COMUNEDI STRIANO
Città Metropolitana di Napoli

Protocollo a margine

Ai Responsabili di Servizio,
anche n.q. di Referenti del RPCT

Ai dipendenti

Al DPO

E p.c. Al Sindaco
Al NdV

OGGETTO: DIRETTIVA OPERATIVA IN MATERIA DI CYBERSECURITY – ATTUAZIONE DELLE BUONE PRASSI CONTENUTE NEL VADEMECUM NOIPA – ACN (22 LUGLIO 2025)

Premesso che:
- la crescente digitalizzazione dei processi amministrativi espone le pubbliche amministrazioni a rischi cibernetici sempre più significativi;
- il 22 luglio 2025 è stato pubblicato, a cura dell'Agenzia per la Cybersicurezza Nazionale (ACN), il Vademecum di base per la cybersecurity per i dipendenti della Pubblica Amministrazione, in collaborazione con il Dipartimento della Funzione Pubblica e con il supporto del sistema NoiPA;

Considerato che:
- secondo il documento, oltre il 50 % degli incidenti informatici nelle PA è causato da comportamenti umani non consapevoli o negligenti;
- il Vademecum individua 12 regole operative che ciascun dipendente è tenuto ad adottare nell'uso quotidiano delle tecnologie;

Ritenuto opportuno:
- **richiamare formalmente l'attenzione di <u>tutto il personale del Comune</u> sull'importanza della sicurezza digitale e sul VADEMECUM ad oggetto "*Buone pratiche di cybersecurity***

di base per i dipendenti delle PP.AA" **indicato in oggetto e trasmesso in allegato alla presente direttiva;**

- fornire, inoltre, alcune indicazioni pratiche per la corretta gestione degli strumenti informatici e degli account personali/istituzionali.

Le indicazioni pratiche che seguono sono state condivise con il Responsabile della Transizione Digitale e con l'Istruttore informatico (**prot. n.12187/2025 del 21/08/2025**)

Tutto ciò premesso si DISPONE e RACCOMANDA:

1. Protezione delle credenziali

Ogni dipendente deve utilizzare password robuste, da 8 a 16 caratteri, con caratteri maiuscoli, minuscoli, numeri e simboli. È obbligatorio modificare le password almeno ogni 90 giorni e non riutilizzarle per servizi differenti. L'autenticazione a due fattori (2FA) va abilitata ove disponibile.

2. Utilizzo sicuro della posta elettronica

Non devono essere aperti allegati o link sospetti. Le email provenienti da mittenti sconosciuti o che presentano anomalie devono essere segnalate. È vietato inoltrare comunicazioni dubbie.

Tutti i tentativi di phishing (qualcuno finge di essere un'organizzazione affidabile per ingannare e rubare informazioni personali) devono essere comunicati tempestivamente al responsabile per la Transizione al Digitale.

3. Accesso sicuro alla rete

È vietato connettersi alle reti Wi-Fi pubbliche o non protette per accedere ai sistemi dell'Ente. È obbligatorio l'uso di VPN autorizzate quando si lavora da remoto (L'autorizzazione è resa per i dipendenti dal Responsabile del Servizio di appartenenza, per i Responsabili di Servizio e per il Segretario comunale dal R.T.D. ed infine per l'R.T.D. dal Sindaco). L'accesso da dispositivi personali non autorizzati è vietato.

4. Aggiornamenti software

I software e i sistemi operativi utilizzati devono essere sempre aggiornati. È vietata l'installazione di software o componenti non autorizzati.

Qualora possibile, si raccomanda di privilegiare l'utilizzo di software open source, in conformità alle indicazioni fornite dall'Ufficio CED, al fine di garantire l'uniformità delle soluzioni adottate sui dispositivi dell'Ente. Tali software, oltre a presentare numerosi vantaggi, sono generalmente considerati più sicuri e affidabili grazie al contributo della comunità di sviluppatori e alla trasparenza che caratterizza il loro processo di sviluppo.

5. Comportamenti responsabili

I dispositivi devono essere bloccati ogni volta che ci si allontana dalla postazione. È vietato l'uso di account istituzionali per fini personali. I dispositivi non devono mai essere lasciati incustoditi.

6. Utilizzo consapevole dell'Intelligenza Artificiale

È vietato inserire nelle piattaforme di intelligenza artificiale dati personali, sensibili o riservati.

7. Gestione dei dispositivi mobili

Tablet e smartphone comunali devono essere protetti da PIN e/o password. È vietata la connessione a reti non sicure o non approvate.

8. Backup e condivisione sicura dei dati

È obbligatorio eseguire backup secondo le indicazioni fornite. È vietata la condivisione di documenti riservati tramite cloud privati non autorizzati.

9. Formazione, simulazioni e test interni

Tutti i dipendenti devono partecipare alle attività formative promosse dall'Ente in materia di sicurezza informatica. La partecipazione è obbligatoria.

Saranno organizzate periodicamente simulazioni di phishing e test comportamentali per verificare il livello di consapevolezza. L'esito sarà utilizzato per rafforzare le politiche di sicurezza.

10. Gestione delle emergenze informatiche

Ogni anomalia, malfunzionamento o sospetto incidente deve essere comunicato immediatamente al Responsabile della Transizione Digitale e al Supporto tecnico.

11. Responsabilità individuale e sanzioni

Ciascun dipendente è personalmente responsabile del rispetto delle presenti disposizioni. In caso di violazione, si applicheranno le sanzioni previste dal CCNL e dal Codice di comportamento dei dipendenti pubblici.

***Allegato**: VADEMECUM ad oggetto "Buone pratiche di cybersecurity di base per i dipendenti delle PP.AA"*

Striano, 21/08/2025

IL SEGRETARIO COMUNALE

Dott. Giovanni Mazza

Firmato digitalmente da:
Mazza Giovanni
Firmato il 21/08/2025 13:34
Seriale Certificato: 4762536
Valido dal 30/07/2025 al 30/07/2028
InfoCamere Qualified Electronic Signature CA