



Trieste

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

Norme di Comportamento Terze Parti

REVISIONI

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

Destinatari	Terze parti
Riferimento misura di base	GV.SC-01
Linee di progetto	5.B

Norme di Comportamento Terze Parti	  Finanziato dall'Unione europea NextGenerationEU   DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE  Dipartimento Innovazione e Servizi al Cittadino Servizio Trasformazione Digitale Comune di Trieste
	Revisione 2 dd 04/08/2025

Indice

Modalità di aggiornamento.....	3
Scopo e Campo di Applicazione.....	3
Controlli e Verifiche.....	3
Regole e Procedura di gestione.....	4
Regole d'accesso e custodia dei locali.....	4
Comportamenti per la sicurezza operativa.....	4
Gestione delle credenziali di accesso e password.....	5
Furto o Smarrimento di dispositivi informatici.....	5
Principi generali per il corretto utilizzo degli strumenti aziendali.....	6
Obbligo di riservatezza.....	6

Norme di Comportamento Terze Parti	  Finanziato dall'Unione europea NextGenerationEU  DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE  Dipartimento Innovazione e Servizi al Cittadino Servizio Trasformazione Digitale Comune di Trieste Revisione 2 dd 04/08/2025
--	--

Modalità di aggiornamento

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

Scopo e Campo 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;
- Consulenti, collaboratori e fornitori esterni che accedono alle risorse comunali da remoto (dalla propria sede o in smart working) anche tramite connessioni VPN.

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

Norme di Comportamento Terze Parti	  Finanziato dall'Unione europea NextGenerationEU   DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE  Dipartimento Innovazione e Servizi al Cittadino Servizio Trasformazione Digitale Comune di Trieste
	Revisione 2 dd 04/08/2025

necessario e consentito dalla normativa, per verificare la corretta applicazione delle norme di sicurezza.

Regole e Procedura di gestione

I locali e tutte le risorse fisiche fornite dal Comune di Trieste 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 che hanno accesso ai locali e alle risorse fisiche e logiche del Comune di Trieste, devono attenersi per garantire la sicurezza fisica di aree ed asset aziendali.

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 consegnate badge o chiavi di accesso dai referenti comunali dell'appalto che vigileranno sul loro corretto utilizzo: tali dispositivi non sono cedibili e non devono essere lasciati incustoditi.

Al termine della collaborazione il badge o le chiavi di accesso devono essere restituiti integri ai referenti dell'appalto.

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.

In caso di smarrimento o furto dovrà essere fatta denuncia alle autorità competenti e comunicare l'evento alla mail cyber@comune.trieste.it.

Potranno essere applicati addebiti per la sostituzione secondo le procedure e i costi definiti dal Comune di Trieste.

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 effettuare attività non autorizzate di analisi del traffico di rete;
- i computer devono essere bloccati quando l'area di lavoro non è occupata;

Norme di Comportamento Terze Parti	  Finanziato dall'Unione europea NextGenerationEU   DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE 
	Dipartimento Innovazione e Servizi al Cittadino Servizio Trasformazione Digitale Comune di Trieste Revisione 2 dd 04/08/2025

- deve inoltre 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.

Gestione delle credenziali di accesso e password

L'accesso ai sistemi informativi da parte delle terze parti deve avvenire solamente mediante credenziali assegnate e non cedibili.

Le terze parti devono prestare la massima attenzione nell'utilizzo, nella gestione e nella conservazione delle credenziali di autenticazione.

In particolare, rifacendosi alle politiche di "igiene delle credenziali", occorre seguire 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 utilizzare password già utilizzate in passato o utilizzate per 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.

Furto o Smarrimento di dispositivi informatici

In caso di furto o smarrimento di un asset di proprietà del Comune oppure che interagisce con sistemi comunali, il fornitore dovrà darne immediata comunicazione al RUP fornendo le seguenti informazioni:

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

Norme di Comportamento Terze Parti	  Finanziato dall'Unione europea NextGenerationEU   DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE 
	Dipartimento Innovazione e Servizi al Cittadino Servizio Trasformazione Digitale Comune di Trieste Revisione 2 dd 04/08/2025

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 utilizzati esclusivamente per finalità di natura lavorativa derivante dall'oggetto dell'appalto.

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.