

Allegato D

ALLEGATO TECNICO DELLE MISURE MINIME DI SICUREZZA

Il presente allegato descrive le misure minime di sicurezza che devono essere rispettate per poter usufruire del servizio telematico di consultazione dei dati anagrafici del Comune di Poggiomarino.

1. L'accesso al sistema è consentito esclusivamente al personale incaricato designati dal di responsabile esterno del trattamento dei dati personali dell'ente;
2. L'accesso è consentito tramite credenziali di autenticazione (username e password) rilasciati dal sistema informatico del Comune di Poggiomarino dopo la profilatura dell'utente. Le credenziali verranno automaticamente inviate all'indirizzo di posta elettronica personale dell'utente indicate sul modulo;
3. La username è univoca per ogni incaricato e coincide con il Codice Fiscale;
4. La password fornita è un codice alfanumerico di almeno 8 caratteri, la password deve contenere almeno una lettera maiuscola, una lettera minuscola ed un numero.
5. La password ha una scadenza di 30 giorni.
6. La nuova password non può coincidere con le password precedentemente inserite;
7. La piattaforma informerà l'utente, non appena effettua l'accesso, la data dell'ultimo accesso e l'indirizzo IP da cui è stato effettuato;
8. La password può essere modificata in qualsiasi momento, anche prima della sua scadenza;
9. L'account si bloccherà se si effettuano più di 5 tentativi errati di accesso.
10. L'accesso non è consentito dopo la scadenza della password. L'incaricato dovrà richiedere, per tramite del Responsabile esterno per l'accesso ai dati e del Responsabile della Convenzione dell'Amministrazione Richiedente la nuova password di primo accesso, compilando l'allegato E;
11. L'account viene disabilitato se non si effettuano accessi per più di 6 mesi. L'incaricato dovrà richiedere, per tramite del Responsabile esterno per l'accesso ai dati e del Responsabile dell'Amministrazione richiedente la nuova abilitazione, compilando l'allegato F;
12. Le credenziali devono essere custodite dall'incaricato che risponde personalmente per gli accessi effettuati se a seguito di controlli venissero riscontrare delle anomalie;
13. Tempestivamente l'incaricato dovrà informare sia il Responsabile esterno per l'accesso ai dati che il Responsabile dell'Amministrazione richiedente qualora incidenti di carattere organizzativo - tecnico occorsi sui propri sistemi di autenticazione abbiano impatti diretti e/o indiretti nei processi di sicurezza afferenti l'amministrazione titolare della banca dati. In tal caso sarà cura del Responsabile dell'Amministrazione richiedente informare il Supervisore al fine di disattivare gli accessi e monitorare se sussistono eventuali abusi;

14. Le postazioni utilizzate per l'accesso on-line alla banca dati anagrafica devono rispettare le misure minime di sicurezza previste dal codice per la protezione dei dati personali, quindi:
- a. Essere protetti da username e password;
 - b. La username deve individuare univocamente l'incaricato al trattamento;
 - c. La password deve essere sufficientemente complessa da non essere individuata e custodita dall'incaricato;
 - d. La password ha una scadenza;
 - e. La postazione di lavoro ha idonei software antivirus ed anti-spyware aggiornati per la protezione da software maligni;
15. Si allega vademecum per la scelta della password.

Si informa che il titolare del trattamento è il Comune di Poggiomarino e che il Responsabile interno del trattamento è il Responsabile del Settore Affari Generali ed Istituzionali – Responsabile dei Servizi Demografici, secondo gli atti di organizzazione vigente.

_____ li _____

Il Responsabile esterno al trattamento dei dati

L'Incaricato al trattamento dei dati

Alla presente si allega anche copia di un valido documento di riconoscimento dell'incaricato.

Vademecum sulla scelta delle password

La password è una chiave di accesso ad un'area personale, contenente dati personali e/o dati sensibili che devono trattare solo dall'interessato. Inoltre, non essendo possibile distinguere se l'utente che ha effettuato l'accesso è il reale utilizzatore o un usurpatore, è bene sceglierne una abbastanza semplice da ricordare ma allo stesso tempo abbastanza complessa da individuare.

Pertanto è opportuno scegliere la password in modo tale che:

- Sia almeno composta da 8 caratteri, con almeno 2 numeri, con l'alternanza di minuscole e maiuscole;
- Cambiarla frequentemente
- Non sia la data di nascita, cognome, nome
- Non siano scritte su post-it o sotto alla tastiera
- Non siano scritte su file, a meno di utilizzare algoritmi di crittografia, che non ne permettano l'apertura se non è nota la chiave;

E' bene tenere presente che esistono dei software capaci di individuare la password utilizzando speciali algoritmi che, alla velocità di circa 1 milione di tentativi al secondo, permettono di scoprire il codice segreto.

Di seguito viene riportato il tempo che tali programmi impiegano per risalire alla password:

	Numero di simboli utilizzati				
	solo lettere minuscole o maiuscole	combinazione di minuscole e maiuscole	uso anche di numeri	uso anche simboli particolari	tutti i simboli
lunghezza password	26	52	62	80	256
4	0,5 secondi	7 secondi	15 secondi	40 secondi	2 ore
6	5 minuti	5 ore	15 ore	3 giorni	9 anni
8	58 ore	2 anni	7 anni	53 anni	585 millenni
10	5 anni	45 secoli	266 secoli	340 millenni	38 miliardi di anni

Tabella 5: Tempi per intercettare la password

Si osserva come aumentando di solo 2 caratteri, a parità di simboli utilizzati, la password diventa più complessa da identificare.

Alla complessità del codice segreto scelto, c'è da aggiungere la probabilità che questa venga individuata da altri durante la digitazione, pertanto il codice impone che questa venga modificata con una certa frequenza, con massimo ogni 6 mesi per l'accesso a sistemi che trattano solo dati comuni, mentre la validità massima è di mesi 3 per l'accesso a dati sensibili.