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

Trieste

Norme di Comportamento Terze Parti

REVISIONI

Rev.	Data	Causale	Redatto	Approvato
1	8/6/2026	Primo rilascio	PO SIAR	NCS

Destinatari	Terze parti
Riferimento misura di base	GV.SC-01

Norme di Comportamento Terze Parti.odt

Indice generale

1 Revisione del documento

Il documento è soggetto a revisione annuale, salvo modifiche sostanziali o nuove disposizioni.

2 Scopo e ambito di applicazione

Questo documento definisce le norme di comportamento che le terze parti, che operano per conto del Comune di Trieste, devono rispettare per garantire la sicurezza delle informazioni.

Per Sicurezza delle Informazioni si intende la tutela dei seguenti principi:

- **Riservatezza:** l'informazione deve essere accessibile solo al personale autorizzato.
- **Integrità:** l'informazione non deve essere modificata o eliminata in maniera inappropriata, né accidentalmente né intenzionalmente.
- **Disponibilità:** l'informazione deve essere accessibile e utilizzabile quando richiesto.

Le presenti norme si applicano a consulenti, collaboratori e fornitori esterni che:

- operano presso le sedi del Comune di Trieste;
- accedono alle risorse comunali da remoto (dalla propria sede o in smart working) anche tramite connessioni VPN.

3 Controlli e verifiche

Il Comune di Trieste si riserva la facoltà di effettuare controlli periodici sull’utilizzo delle risorse IT e sull'osservanza di quanto stabilito nel presente documento, previo preavviso ove necessario e consentito dalla normativa, per verificare la corretta applicazione delle norme di sicurezza.

4 Regole e procedura di gestione

I locali e tutte le risorse fisiche fornite dal Comune di Trieste, che contengono materiale di natura informatica o infrastrutture di rete e/o fonia, devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un’efficiente conduzione dell’attività lavorativa e un adeguato livello di sicurezza delle informazioni.

Nei paragrafi successivi sono descritti i comportamenti a cui tutti i soggetti terzi devono attenersi per garantire la sicurezza, sia fisica delle aree, sia degli asset aziendali.

4.1 Regole d’accesso e custodia dei locali

L’accesso ai locali è consentito solo alle persone che hanno precise e motivate esigenze di accedervi per finalità lavorative.
Alle persone potranno essere consegnati badge o chiavi di accesso dai referenti comunali dell’appalto che vigileranno sul loro corretto utilizzo, e comunicheranno alla mail cyber@comune.trieste.it eventuali smarrimenti o furti; tali dispositivi non sono cedibili e non devono essere lasciati incustoditi.
In caso di smarrimento, furto o danneggiamento del badge o delle chiavi di accesso, la terza parte è tenuta a darne immediata comunicazione ai referenti dell’appalto.
Al termine della collaborazione il badge o le chiavi di accesso devono essere restituiti integri ai referenti dell’appalto.

4.2 Comportamenti per la sicurezza operativa

Le terze parti devono operare per garantire la massima confidenzialità delle informazioni critiche visualizzate.
Vengono di seguito riportate una serie di indicazioni comportamentali alle quali attenersi:

- è vietato eludere i sistemi di sicurezza implementati dal Comune o effettuarne scansioni o verifiche non autorizzate;
- i computer devono essere bloccati quando l’area di lavoro non è occupata;
- deve essere previsto e implementato un meccanismo automatico di blocco della macchina a seguito di un periodo di inattività superiore a 10 minuti;
- le stampe devono immediatamente essere rimosse dalla stampante, non lasciate incustodite e distrutte a fine attività;
- l’utilizzo di dispositivi di archiviazione di massa va limitato ed in ogni caso è richiesta la scansione automatica dell’antivirus al collegamento del dispositivo;
- va effettuato il log-off da applicazioni o servizi di rete quando non più utilizzati.

4.3 Gestione delle credenziali di accesso e password

Le terze parti devono prestare la massima attenzione nell’utilizzo, nella gestione e nella conservazione delle credenziali di autenticazione, seguendo le norme del buon senso, tra cui:

- evitare di annotare le credenziali in luoghi (fisici e virtuali) condivisi;
- evitare di rivelare la logica di creazione della password;
- evitare che venga osservato l’input della password;
- evitare di ri-utilizzare password di altri servizi, anche personali;
- laddove disponibile, abilitare MFA;
- cambiare regolarmente le password scegliendole adeguatamente complesse;
- in caso di sospetto di compromissione delle credenziali si deve provvedere alla rigenerazione delle stesse oppure alla richiesta di disabilitazione.

4.4 Accesso logico ai sistemi mediante profilo amministratore

L’accesso logico ai sistemi informativi del Comune di personale delle terze parti con privilegi amministrativi deve essere limitato ai soli casi strettamente necessari per l’esecuzione delle attività contrattuali.
In particolare:

- devono essere utilizzate credenziali individuali e non condivise, con privilegi coerenti con le mansioni assegnate (principio del minimo privilegio);
- l’accesso deve avvenire attraverso meccanismi di autenticazione forte (es. MFA), ove tecnicamente possibile;
- gli accessi devono essere limitati temporalmente e disabilitati al termine delle attività o alla cessazione del rapporto contrattuale;
- è fatto divieto di utilizzare account amministrativi per attività ordinarie.

Le terze parti si impegnano a operare nel rispetto delle disposizioni normative vigenti, incluse le indicazioni del Garante per la protezione dei dati personali in materia di amministratori di sistema, nonché delle “politiche di sicurezza delle informazioni” adottate dal Comune così come integrate nel PIAO.
Eventuali anomalie o utilizzi impropri degli accessi devono essere immediatamente segnalati ai referenti dell’Ente.

4.5 Furto o smarrimento di dispositivi informatici

In caso di furto o smarrimento di un asset di proprietà del Comune oppure di un dispositivo che interagisce con sistemi informativi e di rete comunali, le terze parti dovranno darne immediata comunicazione ai referenti comunali dell’appalto fornendo le seguenti informazioni:

- nome e cognome dell’utilizzatore dell’asset smarrito e delle relative utenze utilizzate;
- evidenza di avvenuta denuncia alle autorità competenti.

5 Principi generali per il corretto utilizzo degli strumenti aziendali

Nel caso le terze parti, per lo svolgimento dell’attività lavorativa, utilizzino alcuni servizi quali la posta elettronica e la connessione a Internet e/o alla rete comunale messi a disposizione dall’Ente, questi devono essere usati esclusivamente per finalità di natura lavorativa derivante dall’oggetto dell’appalto.

6 Obbligo di riservatezza

Tutte le informazioni, i dati e i documenti del Comune di Trieste di cui le terze parti vengono a conoscenza nell'ambito del contratto devono rimanere strettamente confidenziali. Non possono essere divulgati o utilizzati per scopi diversi dall'esecuzione del contratto. L'obbligo di riservatezza copre ogni tipo di informazione, inclusi dati personali/particolari, know-how e segreti d'ufficio.