Trieste

DIPARTIMENTO INNOVAZIONE E SERVIZI AL CITTADINO
SERVIZIO TRASFORMAZIONE DIGITALE
COMUNE DI TRIESTE

Procedura Controllo Accessi

Rev.	Data	Causale	Redatto	Approvato
1	30/11/2025	Primo rilascio	PO Sicurezza Informatica	

Destinatari	CSIRT Interno / Responsabili e amministratori dei sistemi
Riferimento misure di base	PR.AA-01; PR.AA-03; PR.AA-05; PR.AA-06
Linee di progetto	1.B 4.A 4.B

Procedura Controllo Accessi.odt

Indice generale

1 Revisione del Piano

La procedura è soggetta a revisione annuale, salvo modifiche sostanziali o nuove disposizioni.

2 Scopo e ambito di applicazione

Il presente documento definisce le modalità di gestione delle credenziali di autenticazione e del controllo degli accessi fisici e logici ai sistemi informativi, alle reti, alle applicazioni e ai dati dell'Ente.

L'obiettivo è garantire la sicurezza delle informazioni e la conformità alle normative vigenti.

Il documento si applica a tutte le risorse ICT dell'Ente, comprese quelle gestite da fornitori terzi o in ambienti cloud, coinvolgendo dipendenti, collaboratori, consulenti e utenti esterni.

3 Riferimenti normativi

- Regolamento UE 2016/679 (GDPR)
- D.lgs. 138/2024
- Determinazione ACN n. 164179 del 2025 – Requisiti minimi di sicurezza ICT – Allegato 1

4 Principi generali

La gestione delle credenziali di autenticazione e dell'accesso fisico si fonda su:

- **Minimo privilegio**: concessione del minimo necessario di accesso per svolgere le funzioni assegnate.
- **Separazione dei ruoli**: differenziazione dei compiti per ridurre il rischio di abuso.
- **Identificazione univoca**: ogni utente deve disporre di un'identità digitale esclusiva e non condivisa.
- **Tracciabilità**: tutte le operazioni critiche devono essere registrate e monitorate.
- **Autenticazione forte**: adozione dove possibile di tecniche a più fattori (MFA) per proteggere i sistemi rilevanti.

5 Accessi logici

5.1 Ruoli nella gestione delle credenziali

In un sistema ci sono i seguenti attori:

- Fornitore, che dovrà avere un recapito per questioni inerenti la cybersicurezza;
- “Responsabile interno del sistema”, individuato come il dirigente responsabile del flusso informativo, o in alternativa il RUP della procedura;
- Gli amministratori di sistema, individuati dal “Responsabile interno del sistema”, con compiti tecnici di gestione;
- Gli utenti del sistema;

5.1.1 Responsabile interno del sistema

Il Responsabile interno del sistema:

- nomina gli amministratori di sistema interni (se necessari) previa valutazione di esperienza, capacità ed affidabilità;
- aggiorna l’elenco degli amministratori di sistema;
- revoca gli amministratori di sistema;
- comunica le azioni precedenti alla casella cyber@comune.trieste.it.

Il Responsabile interno del sistema conduce una verifica annuale delle utenze con privilegi amministrativi per confermarne la necessità e revocare quelle non più giustificate.

5.1.2 Amministratori di sistema

Gli amministratori di sistema devono vigilare che le autorizzazioni degli utenti, anche in seguito a spostamenti o cambi mansione siano in conformità con il principio del privilegio minimo.

Gli amministratori di sistema conducono, almeno una volta all’anno, una verifica di tutte le utenze attive per identificare e disabilitare o rimuovere account inattivi in accordo con le informative sul trattamento dei dati dei singoli sistemi.

L’esito della verifica si concretizza nella produzione di un elenco degli utenti attivi che deve essere salvato.

Gli amministratori di sistema definiscono il processo tecnico autorizzativo per la creazione, aggiornamento e revoca delle credenziali degli utenti di sistema.

5.1.3 Utenti di sistema

Ogni utente deve disporre di credenziali di accesso personali limitate alle funzionalità necessarie per l’esecuzione del proprio lavoro.

Le credenziali vengono create, modificate o revocate attraverso un processo tecnico autorizzativo deciso dagli amministratori del sistema.

Gli account temporanei, ove il sistema lo consenta, vengono sempre creati con una scadenza automatica.

5.2 Autenticazione

L'autenticazione deve avvenire preferibilmente tramite identità digitale come ad esempio CIE, SPID, CNS, eIDAS .

L'uso del secondo fattore di autenticazione (MFA) è suggerito ove implementabile.

Le password, ove possibile, devono rispettare i requisiti minimi definiti nel documento "Linee guida per la gestione delle password" reperibile sulla Intranet comunale.

5.3 Monitoraggio e auditing

Gli accessi amministrativi ai sistemi rilevanti, ove presenti, vengono salvati in locale e ove possibile sul concentratore SysLog interno anche al fine di permettere analisi automatiche e conservazione sicura (es. SIEM).

Per motivi di sicurezza informatica, potrà essere attivato il monitoraggio e l'auditing degli accessi a tutti i sistemi per permettere analisi automatizzate.

5.4 Smarrimento o furto

L'utente in caso di perdita o furto delle credenziali di uno o più sistemi è tenuto a segnalare immediatamente l'evento agli amministratori dei sistemi interessati.

A seguito dell'evento le credenziali dovranno essere tempestivamente rigenerate.

6 Accessi fisici

6.1 Gestione dei badge

L'accesso alle sedi comunali è regolato tramite badge personali non cedibili. La gestione del sistema di controllo accessi è un processo strutturato che coinvolge diverse tecnologie e fornitori.

Si distinguono le seguenti modalità di accesso:

- **Accesso Standard**: I dipendenti comunali e il personale di fornitori con contratti di servizio continuativi (es. pulizie, manutenzione) sono dotati di un badge RFID personale o in alternativa tesserino identificativo e chiavi di accesso.

- **Accesso Ospiti**: gli ospiti che devono accedere alle sale controllate da badge, per esempio per manutenzioni occasionali, vengono accompagnati da personale dipendente.

I badge di accesso vengono attivati, modificati e revocati attraverso un processo autorizzativo.

La gestione dell'accesso fisico segue le medesime logiche dei paragrafi 5.1 Ruoli nella gestione delle credenziali e Errore: sorgente del riferimento non trovata Errore: sorgente del riferimento non trovata.

6.2 Smarrimento o furto

Il titolare del badge è tenuto a:

- fare denuncia di smarrimento o furto agli organi competenti;
- segnalare immediatamente l'evento al proprio responsabile
- segnalare immediatamente l'evento alla mail cyber@comune.trieste.it.

A seguito della segnalazione, il badge smarrito viene irrevocabilmente annullato dal sistema e, se necessario, ne viene emesso uno nuovo per sostituirlo.