

COMUNE DI CALENDASCO

POLOCY PER LA GESTIONE DEGLI ACCOUNT ISTITUZIONALI E LA CONTINUITÀ OPERATIVA DEI SERVIZI DIGITALI

Sommario

1. Premessa	2
2. Ambito di applicazione	3
3. Principio di disponibilità delle informazioni	3
4. Gestione degli account istituzionali in caso di assenza	4
5. Accesso agli account per esigenze organizzative o di sicurezza.....	4
6. Cessazione del rapporto di lavoro o collaborazione	5
7. Coordinamento con le procedure di sicurezza	5
8. Revisione e aggiornamento	5
9. Disposizioni finali.....	5

1. Premessa

1.1 La presente policy è adottata da:

COMUNE DI CALENDASCO, con sede in 29010 Calendasco (PC), via G. Mazzini n. 4, codice fiscale 00216710335, in persona del legale rappresentante pro tempore, nella qualità di Titolare del trattamento (di seguito **“Titolare”** o **“Ente”**).

1.2 La policy disciplina le modalità di gestione degli account istituzionali, degli strumenti informatici assegnati al personale e dei dati trattati mediante tali strumenti, al fine di garantire:

- > la continuità operativa dei servizi;
- > la disponibilità delle informazioni necessarie allo svolgimento delle attività istituzionali;
- > la sicurezza delle informazioni trattate;
- > la protezione dei dati personali.

.3 Le misure organizzative previste dal presente documento sono adottate anche ai sensi dell'art. 32 del Regolamento (UE) 2016/679 (GDPR), quale componente del sistema interno di gestione della sicurezza delle informazioni.

1.4 La presente policy si applica a tutto il personale che utilizza account istituzionali e strumenti informatici messi a disposizione dall'Ente nello svolgimento delle attività lavorative.

2. Ambito di applicazione

2.1 La presente policy si applica, in particolare, alla gestione:

- > degli account di posta elettronica istituzionale;
- > degli account di accesso ai sistemi informativi;
- > delle credenziali di autenticazione;
- > delle cartelle di rete e degli spazi di archiviazione condivisi;
- > dei dispositivi informatici assegnati al personale.

2.2 L'utilizzo di tali strumenti comporta il trattamento di informazioni e dati personali funzionali allo svolgimento delle attività istituzionali.

3. Principio di disponibilità delle informazioni

3.1 I dati, i documenti e le comunicazioni trattati mediante strumenti informatici istituzionali costituiscono patrimonio informativo dell'Ente e devono essere gestiti in modo tale da garantirne l'accessibilità per finalità operative e organizzative.

3.2 Il personale è tenuto a:

- > utilizzare gli strumenti assegnati esclusivamente per finalità istituzionali;
- > conservare i documenti di lavoro negli spazi di archiviazione messi a disposizione dall'Ente;
- > evitare la memorizzazione di dati istituzionali esclusivamente su dispositivi locali o supporti esterni.

4. Gestione degli account istituzionali in caso di assenza

4.1 In caso di assenza programmata o prolungata del personale, l'Ente può adottare misure organizzative idonee a garantire la continuità delle attività istituzionali, quali:

- > l'attivazione di messaggi automatici di risposta;
- > l'indicazione di recapiti alternativi per la gestione delle comunicazioni.

4.2 Il personale può preventivamente individuare un collega incaricato (c.d. fiduciario) al quale delegare, per il periodo di assenza:

- > la verifica dei messaggi di posta elettronica istituzionale;
- > l'inoltro delle comunicazioni rilevanti per lo svolgimento dell'attività lavorativa.

4.3 Le attività svolte dal fiduciario devono essere limitate alle sole esigenze organizzative e operative.

5. Accesso agli account per esigenze organizzative o di sicurezza

5.1 In caso di assenza temporanea o prolungata del personale, l'Ente può autorizzare l'accesso agli account istituzionali o agli strumenti informatici assegnati esclusivamente nei limiti di quanto necessario per garantire la continuità operativa delle attività istituzionali e nel rispetto dei principi di pertinenza, minimizzazione e proporzionalità.

5.2 L'accesso è consentito unicamente per finalità organizzative o di sicurezza e non può essere utilizzato per il monitoraggio dell'attività lavorativa del personale interessato.

5.3 L'accesso è effettuato esclusivamente da personale autorizzato alla gestione dei sistemi informativi e secondo procedure interne definite.

5.4 Il personale interessato è informato, alla prima occasione utile, delle operazioni eventualmente effettuate.

6. Cessazione del rapporto di lavoro o collaborazione

6.1 In caso di cessazione del rapporto di lavoro o di collaborazione:

- > gli account istituzionali assegnati sono disattivati;
- > le credenziali di accesso ai sistemi informativi sono revocate;
- > i dispositivi informatici assegnati devono essere restituiti.

6.2 Prima della cessazione, il personale interessato provvede a:

- > trasferire i documenti di lavoro negli spazi di archiviazione istituzionali;
- > eliminare eventuali contenuti personali presenti nella casella di posta elettronica istituzionale.

6.3 L'Ente può attivare, per un periodo limitato, un sistema automatico di risposta volto a informare i terzi della disattivazione dell'account e a fornire recapiti alternativi.

7. Coordinamento con le procedure di sicurezza

7.1 Eventuali anomalie, malfunzionamenti o incidenti che possano incidere sulla sicurezza delle informazioni devono essere segnalati secondo quanto previsto dalla procedura interna per la gestione degli incidenti di sicurezza e delle violazioni di dati personali.

8. Revisione e aggiornamento

8.1 Il presente documento potrà essere revisionato e aggiornato in relazione a mutamenti normativi o organizzativi.

9. Disposizioni finali

9.1 L'Ente provvede alla diffusione della presente policy con le modalità ritenute più opportune.