



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

**Trieste**

# **Capitolato Speciale d'Appalto Reingegnerizzazione della rete di videosorveglianza cittadina**

|                                                                                   |                                                                                                                                  |                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p align="center"><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

## Indice

|                                                                                                                               |    |
|-------------------------------------------------------------------------------------------------------------------------------|----|
| Premesse.....                                                                                                                 | 3  |
| Art. 1 Oggetto del servizio.....                                                                                              | 4  |
| Art. 2 Obiettivi tecnici minimi.....                                                                                          | 6  |
| Art. 3 Rilevazione dello stato di fatto dell'infrastruttura.....                                                              | 6  |
| Art. 4 Deliverable tecnici attesi.....                                                                                        | 8  |
| Art. 5 Requisiti minimi di architettura, routing, trasporto dei flussi video, sicurezza<br>informatica e conformità NIS2..... | 10 |
| 5.1 Modello architetturale e domini.....                                                                                      | 11 |
| 5.2 Indirizzamento, modello Layer 2/Layer 3, discovery e sincronizzazione<br>temporale.....                                   | 12 |
| 5.3 Routing interno, routing esterno, overlay e interconnessioni.....                                                         | 13 |
| 5.4 Multicast, qualità del servizio e trasporto dei flussi video.....                                                         | 14 |
| 5.5 Segmentazione, controllo degli accessi e sicurezza di rete.....                                                           | 15 |
| 5.6 Hardening degli apparati e protezione del control plane.....                                                              | 16 |
| 5.7 Monitoraggio, logging e reporting.....                                                                                    | 17 |
| 5.8 Gestione del rischio, risposta agli incidenti e sicurezza della supply chain<br>secondo la direttiva NIS 2.....           | 18 |
| 5.9 Resilienza e continuità operativa.....                                                                                    | 19 |
| Art. 6 Divieti e prescrizioni di sicurezza.....                                                                               | 19 |
| Art. 7 Migrazione e continuità del servizio.....                                                                              | 20 |
| Art. 8 Collaudo e accettazione.....                                                                                           | 21 |
| Art. 9 Durata delle attività.....                                                                                             | 22 |
| Art. 10 Obblighi e responsabilità delle parti.....                                                                            | 23 |
| 10.1 Obblighi dell'Operatore Economico.....                                                                                   | 23 |
| 10.2 Obblighi della Stazione Appaltante.....                                                                                  | 24 |
| Art. 11 Procedura e Criteri per la scelta discrezionale del contraente nell'ambito<br>dell'affidamento diretto.....           | 24 |
| Art. 12 Verifica di conformità e chiusura del servizio.....                                                                   | 25 |
| Art. 13 Trattamento dei dati, riservatezza e sicurezza delle informazioni.....                                                | 25 |
| Art. 14 Disposizioni finali.....                                                                                              | 26 |
| Art. 15 Riferimenti normativi e tecnici.....                                                                                  | 26 |

|                                                                                   |                                                                                                                   |                                                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

## Premesse

Il presente Capitolato Speciale d'Appalto disciplina l'affidamento di un servizio specialistico integrato per la reingegnerizzazione della rete di videosorveglianza cittadina del Comune di Trieste. Il servizio comprende l'analisi dell'esistente, la progettazione di dettaglio, la configurazione e l'integrazione delle componenti disponibili, la migrazione controllata, l'applicazione delle misure di sicurezza, il collaudo tecnico-funzionale, il trasferimento di conoscenze e l'assistenza alla messa in esercizio. Il perimetro quantitativo e funzionale delle prestazioni è definito nella Relazione Tecnica, che costituisce parte integrante della documentazione contrattuale.

Le prestazioni dovranno essere eseguite in coerenza con il decreto legislativo 31 marzo 2023, n. 36, con il decreto legislativo 4 settembre 2024, n. 138 di recepimento della direttiva NIS2, con i provvedimenti e le determinazioni dell'Agenzia per la cybersicurezza nazionale, con le migliori pratiche tecniche di settore e con la normativa applicabile in materia di protezione dei dati personali e sicurezza sul lavoro. Gli obblighi di cybersicurezza richiesti all'Operatore Economico sono limitati al perimetro contrattuale e alle misure tecniche e organizzative individuate dalla Stazione Appaltante come applicabili; la governance complessiva degli adempimenti dell'Ente resta in capo alla Stazione Appaltante.

|                                                                                   |                                                                                                                                  |                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p align="center"><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

## **Art. 1 Oggetto del servizio**

L'appalto ha per oggetto l'erogazione di un servizio specialistico per la reingegnerizzazione della rete di videosorveglianza cittadina e delle relative componenti di connettività, sicurezza, monitoraggio e gestione.

Nei limiti delle capacità tecniche delle componenti esistenti, la reingegnerizzazione della rete dovrà condurre alla messa in esercizio di un'architettura target segmentata, resiliente, scalabile, sicura, monitorabile e osservabile, idonea a garantire il trasporto continuo e affidabile dei flussi video IP verso le centrali operative, i sistemi VMS/NVR, lo storage, e le postazioni autorizzate.

Il servizio dovrà comprendere almeno:

- la verifica e il completamento dello stato di fatto, dell'inventario e della baseline tecnica, a partire dalla Relazione Tecnica e dalle informazioni rese disponibili dalla Stazione Appaltante;
- la progettazione di dettaglio dell'architettura target, del piano di indirizzamento, della segmentazione, del routing, delle interconnessioni, dei requisiti prestazionali, delle misure di sicurezza e dei criteri di accettazione;
- la razionalizzazione, la configurazione, l'integrazione e l'hardening degli apparati e dei sistemi inclusi nel perimetro, nonché l'integrazione con le funzioni di monitoraggio, logging e telemetria disponibili;
- la migrazione controllata dei servizi e delle configurazioni, con change management, backup, verifiche pre e post intervento e procedure di rollback;
- l'esecuzione dei test funzionali, prestazionali, di sicurezza, resilienza e continuità operativa, il collaudo tecnico-funzionale e la messa in esercizio;
- la produzione dei deliverable contrattuali, l'affiancamento, il trasferimento di conoscenze e l'assistenza all'avviamento.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

Le attività dovranno essere pianificate ed eseguite assicurando, per quanto tecnicamente possibile, la continuità operativa del sistema di videosorveglianza durante tutte le fasi di configurazione, migrazione, verifica e messa in esercizio. Le eventuali interruzioni dovranno essere ridotte al minimo e preventivamente concordate con la Stazione Appaltante quanto a modalità e tempistiche.

Le prescrizioni del presente Capitolato, della Relazione tecnica e del progetto di dettaglio approvato costituiscono il riferimento per l'esecuzione dell'intervento e per la verifica della conformità rispetto ai requisiti funzionali, prestazionali, operativi, di sicurezza e resilienza richiesti dalla Stazione Appaltante.

Al termine del servizio, l'Operatore Economico dovrà consegnare, per il perimetro contrattuale, un'infrastruttura configurata, documentata, verificata e collaudata, trasferita sotto il profilo operativo e manutentivo al personale tecnico dell'Ente. La documentazione dovrà consentire la gestione ordinaria in condizioni di tracciabilità, conoscibilità delle configurazioni e governabilità tecnica.

Il servizio è da intendersi "chiavi in mano" per le attività di analisi, configurazione, integrazione, migrazione, documentazione e collaudo delle componenti incluse nel perimetro e tecnicamente idonee. Restano escluse qualsiasi tipo di fornitura e installazione di nuovi dispositivi, prodotti software o licenze. Qualora per il raggiungimento degli obiettivi sia necessaria la realizzazione ex-novo di servizi di supporto (quali, a titolo esemplificativo, server radius, syslog), l'OE dovrà utilizzare la piattaforma hardware messa a disposizione dalla SA. L'attività comprende l'installazione da zero dell'hypervisor, la creazione e la configurazione delle VM, nonché l'implementazione e l'integrazione dei relativi servizi.

Qualora il raggiungimento di un requisito sia impedito da limiti documentati di apparati, licenze, infrastrutture o servizi di terzi preesistenti, l'Operatore Economico dovrà segnalarlo tempestivamente alla Stazione Appaltante, proporre le misure compensative praticabili e, ove necessario, formulare una motivata azione di adeguamento dell'infrastruttura. Eventuali proposte di acquisto di dispositivi o

|                                                                                   |                                                                                                                   |                                                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

prodotti software, potranno essere sottoposte alla SA, che ne valuterà l'acquisto mediante procedura autonoma e separata dal servizio in oggetto.

## **Art. 2 Obiettivi tecnici minimi**

L'Operatore Economico dovrà progettare e realizzare gli interventi inclusi nel perimetro in modo da conseguire i seguenti obiettivi minimi, secondo valori e criteri definiti nella baseline e nel progetto di dettaglio approvato:

- architettura modulare, scalabile, governabile e basata, per quanto tecnicamente sostenibile, su standard aperti e interoperabili, capace di accompagnare l'evoluzione del servizio senza interventi radicali sulla infrastruttura del sistema;
- separazione dei domini funzionali e applicazione del principio del minimo privilegio, con controllo e tracciabilità degli accessi amministrativi e operativi;
- resilienza commisurata alla criticità dei servizi e alle capacità degli apparati esistenti, con riduzione dei single point of failure e rapido ripristino delle funzioni essenziali;
- trasporto stabile dei flussi video, con capacità e qualità del servizio adeguate ai profili reali e agli scenari di picco approvati;
- protezione degli apparati, hardening, monitoraggio, logging, telemetria e rilevazione tempestiva di anomalie e compromissioni;
- documentazione completa, tracciabilità delle configurazioni, manutenibilità nel tempo e attuazione, per il perimetro contrattuale, delle misure NIS2 individuate dalla Stazione Appaltante come applicabili.

## **Art. 3 Rilevazione dello stato di fatto dell'infrastruttura**

L'Operatore Economico dovrà verificare e completare, quale attività preliminare, il quadro conoscitivo dell'infrastruttura descritto nella Relazione Tecnica. La

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

ricognizione ha lo scopo di validare il perimetro degli interventi, rilevare la baseline tecnica e acquisire gli elementi necessari alla nuova progettazione.

La ricognizione dovrà comprendere almeno:

- la verifica dell'inventario degli apparati e dei sistemi, con modello, ubicazione, numero di serie, versione firmware/software, ruolo, indirizzamento, stato di supporto, criticità e dipendenze;
- la ricostruzione della topologia fisica e logica, dei collegamenti, dei domini, delle VLAN, subnet e VRF, del piano di indirizzamento, del modello Layer 2/Layer 3, dei protocolli di routing, delle interconnessioni e degli eventuali overlay;
- l'analisi dei profili di traffico e la misurazione della baseline prestazionale, incluse banda, latenza, jitter, perdita di pacchetti, saturazione, errori di interfaccia e scenari di picco realistici;
- la verifica di segmentazione, superfici di esposizione, accessi e manutenzione remota, servizi e protocolli attivi, credenziali privilegiate, policy di filtraggio, backup, patch, firmware e rischi connessi alla supply chain;
- la verifica dei sistemi e delle funzioni disponibili per management, monitoraggio, telemetria, logging, alerting, correlazione degli eventi e sincronizzazione temporale;
- l'individuazione di single point of failure, interdipendenze, criticità, vincoli tecnici e organizzativi, capacità di ripristino e incompatibilità che possano limitare il raggiungimento dei requisiti.

Gli esiti dovranno confluire nel documento "2 – Stato di fatto e baseline", corredato da inventario, schemi, mapping dei collegamenti, misure rilevate, criticità e vincoli.

La relazione sullo stato di fatto, il progetto di dettaglio, il piano di migrazione e il piano dei test dovranno essere condivisi e validati con il personale tecnico della Stazione Appaltante. Nessuna modifica in ambiente di produzione potrà essere avviata prima della relativa approvazione da parte della SA.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

L'attività di verifica e sopralluogo dovrà essere effettuata in presenza presso la sede dell'Ente dal personale dell'OE. Le attività che possono essere effettuate a distanza, dovranno utilizzare canali autorizzati e modalità preventivamente concordate con la Stazione Appaltante.

## Art. 4 Deliverable tecnici attesi

All'avvio del contratto, l'OE dovrà produrre una serie di deliverables tecnici che dovranno essere organizzati nei seguenti pacchetti documentali. La consegna dovrà avvenire in formato modificabile aperto (odt o equivalente) e, ove richiesto, anche in formato di consultazione PDF.

Fase 1 – Ricognizione e consolidamento stato di fatto

1. **Cronoprogramma.** Articolazione per fasi, ruoli, contatti, dipendenze, finestre operative, verifiche pre e post intervento, backup, criteri di annullamento e rollback.
2. **Stato di fatto e baseline.** Inventario (modello, ubicazione, numero di serie, versione firmware/software, ruolo funzionale, indirizzamento, stato di supporto del produttore), topologia fisica e logica, configurazioni iniziali, dipendenze, criticità e misure prestazionali rilevate.

Fase 2 – Progettazione di dettaglio e piano di migrazione

3. **Progetto di dettaglio e criteri di accettazione.** Architettura target, modello Layer 2/Layer 3, piano di indirizzamento IP e rinumerazione, segmentazione dei domini, IPAM o registro equivalente, VRF, routing, interconnessioni, matrice dei flussi, QoS, multicast, capacity planning, policy di sicurezza.
4. **Piano di migrazione e criteri di accettazione.** Modalità di transizione dall'architettura esistente alla nuova architettura, azioni preliminari, attività di attivazione, verifiche post-migrazione con relativi valori attesi e metodi di prova, procedure di rollback in caso di anomalie o insuccesso.

|                                                                                   |                                                                                                                   |                                                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

5. **Sicurezza, monitoraggio e continuità.** Piano di hardening, trattamento del rischio, accessi privilegiati, vulnerability e patch management, integrazione con NMS, logging e SIEM disponibili, soglie e dashboard, conservazione dei log, risposta agli incidenti, supply chain, backup, restore, RTO, RPO e continuità operativa.

Fase 3 – Implementazione del servizio di reingegnerizzazione

#### 6. **Implementazione e documentazione as-built.**

1. Evidenza delle misure di hardening effettivamente implementate sugli apparati e sui sistemi, inclusi disabilitazione dei servizi non necessari, protezione degli accessi amministrativi, segmentazione, policy di filtraggio, protezione del control plane, sincronizzazione temporale e altri presidi di sicurezza applicati.
2. Matrice dei flussi e delle regole di comunicazione, riportante i flussi autorizzati tra i diversi domini della rete, le relative porte e protocolli, i sistemi sorgente e destinazione, nonché la giustificazione funzionale e operativa di ciascuna comunicazione consentita.
3. Piano di monitoraggio, logging e telemetria, indicazione delle metriche raccolte, sorgenti log abilitate, dashboard operative predisposte, soglie di allarme, meccanismi di correlazione eventi e modalità di integrazione con eventuali piattaforme NMS, SIEM o sistemi equivalenti.
4. Piano di backup e ripristino delle configurazioni, procedure operative per il salvataggio, il versionamento, il restore e la verifica periodica delle configurazioni e degli elementi essenziali al ripristino della rete in caso di guasto o compromissione.
5. Configurazioni as-built finali (switch, router, firewall, apparati di accesso, sistemi di gestione e componenti connessi), baseline di esercizio, registro delle modifiche, verbali di attivazione, topologia, mapping logico e fisico

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

aggiornati, servizi attivi, scostamenti approvati dalla SA e istruzioni per gestione e manutenzione.

Fase 4 – Test, collaudo e correzione anomalie

7. **Test e collaudo.** Piano dei test, evidenze, misure, risultati, prove di connettività, routing, sicurezza, QoS, failover, backup e ripristino, non conformità, azioni correttive e verbali di accettazione.

Fase 5 – As-built e handover

8. **Trasferimento di conoscenze.** Piano di affiancamento, sessioni di handover, procedure operative, modalità di gestione ordinaria, scenari di guasto, modalità di verifica e ripristino.
9. **Relazione tecnica finale di intervento.** Descrizione delle attività eseguite, criticità riscontrate e risolte, soluzioni adottate, scostamenti eventualmente intervenuti rispetto alla pianificazione iniziale e stato conclusivo della reingegnerizzazione.

## **Art. 5 Requisiti minimi di architettura, routing, trasporto dei flussi video, sicurezza informatica e conformità NIS2**

L'Operatore Economico dovrà progettare, configurare e realizzare gli interventi secondo criteri di modularità, scalabilità, resilienza, fault tolerance e sicurezza by design e by default, assicurando la continuità del servizio, la stabilità del piano di controllo e l'affidabilità del trasporto dei flussi video nel perimetro contrattuale.

Le tecnologie e i protocolli citati nel presente articolo costituiscono riferimenti tecnici o soluzioni preferenziali e non prescrizioni di marca o di prodotto, salvo i divieti espressamente indicati. Sono ammesse soluzioni equivalenti che assicurino almeno pari interoperabilità, sicurezza, prestazioni, manutenibilità e sostenibilità del ciclo di vita. Le scelte dovranno essere motivate nel progetto di dettaglio; per le componenti

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

legacy non compatibili dovranno essere documentati i limiti, le misure compensative e il rischio residuo.

## 5.1 Modello architetturale e domini

La topologia dovrà perseguire, in relazione alla criticità dei servizi e alle risorse comprese nel perimetro, ridondanza geografica e logica, percorsi alternativi e riduzione dei single point of failure. Il progetto dovrà distinguere almeno i seguenti domini:

- **Dominio di accesso/campo:** telecamere IP, encoder, switch industriali o outdoor, PoE, enclosure e sistemi di alimentazione.
- **Dominio di aggregazione:** nodi di zona o quartiere con funzioni di routing, controllo del traffico, applicazione delle policy e raccolta della telemetria.
- **Dorsale urbana:** collegamenti in fibra e/o radio tra i nodi di aggregazione, il data center e le centrali operative.
- **Dominio di management:** rete o segmenti dedicati alla gestione, accessibili soltanto da postazioni amministrative autorizzate e, ove previsto, da jump host.
- **Dominio applicativo:** VMS, NVR, storage, analytics, sistemi di autenticazione e piattaforme di gestione e sicurezza disponibili.
- **Dominio utente:** postazioni operative, sale controllo e accessi applicativi segregati dai domini infrastrutturali.

La rete target dovrà assicurare una separazione chiara tra dominio di gestione, dominio applicativo/VMS, dominio utente e ulteriori domini funzionali, limitando le interazioni non necessarie e rendendo verificabile il controllo degli accessi e dei flussi.

Nei livelli di core e aggregazione dovranno essere utilizzati i meccanismi di alta disponibilità e i percorsi alternativi supportati dalle componenti esistenti. Qualora l'hardware non consenta di eliminare un single point of failure, il progetto dovrà

|                                                                                   |                                                                                                                                  |                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p align="center"><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

esplicitarlo e indicare le misure di mitigazione. Ove utile e sostenibile, potranno essere proposte soluzioni ottiche dedicate, incluse tecnologie BiDi o equivalenti.

L'architettura dovrà essere dimensionata rispetto alle ipotesi di crescita approvate dalla Stazione Appaltante e dovrà privilegiare standard aperti e interoperabili, riducendo le dipendenze non necessarie da funzionalità proprietarie. Le piattaforme di supporto afferenti al dominio di management e al dominio applicativo (sistema di autenticazione, logging, gestione) dovranno essere ospitate in un ambiente virtualizzato (basato preferibilmente su Proxmox, come da infrastruttura della SA) installato e configurato dall'OE sull'hardware reso disponibile dalla SA.

## **5.2 Indirizzamento, modello Layer 2/Layer 3, discovery e sincronizzazione temporale**

Per la dorsale e i nodi di aggregazione dovrà essere privilegiata, ove compatibile con gli apparati e i servizi, una configurazione prevalentemente Layer 3, limitando le estensioni Layer 2 al necessario. Nei segmenti Layer 2 dovranno essere adottati Spanning Tree o meccanismi equivalenti per prevenire loop e instabilità.

Dovrà essere predisposto un piano di rinumerazione degli indirizzi non compatibili con la rete regionale per la pubblica amministrazione RUPAR. La gestione dell'indirizzamento dovrà utilizzare gli strumenti IPAM messi a disposizione dalla Stazione Appaltante o, in loro assenza, un registro strutturato e modificabile.

Ai fini dell'inventario, della ricostruzione topologica e del troubleshooting dovranno essere utilizzati LLDP o meccanismi equivalenti, ove supportati.

La sincronizzazione temporale dovrà essere affidabile e coerente sui domini infrastrutturali e applicativi mediante NTP o sorgenti equivalenti e, ove supportato, con meccanismi di autenticazione. La coerenza temporale dovrà essere adeguata all'analisi forense, consentendo correlazione degli eventi e garantendo la validità temporale delle registrazioni.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

### 5.3 Routing interno, routing esterno, overlay e interconnessioni

La scelta dei protocolli dovrà garantire convergenza controllata, prevedibilità operativa, interoperabilità multi-vendor, separazione dei domini, supporto alla ridondanza e protezione dell'infrastruttura di management. La dorsale e i nodi di aggregazione dovranno adeguare i percorsi in caso di guasto o variazione della topologia.

La rete dovrà essere organizzata gerarchicamente, limitando la propagazione non necessaria delle informazioni di instradamento. Dovranno essere definiti criteri coerenti per selezione dei percorsi, aggregazione delle reti, summarization, route filtering, controllo e autenticazione delle adiacenze, protezione del control plane e protocol policing.

Nei domini interni l'Operatore Economico dovrà proporre un protocollo IGP standard, interoperabile e supportato dagli apparati esistenti e dalla strategia IPv4. Sono ammesse, in funzione del contesto, soluzioni quali OSPFv2, OSPFv3 o equivalenti. L'impiego di eBGP, iBGP, MP-BGP o altri protocolli evoluti sarà ammesso soltanto quando motivato da multi-homing, separazione di domini amministrativi o specifiche esigenze di policy routing.

Dovranno essere evitate ridistribuzioni non controllate, route leaking non motivato, dipendenze circolari e configurazioni suscettibili di generare instabilità. Gli obiettivi di convergenza e ripristino saranno definiti nel progetto di dettaglio e verificati mediante prove documentate.

Le interconnessioni con reti esterne, operatori di telecomunicazioni, infrastrutture di trasporto, data center o siti remoti dovranno assicurare separazione logica, controllo dei percorsi e piena governabilità. In presenza di collegamenti multipli dovranno essere definiti priorità e criteri di commutazione, evitando propagazioni non autorizzate.

|                                                                                   |                                                                                                                   |                                                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

Le comunicazioni tra domini distinti dovranno essere motivate e sottoposte a specifiche policy. Eventuali overlay o sistemi di virtualizzazione dovranno garantire isolamento, interoperabilità, tracciabilità e semplicità di gestione, senza introdurre complessità non giustificate.

## **5.4 Multicast, qualità del servizio e trasporto dei flussi video**

Il trasporto dei flussi video dovrà essere progettato sulla base delle effettive modalità di acquisizione, distribuzione, registrazione, analisi e consultazione, considerando condizioni ordinarie e scenari di massimo carico, inclusi failover, esportazioni forensi o massive, aggiornamenti simultanei e registrazioni concorrenti.

Il multicast potrà essere adottato soltanto quando produca benefici misurabili e risulti sostenibile sotto il profilo operativo. Nei domini interessati dovranno essere utilizzati IGMP snooping o meccanismi equivalenti, ove supportati; PIM-SM o tecnologie equivalenti saranno ammessi solo nei casi tecnicamente giustificati.

Dovrà essere definita una QoS end-to-end sulle componenti che la supportano e nei punti in cui sia necessaria, distinguendo almeno traffico video in tempo reale, management, telemetria, sincronizzazione temporale, backup, aggiornamenti e accessi operativi. Per gli apparati non compatibili dovranno essere adottate le misure alternative praticabili.

Il dimensionamento di uplink, capacità di commutazione, buffer, code e meccanismi di regolazione dovrà basarsi su scenari realistici. I valori attesi di banda, latenza, jitter e perdita di pacchetti, le tolleranze e i metodi di prova saranno definiti a partire dalla baseline, approvati nel progetto di dettaglio e verificati nel piano dei test.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## 5.5 Segmentazione, controllo degli accessi e sicurezza di rete

La sicurezza dovrà fondarsi sulla separazione dei domini, sulla minimizzazione delle superfici di esposizione e sulla protezione del piano dati, del piano di controllo e del piano di gestione. Fermi restando i divieti di cui all'Art. 6, dovranno essere applicate almeno le seguenti misure:

- segmentazione Layer 3 mediante subnet, VRF o meccanismi equivalenti coerenti con l'architettura, distinguendo telecamere, management, VMS/NVR, operatori, manutenzione e servizi di supporto;
- policy enforcement point configurati secondo un modello deny-by-default, con abilitazione dei soli flussi necessari e documentati nella matrice delle comunicazioni;
- accesso alle funzioni di gestione esclusivamente da postazioni amministrative protette e autorizzate e, ove previsto, tramite jump host; gli accessi remoti dovranno essere temporanei, controllati e tracciati;
- protezione dei segmenti di accesso, ove sostenibile, mediante 802.1X; quando non applicabile, adozione di controlli compensativi quali port security, ACL, profili statici e blocco delle porte inutilizzate;
- misure di mitigazione Layer 2, ove supportate, per prevenire manipolazioni del traffico locale, instabilità e attacchi alle funzioni elementari di rete;
- autenticazione forte e MFA ove applicabili e supportate, segregazione dei profili privilegiati, gestione controllata delle credenziali, revisione periodica e rotazione dei segreti.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## 5.6 Hardening degli apparati e protezione del control plane

Le operazioni di hardening dovranno essere applicate agli apparati attivi, agli endpoint e ai sistemi di supervisione inclusi nel perimetro, tenendo conto delle funzionalità effettivamente supportate e della continuità del servizio. Dovranno essere previste almeno le seguenti attività:

- disabilitazione dei servizi e delle funzioni non necessari, inclusi, a titolo esemplificativo, Telnet, HTTP in chiaro, UPnP, discovery non essenziale, accessi cloud non autorizzati e protocolli legacy;
- amministrazione mediante protocolli e interfacce sicure quali SSH, HTTPS/TLS, SNMPv3 o soluzioni equivalenti; quando gli apparati non supportino protocolli moderni dovranno essere applicati segregazione, filtraggio e ulteriori controlli compensativi;
- separazione delle credenziali privilegiate per ruolo o funzione, controllo e tracciabilità degli accessi, revisione periodica e rinnovo secondo politiche coerenti con la criticità;
- backup delle configurazioni, cifratura ove prevista dalle politiche della Stazione Appaltante, versionamento, procedure di restore e verifica della recuperabilità;
- Control Plane Policing o misure equivalenti, autenticazione dei protocolli, controllo delle porte, logging di sicurezza e limitazione del traffico anomalo diretto alle componenti di controllo;
- vulnerability, patch e firmware management, verifica dello stato di supporto dei prodotti e documentazione delle componenti non più adeguatamente manutenibili.

Per gli apparati Axis, la Axis OS Hardening Guide costituisce riferimento tecnico. Il basic hardening dovrà essere applicato per quanto compatibile con modello, versione e funzioni in esercizio; l'extended hardening dovrà essere valutato congiuntamente alla Stazione Appaltante e applicato soltanto dopo verifica di

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

compatibilità. Restano applicabili, per quanto pertinenti, le linee guida AGID richiamate all'Art. 15.

## 5.7 Monitoraggio, logging e reporting

La soluzione dovrà integrare gli apparati e i sistemi inclusi nel perimetro con le piattaforme di gestione, monitoraggio e sicurezza messe a disposizione dalla Stazione Appaltante.

- integrazione con l'NMS o sistema equivalente disponibile, mediante polling sicuro e con frequenza commisurata alla criticità, raccogliendo le metriche supportate quali disponibilità, latenza, saturazione, errori di interfaccia, PoE, temperatura e sessioni di routing;
- raccolta centralizzata dei log provenienti dalle componenti che la supportano, inclusi apparati di rete, firewall, sistemi VPN, postazioni amministrative, VMS/NVR, sistemi operativi e componenti di autenticazione; tale servizio, se non già presente o non adeguatamente dimensionato, dovrà essere realizzato dall'OE mediante istanza dedicata sulla piattaforma hardware resa disponibile dalla SA.
- configurazione di syslog, soglie, alerting e correlazione mediante il SIEM o strumenti equivalenti esistenti; in assenza di tali piattaforme, produzione delle specifiche tecniche necessarie alla successiva attivazione;
- predisposizione, tramite gli strumenti disponibili, di viste o dashboard differenziate per esercizio, sicurezza e continuità del servizio;
- definizione nel progetto del periodo di conservazione dei log, da approvare dalla Stazione Appaltante in coerenza con esigenze operative, sicurezza, protezione dei dati e capacità di archiviazione disponibili.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## 5.8 Gestione del rischio, risposta agli incidenti e sicurezza della supply chain secondo la direttiva NIS 2

Le attività dovranno supportare, limitatamente al perimetro contrattuale, l'attuazione delle misure tecniche e organizzative individuate dalla Stazione Appaltante come applicabili ai sensi del decreto legislativo n.138/2024, della Determinazione ACN n. 379907/2025 e dei successivi atti attuativi.

- classificazione degli asset, analisi delle dipendenze, individuazione dei single point of failure, definizione degli scenari di minaccia e predisposizione di un piano di trattamento del rischio;
- procedure operative e playbook proporzionati agli scenari rilevanti, inclusi compromissione di telecamere, perdita di connettività, guasto di nodi, abuso di credenziali privilegiate, malware sui sistemi di gestione, perdita di storage e interruzione dei flussi;
- procedure di incident handling, contenimento, ripristino e raccolta delle evidenze tecniche, coerenti con il modello di esercizio e con le procedure dell'Ente;
- verifica, per i prodotti inclusi nel perimetro, dello stato di supporto, della disponibilità delle patch, della tracciabilità delle componenti software e dei canali di manutenzione remota, sulla base delle informazioni rese disponibili dai produttori e dalla Stazione Appaltante.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## 5.9 Resilienza e continuità operativa

La rete reingegnerizzata dovrà mantenere o ripristinare le funzioni essenziali secondo gli obiettivi approvati e le capacità di ridondanza effettivamente disponibili. Dovranno essere soddisfatti almeno i seguenti requisiti:

- attivazione automatica dei meccanismi di continuità supportati, limitando gli interventi manuali ai casi tecnicamente motivati;
- definizione, prima della migrazione, degli obiettivi di tempo di ripristino e perdita massima ammissibile dei dati (RTO e RPO) per le componenti interessate;
- disponibilità di backup validati e procedure per il ripristino delle configurazioni, il recovery dei servizi applicativi, la riattivazione dei flussi e l'eventuale ritorno alla configurazione precedente;
- esecuzione, prima della messa in produzione, di prove o simulazioni rappresentative e non distruttive di failover, riavvio, restore e rientro in esercizio; il piano dovrà inoltre indicare la periodicità raccomandata per le verifiche successive alla chiusura del contratto;
- produzione dei verbali di prova con scenari, tempi rilevati, disservizi, esiti e azioni correttive.

## Art. 6 Divieti e prescrizioni di sicurezza

È fatto divieto all'Operatore Economico, salvo espressa autorizzazione scritta della Stazione Appaltante, di:

- esporre direttamente su Internet telecamere IP, NVR, switch, router, apparati di campo, interfacce web o API di management e servizi di amministrazione remota;
- utilizzare credenziali di default, account condivisi privi di tracciabilità nominativa o configurazioni non documentate;

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

- attivare accessi remoti permanenti del fornitore senza segregazione, controllo degli orari, registrazione delle attività e approvazione preventiva;
- trasferire flussi video o dati di configurazione verso servizi cloud, IA o sistemi terzi non espressamente previsti dal contratto;
- eseguire modifiche in produzione prive di change management, backup preliminare e piano di rollback;
- utilizzare i dati rilevati dall'infrastruttura al di fuori dell'oggetto della procedura, con particolare riferimento a finalità di addestramento di strumenti di intelligenza artificiale.

## **Art. 7 Migrazione e continuità del servizio**

L'Operatore Economico dovrà eseguire la migrazione minimizzando l'impatto sull'operatività e assicurando il mantenimento o il rapido ripristino delle funzioni essenziali di trasporto, registrazione, visualizzazione, analisi e gestione dei flussi video in caso di guasto o indisponibilità di singoli componenti.

Per ciascuna finestra operativa dovrà essere predisposto un piano di intervento contenente almeno:

- prerequisiti, attività, ruoli, contatti e tempi previsti;
- backup preliminari e verifiche pre e post intervento;
- criteri di annullamento e procedure di rollback e ripristino.

Le attività che possano incidere sulla disponibilità dei flussi video o dei sistemi centrali dovranno essere preventivamente concordate con la Stazione Appaltante e svolte, di norma, in finestre compatibili con il presidio operativo.

La soluzione dovrà inoltre prevedere:

- attivazione automatica dei meccanismi di continuità, ove tecnicamente applicabile;

|                                                                                   |                                                                                                                                  |                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p align="center"><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

- backup validati e procedure documentate per il ripristino delle configurazioni, dei flussi dei siti remoti e dei servizi applicativi compresi nel perimetro contrattuale;
- definizione, d'intesa con la Stazione Appaltante, degli obiettivi di ripristino e dell'eventuale perdita massima ammissibile dei dati;
- verifica dei meccanismi di ridondanza, failover e ripristino previsti dal progetto.

Prima della messa in produzione dovranno essere eseguite e documentate, secondo il piano dei test approvato, le prove applicabili di failover, riavvio, restore, ripristino e rientro in esercizio. I relativi verbali dovranno riportare gli scenari verificati, i tempi rilevati, gli eventuali disservizi o anomalie e le azioni correttive necessarie.

## **Art. 8 Collaudo e accettazione**

Il collaudo tecnico-funzionale sarà eseguito dai tecnici della Stazione Appaltante con il supporto dell'Operatore Economico, sulla base di un piano dei test approvato prima della migrazione. Per ciascun requisito il piano dovrà indicare oggetto e campione di prova, configurazione iniziale, metodo, strumenti, valore atteso o tolleranza, evidenza da produrre e criterio di accettazione. I valori dovranno essere coerenti con la baseline, con i requisiti dei sistemi applicativi e con il progetto approvato.

- verifica di raggiungibilità, stabilità, topologia, segmentazione, isolamento e corretta applicazione della matrice dei flussi;
- verifica di routing, adiacenze, filtri, interconnessioni, riconvergenza, ridondanza e failover rispetto agli obiettivi approvati;
- verifica del trasporto dei flussi video, della registrazione, analisi e consultazione, della QoS, dell'eventuale multicast e dei parametri prestazionali negli scenari previsti;

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

- verifica dei controlli di accesso, autenticazione, hardening, protezione del control plane, logging, monitoraggio, alerting, sincronizzazione temporale e divieti di esposizione;
- verifica di backup, restore, rollback, ripristino, recovery dei servizi, procedure di risposta agli incidenti e continuità operativa;
- verifica della coerenza di inventario, configurazioni, documentazione as-built e procedure operative con lo stato reale dell'infrastruttura.

Gli esiti dovranno essere riportati in verbali di prova con scenari, misure, evidenze, disservizi, non conformità e azioni correttive. L'accettazione sarà subordinata alla chiusura delle non conformità che impediscano il rispetto dei criteri approvati e alla consegna dei deliverable previsti. Le limitazioni preesistenti, documentate nella baseline e accettate nel progetto di dettaglio, non costituiscono non conformità imputabili all'Operatore Economico.

## **Art. 9 Durata delle attività**

La conclusione delle prestazioni è determinata in 60 giorni naturali consecutivi decorrenti dal verbale di avvio, e in ogni caso non oltre la data del 31 Dicembre 2026.

I termini potranno essere sospesi, per la sola parte interessata, solo in caso di ritardi non imputabili all'Operatore Economico derivanti da mancata disponibilità di siti, apparati, credenziali o personale della Stazione Appaltante, ritardi nelle approvazioni, modifiche richieste dalla Stazione Appaltante o cause di forza maggiore. L'Operatore Economico dovrà segnalare tempestivamente l'impedimento e proporre l'aggiornamento del cronoprogramma concordato con la SA.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## **Art. 10 Obblighi e responsabilità delle parti**

### **10.1 Obblighi dell'Operatore Economico**

L'Operatore Economico assume, oltre agli obblighi previsti dalla legge e dal contratto, i seguenti obblighi specifici:

- eseguire il servizio a regola d'arte, con piena responsabilità tecnica delle scelte adottate, fatti salvi gli atti approvati dalla Stazione Appaltante;
- operare esclusivamente sul perimetro autorizzato e non apportare modifiche in produzione senza piano approvato, backup e rollback;
- osservare le politiche di sicurezza, le procedure di accesso ai siti e ai sistemi e le istruzioni in materia di protezione dei dati impartite dalla Stazione Appaltante;
- garantire tracciabilità delle modifiche, custodia dei backup e riservatezza di dati, configurazioni e credenziali;
- segnalare tempestivamente anomalie, vulnerabilità gravi, incidenti, indisponibilità, scostamenti dal perimetro e rischi di progetto;
- cooperare con DEC, RUP, ufficio ICT, responsabili della sicurezza e soggetti terzi coinvolti, nei limiti delle rispettive competenze;
- rispettare gli obblighi applicabili in materia di personale, CCNL, sicurezza sul lavoro e prevenzione dei rischi interferenziali, come disciplinati dagli atti di gara e dal contratto;
- garantire per tutta la durata del servizio la presenza nel gruppo di lavoro di almeno una figura con ruolo di Specialista Cybersecurity, con esperienza professionale documentata di almeno tre anni nella sicurezza di infrastrutture di rete

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## 10.2 Obblighi della Stazione Appaltante

La Stazione Appaltante, per consentire la corretta esecuzione delle prestazioni, si impegna a:

- mettere a disposizione la documentazione esistente, le credenziali e gli accessi necessari, nonché le politiche e le procedure applicabili;
- indicare i referenti tecnici e autorizzativi, assicurare l'accesso ai siti e coordinare gli operatori di telecomunicazioni e gli altri soggetti terzi di propria competenza;
- rendere disponibili, nei limiti del perimetro, apparati, licenze e piattaforme esistenti necessari all'integrazione;
- approvare o formulare osservazioni sugli elaborati e sulle finestre operative in tempi coerenti con il cronoprogramma;
- comunicare tempestivamente vincoli, indisponibilità o modifiche che possano incidere sulle attività.

## Art. 11 Procedura e Criteri per la scelta discrezionale del contraente nell'ambito dell'affidamento diretto

Nella valutazione delle proposte ricevute saranno considerati ai fini della valutazione complessiva e della motivazione della scelta gli elementi di seguito indicati che costituiranno il fondamento delle ragioni della scelta del contraente ai sensi dell'art. 17, comma 2 del D.Lgs. 36/2023:

- i contenuti della Relazione Metodologica Preliminare (Allegato B – Relazione metodologica preliminare); la relazione dovrà mantenere carattere metodologico e preliminare e non dovrà contenere un progetto esecutivo dell'intervento, configurazioni di dettaglio, indicazioni economiche o l'individuazione vincolante di specifici prodotti, apparati, tecnologie o

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

protocolli; l'elaborato è richiesto al fine di consentire alla Stazione Appaltante di acquisire elementi conoscitivi circa l'approccio metodologico, la capacità organizzativa e la concreta esperienza dell'Operatore Economico rispetto alla natura e alla complessità delle attività oggetto del futuro affidamento;

- congruità e convenienza complessiva del prezzo proposto per la realizzazione del servizio oggetto dell'Appalto;
- adeguatezza e sostenibilità del tempo proposto per la realizzazione delle prestazioni oggetto dell'appalto rispetto alla data indicata all'Art.9 del presente Capitolato e secondo quanto riportato nella Relazione Metodologica Preliminare (Allegato B – par. 10).

I suddetti elementi sono utilizzati dalla Stazione Appaltante ai fini dell'apprezzamento complessivo e della motivazione della scelta dell'operatore economico nell'ambito dell'affidamento diretto. Non è prevista l'attribuzione di punteggi o ponderazioni, l'applicazione di formule matematiche né la formazione di una graduatoria. La scelta dell'operatore economico resta discrezionale e sarà motivata ai sensi dell'art. 17, comma 2, del D.Lgs. 36/2023

## **Art. 12 Verifica di conformità e chiusura del servizio**

La verifica di conformità finale avverrà a seguito del completamento di tutte le prestazioni contrattuali, della chiusura delle non conformità e della consegna di tutti i deliverable previsti. Solo a seguito di tale verifica il servizio potrà considerarsi integralmente eseguito.

## **Art. 13 Trattamento dei dati, riservatezza e sicurezza delle informazioni**

L'Operatore Economico dovrà trattare dati video, log, credenziali, configurazioni e informazioni tecniche esclusivamente per l'esecuzione del contratto, secondo le istruzioni documentate della Stazione Appaltante, applicando i principi di minimizzazione, necessità, riservatezza, integrità e sicurezza by design e by default.

|                                                                                   |                                                                                                                                  |                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|  | <p align="center"><b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b></p> | <p><b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b></p> |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

Gli accessi dovranno essere limitati al personale autorizzato, tracciati e protetti; ove possibile dovranno essere utilizzati dati di prova o modalità che evitino l'accesso alle immagini.

L'Operatore Economico dovrà segnalare senza ingiustificato ritardo – entro un tempo massimo di 2 ore dalla rilevazione - violazioni, accessi indebiti o perdita di informazioni, cooperare nelle verifiche e nelle notifiche previste dalla normativa e, al termine delle attività, restituire o cancellare copie, credenziali e dati secondo le istruzioni della Stazione Appaltante, salvo obblighi di conservazione di legge. È vietata la duplicazione o il trasferimento dei dati su sistemi non autorizzati.

## **Art. 14 Disposizioni finali**

Per quanto non espressamente previsto nel presente Capitolato si applicano le disposizioni del codice dei contratti pubblici, della normativa civilistica e della normativa speciale vigente in materia di cybersicurezza, protezione dei dati, sicurezza delle reti e dei sistemi informativi e tutela della salute e sicurezza sul lavoro.

Gli aspetti amministrativi relativi, tra l'altro, a CCNL, costi della manodopera, oneri della sicurezza, revisione dei prezzi, garanzie, subappalto, termini di pagamento e penali sono disciplinati dagli ulteriori atti di gara e dal contratto.

Il progetto approvato può specificare modalità, valori e soluzioni tecniche, ma non può derogare ai requisiti contrattuali senza espressa autorizzazione e senza l'impiego degli strumenti previsti dalla normativa vigente. Ogni riferimento a una specifica tecnologia deve intendersi comprensivo di soluzioni tecnicamente equivalenti, nei limiti stabiliti all'Art. 5.

## **Art. 15 Riferimenti normativi e tecnici**

- Decreto legislativo 31 marzo 2023, n. 36, Codice dei contratti pubblici, nel testo vigente.
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS2).
- Decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555.

|                                                                                   |                                                                                                            |                                                                                                                       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | <b>Capitolato Speciale d'Appalto<br/>Reingegnerizzazione della rete di<br/>videosorveglianza cittadina</b> | <b>Dipartimento Innovazione e<br/>Servizi al Cittadino<br/>Servizio Trasformazione Digitale<br/>Comune di Trieste</b> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|

- Determinazione ACN n. 379907 del 19 dicembre 2025, relative specifiche di base, linee guida e successivi atti applicabili in materia NIS.
- LEGGE 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.
- Regolamento (UE) 2016/679, decreto legislativo 30 giugno 2003, n. 196, e linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video.
- Decreto legislativo 18 maggio 2018, n. 51, ove applicabile ai trattamenti effettuati dalle autorità competenti per finalità di prevenzione, indagine e accertamento di reati.
- Decreto legislativo 9 aprile 2008, n. 81, con particolare riferimento agli obblighi connessi ai contratti d'appalto e ai rischi interferenziali.
- Axis OS Hardening Guide – Basic Hardening: <https://help.axis.com/it-it/axis-os-hardening-guide#basic-hardening>
- Axis OS Hardening Guide – Extended Hardening:  
<https://help.axis.com/it-it/axis-os-hardening-guide#extended-hardening>
- AGID, “Linee Guida per la configurazione per adeguare la sicurezza del software di base”, Capitolo 5 “Best practices per adeguare e mantenere la sicurezza del software di base”, ultima versione disponibile.

**La Dirigente**

**Servizio Trasformazione Digitale**

Dott.ssa Giannina Ceschin