sul sito aziendale, nell'area dedicata situata nella pagina "Area dipendenti".

# 5 La VPN aziendale

Una volta ricevuta la mail di avvenuta attivazione sarà possibile utilizzarle in due modi.

## 5.1 Utilizzo tramite un Browser

Questa modalità ben si adatta alla maggior parte degli utilizzi:

- Contabilità C4H
- Gupar Web
- Anagrafe Sanitaria
- Atti Digitali (solo se si intende istruire determine o delibere ed inoltrarle senza firma digitale)
- Cruscotto direzionale
- Giava
- Paghe Sigru
- Siste WEB

Richiede che il dipendente abbia installato sul proprio computer un browser. Assicurarsi quindi di aver disponibile uno dei browser come Chrome, Firefox, Internet Explorer o Edge.

Per utilizzare la VPN tramite un browser, solo dall'esterno della rete aziendale, seguire le istruzioni che seguono:

1. Aprire il browser (per esempio Chrome).
2. Inserire nella barra l'indirizzo https://vpn.aspbasilicata.it/
3. Inserire le proprie credenziali VPN, coincidenti con le credenziali della posta elettronica, e cliccare su "Login"
4. All'accesso troverete una serie di bottoni "Your Bookmark". Basterà cliccarci sopra per accedere alle procedure di cui si è fatta richiesta. Se non presenti seguire le istruzioni disponibili al capitolo 8

## 5.2 Utilizzare FortiClient

Questa modalità permette di collegare il proprio computer alla rete aziendale simulando una connessione diretta alla rete.

L'utilizzo di questa modalità richiede conoscenze medie/avanzate il cui scopo è quello di permettere la firma digitale di Deliberazioni e Determinazioni, avendo collegata la propria penna USB al proprio computer.

Dopo aver installato "FortiClient VPN", liberamente scaricabile su Internet, chiedere l'autorizzazione al SIA per collegarsi ad un computer remoto per utilizzare le procedure "Atti Digitali". Di seguito un esempio di configurazione.


## 6 L'assistenza remota

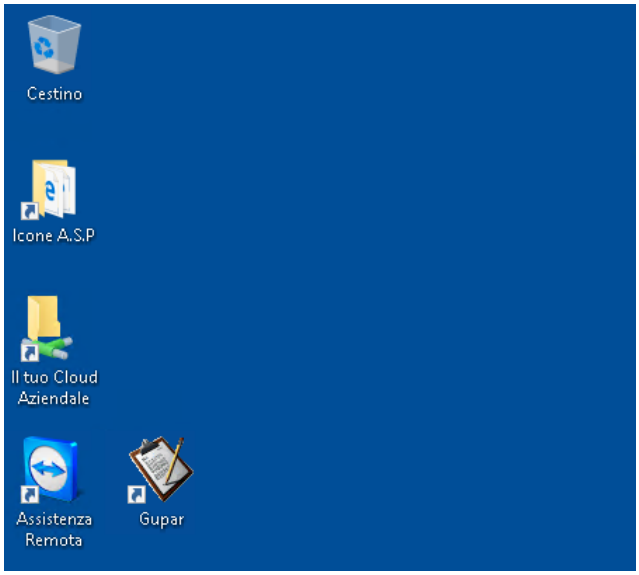
Per richiedere assitenza, bisogna far riferimento sempre ai propri referenti di ambito che si collegheranno da remoto o daranno istruzioni telefonicamente.
Per permettere il collegamento da remoto bisogna scaricare il software TeamViewer sul proprio computer:

1. Utilizzando un comune browser scaricare dall'area dipendenti, sul sito Aziendale, il software di Assistenza Remota e salvarlo sul desktop del proprio computer
   https://get.teamviewer.com/aspbasilicata

2. Eseguire lo strumento quando il proprio referente di ambito lo chiederà, al fine di assistere l'utente nei suoi compiti istituzionali

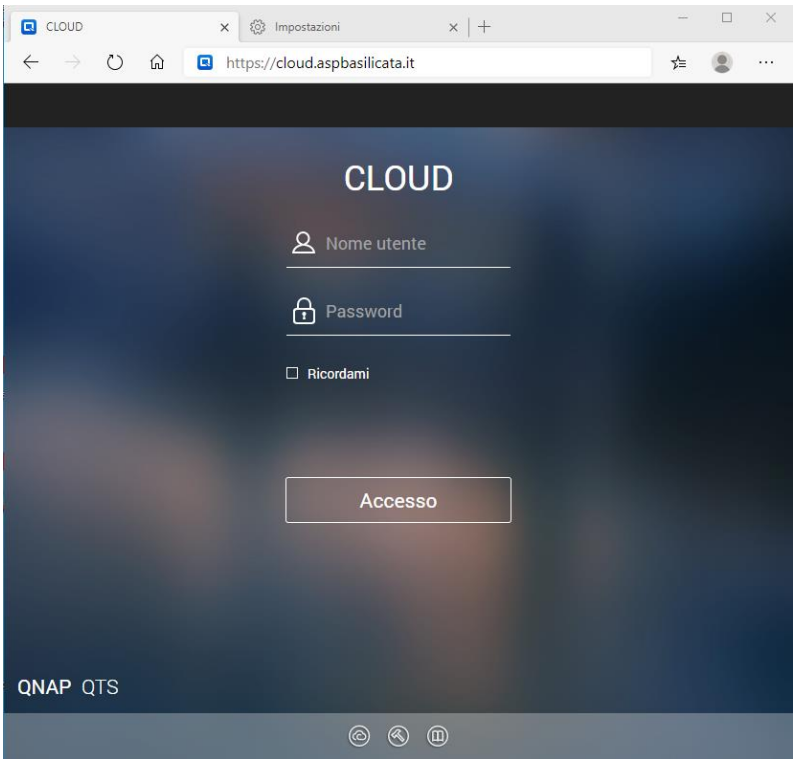
# 7 Il Cloud aziendale

Sul desktop del nostro computer aziendale, solo se in dominio, è presente una cartella “Il tuo Cloud Aziendale”

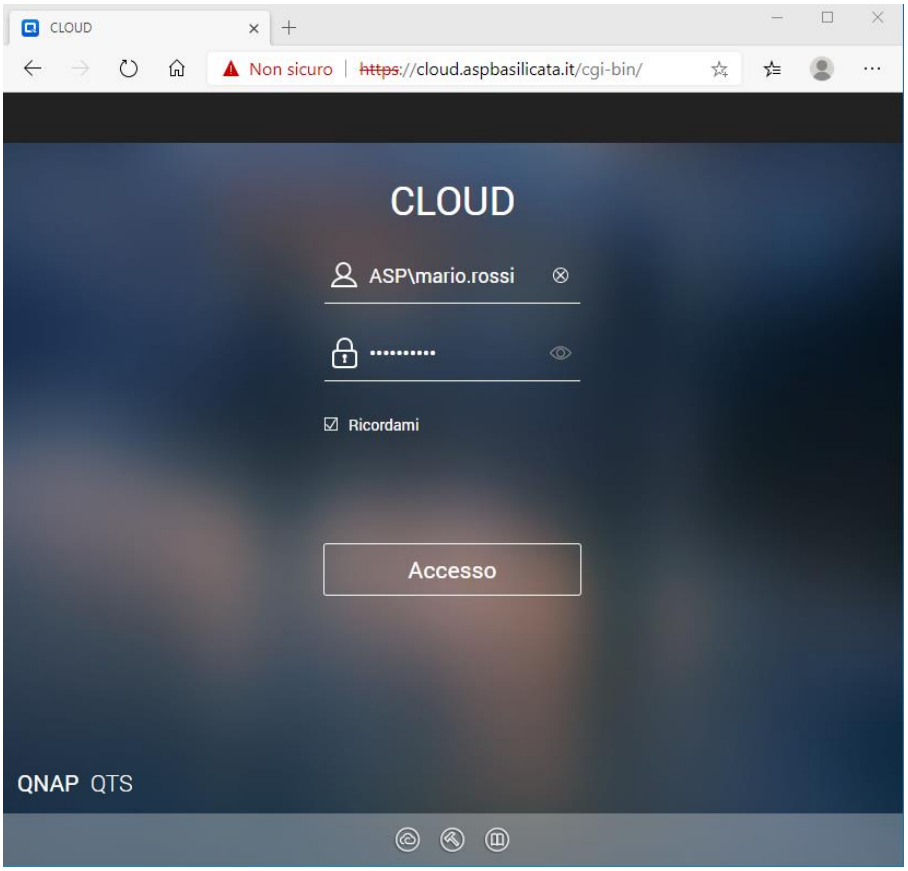



Tutto quello che mettiamo in questa cartella è visibile su tutti i computer aziendali, ovunque faremo il login con le nostre credenziali.
L’accesso a questa cartella è possibile anche dall’esterno della rete aziendale, attraverso l’utilizzo di un comune browser (Chrome, Firefox, Internet Explorer, Edge, ecc.).
Oltre a questa cartella, avremo accesso anche ad altre cartelle condivise, per esempio quella condivisa con tutti gli utenti della nostra unità operativa (se il dirigente ne ha fatto esplicita richiesta).
Per accedere, seguire le istruzioni che seguono:

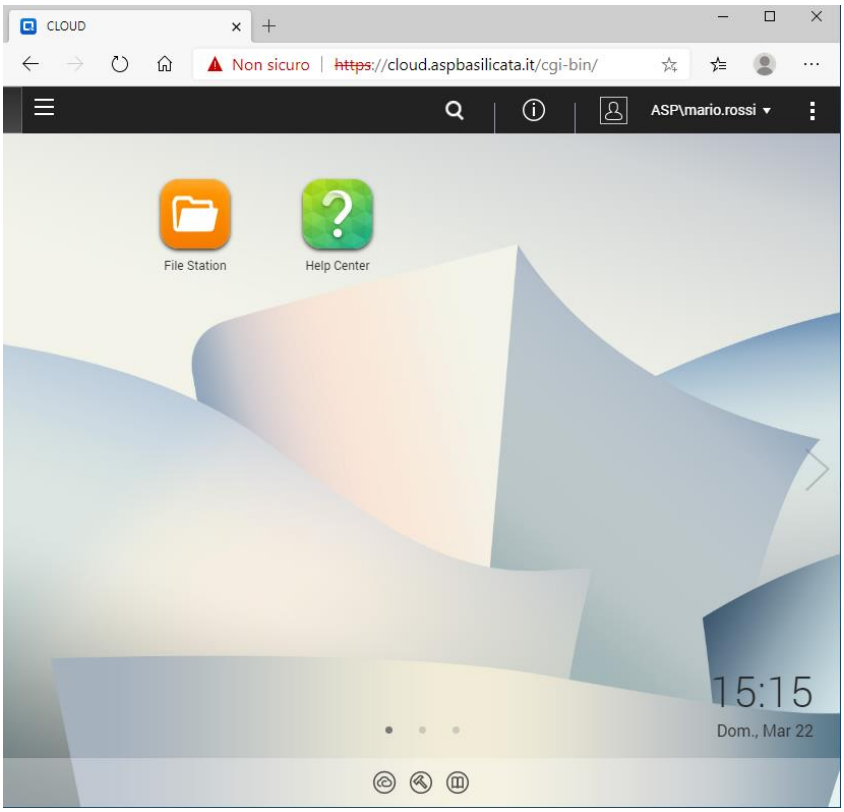
1. Aprire un browser (Chrome, Internet Explorer, ecc.)
2. Nella barra degli indirizzi inserire https://cloud.aspbasilicata.it/



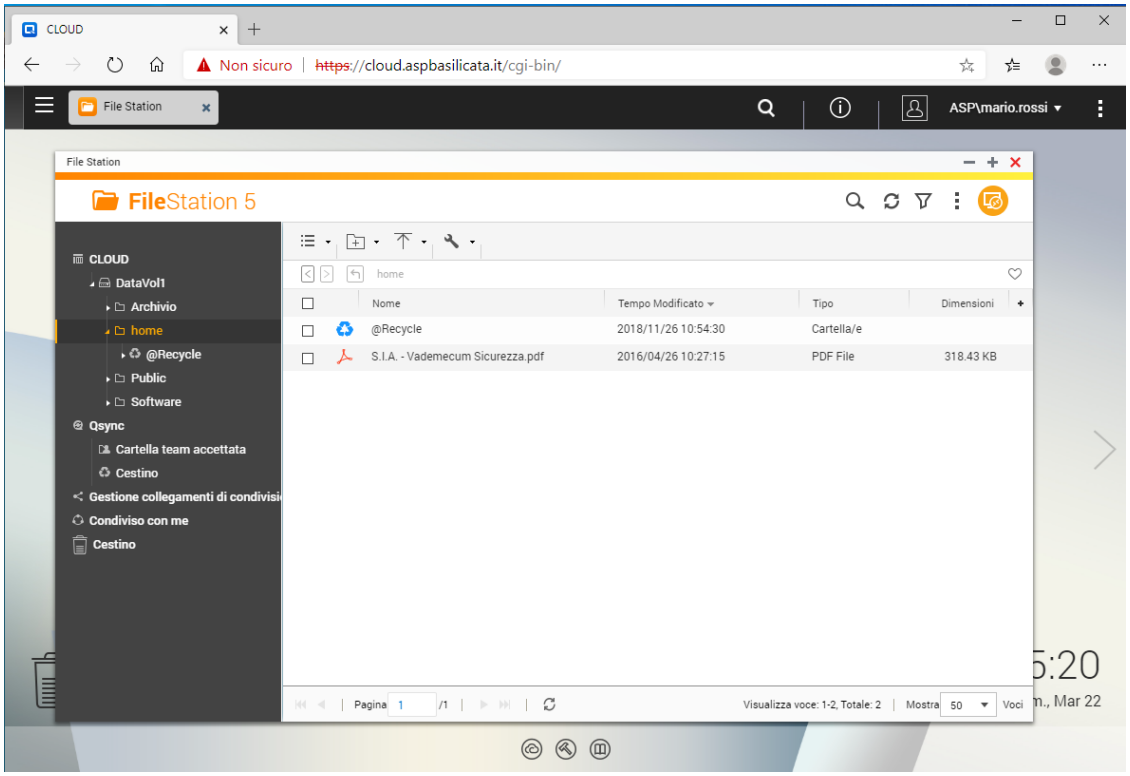

3. Inserire le proprie credenziali di dominio nel formato *ASP\nome.cognome* e la password




4. Dopo aver effettuato il login ci troveremo davanti alla pagina HOME




5. Cliccando adesso sull'icona "File Station" verranno mostrate, sulla sinistra, tutte le cartelle a cui si ha accesso, dove la cartella "home" corrisponde alla cartella "Il tuo Cloud Aziendale" presente sul nostro Desktop in ufficio




6. All'indirizzo che segue viene mostrato, brevemente, come si usa questo strumento

https://docs.qnap.com/nas/4.3/cat1/it/index.html?file_station.htm

# 8 Creare un Bookmark su FortiClient

Dopo aver fatto l'accesso alla VPN con il browser:

- Cliccare sul tasto "New Bookmark"


- Nella pagina risultante cliccare su "HTTP/HTTPS"
- Inserire le informazioni nei campi "Name" e "URL" e premere il tasto "Save". Di seguito le informazioni utili per le varie procedure:
    a. Anagrafe Sanitaria
        i. Name : Anagrafe Sanitaria
        ii. URL : http://172.16.252.96:8080/anagsani
    b. Amico (Ricetta dematerializzata)
        i. Name : Amico
        ii. URL : http://172.16.252.96:8080/amico
    c. Contabilità
        i. Name : Contabilità – C4H
        ii. URL : http://172.18.46.92/C4H_WebUI/
    d. Cruscotto Direzionale
        i. Name : Cruscotto Direzionale
        ii. URL : http://172.16.252.99:8080/cruscottoMonitoraggio
    e. Giava
        i. Name : Giava
        ii. URL : http://172.18.14.51/
    f. Gupar WEB
        i. Name : Gupar WEB
        ii. URL : http://protocollo.aspbasilicata.it/guparng/user/login
    g. Paghe SIGRU
        i. Name : Paghe - SIGRU
        ii. URL : http://172.16.252.14:8080/sigru/
    h. Siste WEB
        i. Name : Siste WEB
        ii. URL : http://172.16.252.85/SisteWEB

Nel caso in cui ci si voglia collegare al proprio PC in ufficio (autorizzati dal SIA), dopo aver cliccato su "New Bookmark" cliccare su "RDP" ed inserire i seguenti parametri, lasciando inalterati i rimanenti:

| | | |
|---|---|---|
| Name | : | Il mio PC |
| Host | : | L'indirizzo IP del PC in ufficio (se non lo si conosce chiedere al SIA) |
| Port | : | 3389 |
| Use SSL-VPN Credentials | : | Abilitato |
| Security | : | Network Level Authentication. |

Inutile dire che in questo caso il computer in ufficio DEVE essere sempre acceso e tale modalità è ammessa **SOLO** in casi eccezionali.

SERVIZIO SANITARIO REGIONALE
BASILICATA
Azienda Sanitaria Locale di Potenza

Spett.le U.O.C. Sistema Informativo Aziendale
Dott. Nicola Mazzeo
Via Torraca n.2
85100 – Potenza

E-mail: sia@aspbasilicata.it

OGGETTO: Richiesta credenziali VPN per l'accesso alla rete aziendale

Il/La sottoscritto/a_____ nato/a _____ il _____ , telefono_____ , matricola _____ in qualità di Dirigente dell'Ufficio _____

**CHIEDE**

il rilascio di credenziali ai soggetti presenti nelle n. _____ schede allegate da utilizzare per l'accesso tramite VPN alla rete aziendale e ai servizi in esse dichiarati. Inoltre

**DICHIARA**

1. Di aver preso visione, e di accettare in ogni sua parte quanto riportato:
   a. nell'informativa ai sensi dell'art. 13 del Regolamento (UE) 2016/679 (**Allegato 1**);
   b. nell'**Allegato 2** - Informazioni e Istruzioni agli autorizzati al trattamento dati personali fornite dal Titolare;
2. Di impegnarsi a comunicare tempestivamente ogni eventuale variazione di titolarità della funzione istituzionale che ha effetto sulla gestione della predetta richiesta.

Data _____

Il Dirigente

Non allegare alla richiesta

## ALLEGATO 1. Informativa ai sensi dell'articolo 13 del Regolamento (UE) 2016/679

Gentile utente,

ai sensi dell'art. 13 del Regolamento Generale Europeo per la protezione dei dati personali (GDPR) General Data Protection Regulation (UE) 2016/679, l'Azienda Sanitaria di Potenza, in qualità di "Titolare" del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali. Il trattamento dei dati acquisiti per lo svolgimento di funzioni istituzionali e nell'esecuzione dei propri compiti di interesse pubblico, o comunque connessi all'esercizio dei propri pubblici poteri da parte dell'Azienda Sanitaria di Potenza, è lecito ai sensi dell'art. 6 "Liceità del trattamento" e non necessita del suo consenso.

1. **Fonte dei dati personali**

La raccolta dei dati personali avviene con la registrazione delle informazioni fornite dall'interessato al momento della compilazione della modulistica per la presentazione dell'istanza per il rilascio dell'account di rete e/o posta elettronica dell'Azienda Sanitaria di Potenza. In particolare, i dati trattati sono i dati anagrafici e la matricola.

2. **Finalità del trattamento e base giuridica**

I dati personali sono trattati esclusivamente per le seguenti finalità:

- Richiesta credenziali per l'accesso al sistema informatico tramite VPN SSL

La base giuridica è il Codice dell'Amministrazione Digitale D.lgs. 82/2005.

3. **Modalità di trattamento dei dati**

In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi in conformità alle disposizioni previste dall'articolo 32 GDPR.

4. **Facoltatività del conferimento dei dati**

Il conferimento dei dati è facoltativo. In mancanza, non sarà possibile adempiere alle finalità descritte al punto 2.

5. **Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati**

I dati personali potranno essere conosciuti esclusivamente dai funzionari dell'Azienda Sanitaria di Potenza autorizzati e/o Incaricati del trattamento. Per le sole finalità previste al paragrafo 2 (Finalità del trattamento), possono venire a conoscenza dei dati personali società terze fornitrici di servizi per l'Azienda Sanitaria di Potenza, previa designazione di Responsabili esterni del trattamento, che garantiranno il medesimo livello di protezione. Alcune delle informazioni personali fornite all'Azienda Sanitaria di Potenza, nel rispetto della normativa di cui al D. Lgs. 33/2013, potranno essere pubblicizzate sul sito istituzionale dell'Ente.

6. **Trasferimento dati**

I dati personali saranno conservati su server (fisici o virtuali) aziendali allocati in sedi all'interno dell'Unione Europea. Ove necessario, il Titolare avrà facoltà di spostare tali server, che rimarranno, in ogni caso, dentro i confini dell'Unione.

7. **Diritti dell'Interessato**

L'interessato/a al trattamento dati potrà esercitare, nei confronti del Titolare del trattamento, i diritti di cui agli articoli 15, 16, 17, 18 del GDPR (Diritto di accesso; Diritto di rettifica; Diritto alla cancellazione; Diritto di limitazione di trattamento).

8. **Titolare e Responsabili del trattamento**

Il Titolare del trattamento dei dati personali di cui alla presente Informativa è l'Azienda
Sanitaria di Potenza, con sede in Potenza alla via F. Torraca n. 2, CAP 85100. Responsabile per il riscontro delle richieste, da parte degli interessati del trattamento, per esercitare i diritti descritti nel paragrafo precedente è il RPD aziendale. Tali istanze potranno essere presentate dagli interessati tramite Posta Elettronica (rpd@aspbasilicata.it ) o, in alternativa, recandosi direttamente presso gli sportelli Urp i cui riferimenti sono presenti sul sito istituzionale (www.aspbasilicata.it - sezione URP).

9. **Diritto di reclamo**

L'interessato, qualora ritenesse che il trattamento dei suoi dati personali avvenga in violazione di quanto previsto dal Regolamento Generale Europeo, ha il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

10. **Responsabile della protezione dati**

Il Responsabile della Protezione dei Dati (RPD), è raggiungibile al seguente indirizzo:
Via F. Torraca n. 2, 85100, Potenza (Email: rpd@aspbasilicata.it).

Non allegare alla richiesta

**ALLEGATO 2 . Informazioni e Istruzioni agli autorizzati al trattamento dati personali fornite dal Titolare**

A tal fine, vengono fornite **INFORMAZIONI ED ISTRUZIONI** alle quali attenersi per l'assolvimento del compito assegnato:

- trattare i dati personali, in base all'art. 5 del GPDR**, in modo lecito**, corretto e trasparente e dovranno essere: ○ raccolti per finalità implicite e legittime e successivamente trattati in modo che non vi sia incompatibilità con tali finalità;
  - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
  - esatti, e se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
  - conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
  - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate ("integrità e riservatezza");
- 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 (ex Sensibili) e non;
- **raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli 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;
- recepire nuove indicazioni fornite dal Titolare del Trattamento anche partecipando a percorsi formativi quando previsti;
- **assicurare la riservatezza** opportuna e necessaria affinché il trattamento dei dati, sia effettuato in conformità alle disposizioni del GDPR e del D.lgs 196/2003 s.m.i. e volte alla prevenzione da parte del Titolare dei crimini informatici e del trattamento illecito di dati;
- trattare i dati personali, eventualmente riferiti a categorie particolari (art. 9) o relativi a condanne penali e reati (art. 10) è ammesso se lecito (art. 6) e cioè quando:
- l'interessato ha espresso il consenso al trattamento dei propri dati personali;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo di legge cui è tenuto il Titolare o per salvaguardare gli interessi vitali dell'interessato;

- il trattamento è necessario per il perseguimento del legittimo interesse del Titolare;
- **garantire all'interessato l'esercizio dei diritti** sui propri dati secondo quanto previsto dal GDPR (es: diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.); **Inoltre:**
- **è consentita la trasmissione di dati all'interno dell'organico del Titolare** per i compiti ed i fini stabiliti dallo stesso, agendo sotto la sua diretta autorità, allo stesso modo sono autorizzati i trattamenti di dati pseudonimizzati;
- **È vietata ogni comunicazione/diffusione di dati verso l'esterno dell'Amministrazione senza preventiva autorizzazione del Titolare stesso o del Responsabile**; il divieto permane anche dopo la cessazione dell'incarico e/o del rapporto di lavoro;
- **nessun dato deve essere comunicato a soggetti identificati esterni all'Amministrazione o diffuso** (trasmesso a soggetti indeterminati), senza specifica autorizzazione del Responsabile del Trattamento; è vietata la diffusione dei dati trattati ed in particolare di quelli sensibili;
- sono consentite le comunicazioni di dati che avvengono nell'ambito di un rapporto contrattuale/convenzionale instaurato dall'Amministrazione con terzi per l'esternalizzazione di attività/funzioni/servizi, **a condizione che il terzo sia stato nominato Responsabile esterno del trattamento dei dati**;
- **l'incarico conferito autorizza l'accesso agli archivi contenenti atti e documenti** riportanti dati personali comuni e al trattamento di questi; l'accesso ed il trattamento dati vanno limitati alle necessità per l'adempimento dei compiti da assolvere;
- per il tempo necessario allo svolgimento delle operazioni di trattamento si **dovrà diligentemente controllare e custodire gli atti e documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati**;
- **astenersi** dall'effettuare operazioni di trattamento dei dati personali, di cui si a conoscenza durante lo svolgimento dell'incarico, evitare di conservarli, duplicarli, comunicarli o cederli ad altri, dopo la cessazione del rapporto di lavoro;
- **in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati**;
- informare tempestivamente il Responsabile del trattamento di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste pervenute dagli interessati;
- nel caso in cui si constati o si sospetti un disguido o **un incidente che abbia messo o possa mettere a repentaglio la sicurezza dei dati trattati, darne immediata comunicazione al Responsabile del trattamento**;
- segnalare al Responsabile eventuali circostanze, che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro una adeguata azione di controllo;
- **non trasmettere dati particolari (sensibili) via e-mail.** Nel caso in cui sia strettamente necessaria tale forma di trasmissione per ragioni d'ufficio,

occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;
- rispettare, se presente, il documento sulla sicurezza dei dati, predisposto dall'Amministrazione;
- **non alterare in alcun modo la configurazione software della stazione di lavoro**, evitando di installare qualunque software sconosciuto o non approvato;
- **non utilizzare la rete dell'Amministrazione per fini non espressamente autorizzati**;
- è vietato l'utilizzo improprio di documenti, dati, informazioni a qualsiasi titolo posseduti, ricevuti o trasmessi;

**Con riferimento alle misure di sicurezza, le PERSONE AUTORIZZATE AL TRATTAMENTO O INCARICATI:**
- accedono al sistema informativo per **mezzo di credenziali di autenticazione**; le credenziali di autenticazione consistono in un codice (user id o username) per l'identificazione dell'incaricato, associata ad una parola chiave (password) conosciuta solo dall'incaricato;
- utilizzano la **password con una lunghezza minima di otto caratteri, contenenti caratteri numerici, alfanumerici e almeno un carattere speciale** (o, se il programma in uso non lo permette, dal numero massimo di caratteri consentito);
- **nella generazione della password non utilizzano elementi o notizie a loro facilmente riconducibili;**
- **modificano la password** al primo utilizzo, ogni volta che viene richiesto dal sistema (al massimo 6 mesi, 3 mesi se i dati trattati sono sensibili (ad. es. di salute) e/o giudiziari) e nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;
- qualora il sistema non renda obbligatoria la modifica della password nel rispetto dei predetti termini, **l'utilizzatore provvede autonomamente a tale variazione**;
- adottano particolari cautele per assicurare la **segretezza della password** (evitare la digitazione in presenza di terzi, conservarne i riferimenti in luogo non accessibile a terzi);
- nel caso di allontanamento dalla propria postazione di lavoro, **l'incaricato adotta tutte le cautele necessarie atte ad evitare l'accesso ai dati personali trattati o in trattamento sia cartaceo che automatizzato da parte di terzi**, anche se dipendenti, a meno che non siano autorizzati;
- **non lasciano la propria stazione di lavoro incustodita e collegata con il proprio account (nome utente) e password all'ambiente di rete**;
- **bloccano la propria stazione di lavoro durante la pausa pranzo**, ovvero in tutte le occasioni in cui ci si assenti dall'ufficio; nel caso in cui fosse necessario mantenere accesa la stazione di lavoro, utilizzare i metodi messi a disposizione dal sistema per bloccare la stessa, come ad esempio il blocco sessione o il salvaschermo con password;
- per le banche dati automatizzate utilizzano il proprio codice di accesso personale, evitando di operare su terminali altrui e/o lasciare aperto il sistema

operativo con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

- **tenere un comportamento corretto durante la navigazione in internet**, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete.
- devono garantire sempre la **corretta custodia** degli stessi; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri incaricati addetti al medesimo trattamento; non devono essere consultati da altri incaricati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
- devono conservare i documenti o gli atti che contengono **dati particolari (ex sensibili e/o giudiziari) in archivi ad accesso controllato** (armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale preposto);
- al termine delle operazioni di trattamento, devono, restituire tempestivamente la documentazione prelevata dagli archivi;
- **in caso di utilizzo di stampante, fotocopiatrice o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola stazione di lavoro, le stampe devono essere immediatamente raccolte e custodite** con le modalità sopra descritte;
- **non devono gettare via copie cartacee contenenti dati personali, senza averle distrutte prima in modo opportuno**;
- devono adottare misure che siano idonee a limitare la conoscenza dei dati sensibili qualora essi siano presenti nei flussi documentali dell'Amministrazione garantendo il rispetto della riservatezza dei dati degli interessati.

SERVIZIO SANITARIO REGIONALE
BASILICATA
Azienda Sanitaria Locale di Potenza

## Scheda richiesta accesso al sistema informatico con VPN

NOME : _____

COGNOME : _____

MATRICOLA : _____

PROCEDURE AZIENDALI DA UTILIZZARE:

- Anagrafe Web
- Sigru
- Atti Digitali
  - Con relativa Firma Digitale
  - Senza Firma Digitale
- CEA Web
- Cruscotto Direzionale
- Giava – Vaccinazioni
- Gupar
- Gupar Web
- CUP – AIRO – ARCA
- Protesica
- Rilpres
- Siste Web
- Il proprio computer aziendale
  - Indirizzo IP (disponibile in alto a destra sul proprio Desktop) 172 . 16 . ___ . ___
- Altro

_____

_____

**Il richiedente dichiara che si impegna:**

- a non divulgare le credenziali aziendali ad altri soggetti;
- a rispettare le attuali disposizioni di legge in merito alla tutela dei dati personali.

**Dichiara, altresì, di essere a conoscenza che:**

- le predette credenziali sono nominali;
- tutte le operazioni effettuate con tali credenziali sono direttamente attribuibili al loro proprietario e verranno tracciate in appositi log;
- gli accessi e tutte le operazioni effettuate saranno registrati e controllati;
- gli utilizzi impropri delle suddette credenziali sono perseguibili a norma di legge;
- le credenziali saranno disattivate a fine rapporto e qualora siano utilizzate impropriamente, siano divulgate o smarrite, o in presenza di qualsivoglia violazione perpetrata mediante il loro utilizzo;
- di aver preso visione, e di accettare in ogni sua parte quanto riportato:

1. nell'informativa ai sensi dell'art. 13 del Regolamento (UE) 2016/679 (**Allegato 1**);
2. nell'**Allegato 2**- Informazioni e Istruzioni agli autorizzati al trattamento dati personali fornite dal Titolare;

- di impegnarsi a comunicare tempestivamente ogni eventuale variazione di titolarità della funzione istituzionale che ha effetto sulla gestione della predetta richiesta.

Data __/__/___

Il richiedente (Firma leggibile)

_____

Non allegare alla richiesta

## ALLEGATO 1. Informativa ai sensi dell'articolo 13 del Regolamento (UE) 2016/679

Gentile utente,

ai sensi dell'art. 13 del Regolamento Generale Europeo per la protezione dei dati personali (GDPR) General Data Protection Regulation (UE) 2016/679, l'Azienda Sanitaria di Potenza, in qualità di "Titolare" del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali. Il trattamento dei dati acquisiti per lo svolgimento di funzioni istituzionali e nell'esecuzione dei propri compiti di interesse pubblico, o comunque connessi all'esercizio dei propri pubblici poteri da parte dell'Azienda Sanitaria di Potenza, è lecito ai sensi dell'art. 6 "Liceità del trattamento" e non necessita del suo consenso.

11. **Fonte dei dati personali**

La raccolta dei dati personali avviene con la registrazione delle informazioni fornite dall'interessato al momento della compilazione della modulistica per la presentazione dell'istanza per il rilascio dell'account di rete e/o posta elettronica dell'Azienda Sanitaria di Potenza. In particolare, i dati trattati sono i dati anagrafici e la matricola.

12. **Finalità del trattamento e base giuridica**

I dati personali sono trattati esclusivamente per le seguenti finalità:

- Richiesta credenziali per l'accesso al sistema informatico tramite VPN SSL

La base giuridica è il Codice dell'Amministrazione Digitale D.lgs. 82/2005.

13. **Modalità di trattamento dei dati**

In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi in conformità alle disposizioni previste dall'articolo 32 GDPR.

14. **Facoltatività del conferimento dei dati**

Il conferimento dei dati è facoltativo. In mancanza, non sarà possibile adempiere alle finalità descritte al punto 2.

15. **Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati**

I dati personali potranno essere conosciuti esclusivamente dai funzionari dell'Azienda Sanitaria di Potenza autorizzati e/o Incaricati del trattamento. Per le sole finalità previste al paragrafo 2 (Finalità del trattamento), possono venire a conoscenza dei dati personali società terze fornitrici di servizi per l'Azienda Sanitaria di Potenza, previa designazione di Responsabili esterni del trattamento, che garantiranno il medesimo livello di protezione. Alcune delle informazioni personali fornite all'Azienda Sanitaria di Potenza, nel rispetto della normativa di cui al D. Lgs. 33/2013, potranno essere pubblicizzate sul sito istituzionale dell'Ente.

16.**Trasferimento dati**

I dati personali saranno conservati su server (fisici o virtuali) aziendali allocati in sedi all'interno dell'Unione Europea. Ove necessario, il Titolare avrà facoltà di spostare tali server, che rimarranno, in ogni caso, dentro i confini dell'Unione.

17.**Diritti dell'Interessato**

L'interessato/a al trattamento dati potrà esercitare, nei confronti del Titolare del trattamento, i diritti di cui agli articoli 15, 16, 17, 18 del GDPR (Diritto di accesso; Diritto di rettifica; Diritto alla cancellazione; Diritto di limitazione di trattamento).

18.**Titolare e Responsabili del trattamento**

Il Titolare del trattamento dei dati personali di cui alla presente Informativa è l'Azienda
Sanitaria di Potenza, con sede in Potenza alla via F. Torraca n. 2, CAP 85100. Responsabile per il riscontro delle richieste, da parte degli interessati del trattamento, per esercitare i diritti descritti nel paragrafo precedente è il RPD aziendale. Tali istanze potranno essere presentate dagli interessati tramite Posta Elettronica (rpd@aspbasilicata.it ) o, in alternativa, recandosi direttamente presso gli sportelli Urp i cui riferimenti sono presenti sul sito istituzionale (www.aspbasilicata.it - sezione URP).

19.**Diritto di reclamo**

L'interessato, qualora ritenesse che il trattamento dei suoi dati personali avvenga in violazione di quanto previsto dal Regolamento Generale Europeo, ha il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

20. **Responsabile della protezione dati**

Il Responsabile della Protezione dei Dati (RPD), è raggiungibile al seguente indirizzo:
Via F. Torraca n. 2, 85100, Potenza (Email: rpd@aspbasilicata.it).

Non allegare alla richiesta

**ALLEGATO 2 . Informazioni e Istruzioni agli autorizzati al trattamento dati personali fornite dal Titolare**

A tal fine, vengono fornite **INFORMAZIONI ED ISTRUZIONI** alle quali attenersi per l'assolvimento del compito assegnato:

- trattare i dati personali, in base all'art. 5 del GPDR**, in modo lecito**, corretto e trasparente e dovranno essere: ○ raccolti per finalità implicite e legittime e successivamente trattati in modo che non vi sia incompatibilità con tali finalità;
  - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
  - esatti, e se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
  - conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
  - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate ("integrità e riservatezza");
- 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 (ex Sensibili) e non;
- **raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli 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;
- recepire nuove indicazioni fornite dal Titolare del Trattamento anche partecipando a percorsi formativi quando previsti;
- **assicurare la riservatezza** opportuna e necessaria affinché il trattamento dei dati, sia effettuato in conformità alle disposizioni del GDPR e del D.lgs 196/2003 s.m.i. e volte alla prevenzione da parte del Titolare dei crimini informatici e del trattamento illecito di dati;
- trattare i dati personali, eventualmente riferiti a categorie particolari (art. 9) o relativi a condanne penali e reati (art. 10) è ammesso se lecito (art. 6) e cioè quando:
- l'interessato ha espresso il consenso al trattamento dei propri dati personali;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo di legge cui è tenuto il Titolare o per salvaguardare gli interessi vitali dell'interessato;

- il trattamento è necessario per il perseguimento del legittimo interesse del Titolare;
- **garantire all'interessato l'esercizio dei diritti** sui propri dati secondo quanto previsto dal GDPR (es: diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.); **Inoltre:**
- **è consentita la trasmissione di dati all'interno dell'organico del Titolare** per i compiti ed i fini stabiliti dallo stesso, agendo sotto la sua diretta autorità, allo stesso modo sono autorizzati i trattamenti di dati pseudonimizzati;
- **È vietata ogni comunicazione/diffusione di dati verso l'esterno dell'Amministrazione senza preventiva autorizzazione del Titolare stesso o del Responsabile**; il divieto permane anche dopo la cessazione dell'incarico e/o del rapporto di lavoro;
- **nessun dato deve essere comunicato a soggetti identificati esterni all'Amministrazione o diffuso** (trasmesso a soggetti indeterminati), senza specifica autorizzazione del Responsabile del Trattamento; è vietata la diffusione dei dati trattati ed in particolare di quelli sensibili;
- sono consentite le comunicazioni di dati che avvengono nell'ambito di un rapporto contrattuale/convenzionale instaurato dall'Amministrazione con terzi per l'esternalizzazione di attività/funzioni/servizi, **a condizione che il terzo sia stato nominato Responsabile esterno del trattamento dei dati**;
- **l'incarico conferito autorizza l'accesso agli archivi contenenti atti e documenti** riportanti dati personali comuni e al trattamento di questi; l'accesso ed il trattamento dati vanno limitati alle necessità per l'adempimento dei compiti da assolvere;
- per il tempo necessario allo svolgimento delle operazioni di trattamento si **dovrà diligentemente controllare e custodire gli atti e documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati**;
- **astenersi** dall'effettuare operazioni di trattamento dei dati personali, di cui si a conoscenza durante lo svolgimento dell'incarico, evitare di conservarli, duplicarli, comunicarli o cederli ad altri, dopo la cessazione del rapporto di lavoro;
- **in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati**;
- informare tempestivamente il Responsabile del trattamento di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste pervenute dagli interessati;
- nel caso in cui si constati o si sospetti un disguido o **un incidente che abbia messo o possa mettere a repentaglio la sicurezza dei dati trattati, darne immediata comunicazione al Responsabile del trattamento**;
- segnalare al Responsabile eventuali circostanze, che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro una adeguata azione di controllo;
- **non trasmettere dati particolari (sensibili) via e-mail.** Nel caso in cui sia strettamente necessaria tale forma di trasmissione per ragioni d'ufficio,

occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;
- rispettare, se presente, il documento sulla sicurezza dei dati, predisposto dall'Amministrazione;
- **non alterare in alcun modo la configurazione software della stazione di lavoro**, evitando di installare qualunque software sconosciuto o non approvato;
- **non utilizzare la rete dell'Amministrazione per fini non espressamente autorizzati**;
- è vietato l'utilizzo improprio di documenti, dati, informazioni a qualsiasi titolo posseduti, ricevuti o trasmessi;

**Con riferimento alle misure di sicurezza, le PERSONE AUTORIZZATE AL TRATTAMENTO O INCARICATI:**
- accedono al sistema informativo per **mezzo di credenziali di autenticazione**; le credenziali di autenticazione consistono in un codice (user id o username) per l'identificazione dell'incaricato, associata ad una parola chiave (password) conosciuta solo dall'incaricato;
- utilizzano la **password con una lunghezza minima di otto caratteri, contenenti caratteri numerici, alfanumerici e almeno un carattere speciale** (o, se il programma in uso non lo permette, dal numero massimo di caratteri consentito);
- **nella generazione della password non utilizzano elementi o notizie a loro facilmente riconducibili;**
- **modificano la password** al primo utilizzo, ogni volta che viene richiesto dal sistema (al massimo 6 mesi, 3 mesi se i dati trattati sono sensibili (ad. es. di salute) e/o giudiziari) e nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;
- qualora il sistema non renda obbligatoria la modifica della password nel rispetto dei predetti termini, **l'utilizzatore provvede autonomamente a tale variazione**;
- adottano particolari cautele per assicurare la **segretezza della password** (evitare la digitazione in presenza di terzi, conservarne i riferimenti in luogo non accessibile a terzi);
- nel caso di allontanamento dalla propria postazione di lavoro, **l'incaricato adotta tutte le cautele necessarie atte ad evitare l'accesso ai dati personali trattati o in trattamento sia cartaceo che automatizzato da parte di terzi**, anche se dipendenti, a meno che non siano autorizzati;
- **non lasciano la propria stazione di lavoro incustodita e collegata con il proprio account (nome utente) e password all'ambiente di rete**;
- **bloccano la propria stazione di lavoro durante la pausa pranzo**, ovvero in tutte le occasioni in cui ci si assenti dall'ufficio; nel caso in cui fosse necessario mantenere accesa la stazione di lavoro, utilizzare i metodi messi a disposizione dal sistema per bloccare la stessa, come ad esempio il blocco sessione o il salvaschermo con password;
- per le banche dati automatizzate utilizzano il proprio codice di accesso personale, evitando di operare su terminali altrui e/o lasciare aperto il sistema

operativo con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

- **tenere un comportamento corretto durante la navigazione in internet**, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete.
- devono garantire sempre la **corretta custodia** degli stessi; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri incaricati addetti al medesimo trattamento; non devono essere consultati da altri incaricati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
- devono conservare i documenti o gli atti che contengono **dati particolari (ex sensibili e/o giudiziari) in archivi ad accesso controllato** (armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale preposto);
- al termine delle operazioni di trattamento, devono, restituire tempestivamente la documentazione prelevata dagli archivi;
- **in caso di utilizzo di stampante, fotocopiatrice o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola stazione di lavoro, le stampe devono essere immediatamente raccolte e custodite** con le modalità sopra descritte;
- **non devono gettare via copie cartacee contenenti dati personali, senza averle distrutte prima in modo opportuno**;
- devono adottare misure che siano idonee a limitare la conoscenza dei dati sensibili qualora essi siano presenti nei flussi documentali dell'Amministrazione garantendo il rispetto della riservatezza dei dati degli interessati.