CAPITOLATO TECNICO

GARA EUROPEA A PROCEDURA APERTA PER L'AFFIDAMENTO DEI SERVIZI RELATIVI ALL'ATTUAZIONE DEL PROGETTO DENOMINATO "SecurityAN" - FINANZIATO CON FONDI NEXT GENERATION EU – PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 1 – COMPONENTE 1 "DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA P.A." – INVESTIMENTO 1.5 "CYBERSECURITY" – M1C1I1.5.

CUP **G96G23000210006**

CIG **B904D9493C**

Sommario

1. PREMESSA E FINALITÀ DELLA FORNITURA

1.1. Contesto di Riferimento

Il Comune di Giugliano in Campania, nel quadro del suo percorso di trasformazione digitale e in ottemperanza alle direttive nazionali in materia di sicurezza cibernetica per la Pubblica Amministrazione, intende potenziare le proprie difese perimetrali e interne, migliorare la gestione delle identità privilegiate e dotarsi di una capacità di monitoraggio proattivo delle minacce informatiche. L'infrastruttura IT dell'Ente è un asset strategico per l'erogazione dei servizi ai cittadini e deve essere protetta con tecnologie e processi all'avanguardia.

1.2. Obiettivi Strategici

L'affidamento oggetto del presente capitolato mira a conseguire i seguenti obiettivi:

- **Riduzione del Rischio Cibernetico:** mitigare i rischi derivanti da minacce quali ransomware, phishing, accessi non autorizzati e data breach.
- **Innalzamento del Livello di Sicurezza:** adottare tecnologie leader di mercato per la protezione della rete, il controllo degli accessi utilizzando sistemi ZTNA e la gestione dei privilegi.
- **Compliance Normativa:** Assicurare la conformità al Regolamento (UE) 2016/679 (GDPR), alle Misure Minime di Sicurezza di AgID e alle raccomandazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN).
- **Visibilità e Controllo:** Ottenere una visibilità completa sugli asset connessi alla rete e un controllo granulare sugli accessi, in particolare quelli amministrativi.
- **Capacità di Rilevamento e Risposta:** dotarsi di un servizio di monitoraggio specializzato (SOC) in grado di rilevare e gestire gli incidenti di sicurezza in modo tempestivo.

1.3. Riferimenti Normativi e Best Practice

L'offerta tecnica dovrà essere conforme e ispirarsi ai seguenti riferimenti:

- Decreto Legislativo 36/2023 (Codice dei Contratti Pubblici) e s.m.i.
- Regolamento (UE) 2016/679 (GDPR).

- Direttiva NIS (UE) 2016/1148 e relativo recepimento nazionale.
- Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (AgID).
- Framework Nazionale per la Cybersecurity e la Sicurezza Informatica (ACN).
- Standard internazionali ISO/IEC 27001, ISO/IEC 27002.

2. OGGETTO DELL'APPALTO

2.1. Struttura della Fornitura

L'appalto è costituito da un **Lotto Unico indivisibile** al fine di garantire la massima integrazione tra le componenti tecnologiche e l'unicità della responsabilità gestionale e di supporto. Il lotto comprende le seguenti macro-componenti dettagliate nei capitoli a seguire.

1. Fornitura hardware e software.
2. Servizi professionali di installazione, configurazione, personalizzazione e messa in esercizio (deployment).
3. Servizio di monitoraggio SOC 8x5.
4. Servizio di manutenzione e supporto tecnico per l'intera durata contrattuale.
5. Servizio di formazione in e-learning per il personale non specialistico.

2.2. Durata del Contratto

La durata del contratto è fissata con scadenza al 15 marzo 2026, fatte salve proroghe al PNRR stabilite da Enti sovraordinati.

3. LOTTO UNICO – DESCRIZIONE TECNICA E FUNZIONALE

L'offerente dovrà presentare una soluzione "chiavi in mano" che integri le seguenti componenti.

3.1. Componente: Fornitura e Deployment di Next-Generation Firewall (NGFW)

La soluzione proposta dovrà essere basata su tecnologia **Forcepoint Next-Generation Firewall** e prevede un'architettura funzionale di sicurezza richiesta basata su un'infrastruttura distribuita e ridondata, con componenti centralizzati per la gestione e

raccolta log, e apparati NGFW localizzati presso le sedi del cliente. L'intera piattaforma è amministrata attraverso un **Security Management Center (SMC)** configurato in modalità **Active/Standby**, al fine di garantire **continuità operativa e alta disponibilità** della gestione centralizzata. Nell'insieme la soluzione dovrà garantire e prevedere:

- **apparati NGFW Forcepoint** perimetrali e datacenter;
- **licenze di funzionalità avanzate** (Advanced Malware Detection & Protection, URL Filtering) e relative sottoscrizioni software;
- **security Management Center (High Availability)** per la gestione centralizzata;
- progettazione e **definizione delle policy di sicurezza**, suddivise per zone, livelli di rischio e requisiti applicativi;
- installazione fisica, configurazione logica, clustering e integrazione in rete;
- collaudo funzionale e di performance;
- training on the Job per il personale del Cliente;
- documentazione tecnica completa (Run-Book, Policy Design Document, As-built, piani di test, manuali operativi);
- supporto specialistico post-attivazione e gestione RMA.

3.3. Componente: Fornitura e Deployment di una Soluzione PAM (Privileged Access Management)

La soluzione proposta dovrà essere basata sulla piattaforma **CyberArk Core Privileged Access Security**. Nell'insieme la soluzione dovrà garantire e prevedere i servizi di seguito descritti ed il relativo progetto per il deployment.

- **Enterprise Password Vault (EPV):** Un vault digitale sicuro per l'archiviazione centralizzata e la gestione (rotazione automatica, controllo accessi) delle credenziali privilegiate (es. administrator di Windows, root di Linux, account di servizio, credenziali di apparati di rete).
- **CyberArk Policy Manager (CPM):** Scanner per la procedura di Discovery automatica degli account.

- **Privileged Session Manager (PSM):**
  - Isolamento completo delle sessioni privilegiate tramite un proxy sicuro, senza esporre la credenziale all'utente finale.
  - Monitoraggio in tempo reale delle sessioni con possibilità di terminazione immediata.
  - Registrazione video completa e indicizzata di tutte le attività svolte durante la sessione privilegiata, creando un audit trail inoppugnabile.
- **Gateway HTML5:** La soluzione deve prevedere l'accesso sicuro ad una macchina target tramite un gateway HTML5.
- **Threat Analytics:** consente di identificare comportamenti sospetti e dannosi di utenti privilegiati all'interno dell'organizzazione e di proteggere l'ambiente da minacce note e sconosciute.
- **Secrets Manager**: consente di protegge l'accesso privilegiato alle credenziali che si verificano nelle connessioni da sistema a sistema (spesso definite anche "machine to machine" o "app to app").
- **Business**-Critical password: in caso di eventuale blocco della rete alla password Vault, si deve disporre di un approccio che garantisce l'esecuzione delle applicazioni Business Critical.

3.3.2. Requisiti di Architettura, di progetto e integrazione

- La soluzione dovrà essere installata on-premise in una rete segregata (vaulting network) secondo le best practice del vendor.
- Dovrà essere garantita la cifratura dei dati at-rest e in-transit.
- Dovrà essere implementato un workflow di approvazione per l'accesso a credenziali particolarmente critiche (dual control).
- Integrazione con SIEM, Mail Server, Monitoraggio, Backup, altro se necessario
- Utenti privilegiati interni da considerare 25
- Sistemi target ipotesi di 100 max

- Account privilegiati, complessivi, ipotesi di 1000 max
- La soluzione dovrà essere progettata per integrarsi con il resto delle componenti di sicurezza

3.4. Componente: Erogazione di Servizio SOC (Security Operation Center) 8x5

L'offerente dovrà fornire un servizio di SOC gestito per il monitoraggio dell'intera infrastruttura di sicurezza fornita e degli altri asset critici dell'Ente. Si consideri oltre all'infrastruttura descritta, un numero di utenti attivi presso l'ente pari a circa 300 unità.

3.4.1. Descrizione del Servizio

- **Orario di Servizio:** Lunedì-Venerdì, dalle 9:00 alle 18:00 (festività escluse).
- **Proporre una opzione per un servizio H24-**7/7
- **Personale:** Il servizio dovrà essere erogato da analisti di sicurezza certificati.
- **Piattaforma:** L'Offerente dovrà utilizzare una propria piattaforma SIEM (Security Information and Event Management) di classe enterprise. Saranno preferite soluzioni scalabili che utilizzano l'AI per la riduzione dei costi e il miglioramento del servizio
- **Attività Principali:**
  - Monitorare in tempo reale eventi e flussi di rete attraverso strumenti SIEM avanzati;
  - Rilevare e rispondere tempestivamente a minacce informatiche mediante processi di Incident Detection & Response;
  - Garantire la conformità normativa attraverso la gestione e la reportistica degli eventi di sicurezza;
  - Analizzare e correlare i dati provenienti da diverse fonti aziendali per individuare attività sospette;
  - Automatizzare e orchestrare le risposte agli incidenti mediante strumenti SOAR;
  - Gestire le vulnerabilità attraverso analisi periodiche e strumenti dedicati;

- Eseguire analisi forensi per determinare le cause e gli impatti degli incidenti di sicurezza;
- Fornire una dashboard centralizzata che permetta di visualizzare lo stato di sicurezza aziendale in tempo reale;
- Generare reportistica dettagliata, con:
    - Report tecnico settimanale: contenente informazioni dettagliate sugli eventi di sicurezza, le minacce rilevate e le azioni intraprese.
    - Report manageriale mensile: con un riepilogo strategico degli eventi più rilevanti, le tendenze di sicurezza e raccomandazioni per la governance della sicurezza informatica.

3.4.2. Onboarding, Log Management e integrazione

- L'Offerente garantire il corretto on boarding e dovrà definire un piano per la raccolta dei log dalle seguenti fonti (e di quanto altro necessario allo scopo definito in fase iniziale):
    - NGFW Forcepoint.
    - Soluzione PAM CyberArk.
    - Domain Controllers.
    - Principali server (Windows/Linux).
    - Switch di rete e Access Point.
- I log dovranno essere conservati per un periodo minimo secondo le normative vigenti

3.4.3. Evoluzione continua e miglioramenti

Sviluppo e Aggiornamento di nuovi use cases, il fornitore deve definire una metodologia per l'identificazione proattiva di nuove regole di detection in base ai nuovi scenari di minaccia, in particolare:

- Mappare i casi d'uso alle tecniche MITRE ATT&CK.

- Utilizzare la mappatura MITRE ATT&CK per identificare aree scoperte e suggerire al cliente le attività per ridurle.
- Documentare e validare ogni nuova regola prima della messa in esercizio.

3.4.4. Automazioni e Playbook

IL fornitore deve progettare e mantenere playbook di automazione per:

- Auto-triage degli alert
- Notifiche e azioni di mitigazione automatica o semi-automatica degli use cases concordati con il cliente
- Altre automazioni suggerite dal fornitore
- Documentare i Playbook e implementare versioning e test prima della messa in esercizio.

3.5. Componente: Servizio di formazione in e-learning

Si richiede all'Offerente un servizio in modalità SaaS che consenta l'erogazione di formazione di Cyber e che garantisca i seguenti elementi:

- Caratteristiche evolute per migliorare il rendimento dell'apprendimento idoneo alle organizzazioni pubbliche.
- Configurabilità del percorso formativo per singolo utente o per gruppi.
- Monitoraggio e avanzamento dell'apprendimento.
- Contenuti multimediali e testuali, con test finali di apprendimento
- Simulatore di campagne di Phishing in grado di produrre risultati efficaci mediante metodologia di addestramento esperienziale
- Presenza di funzionalità di Gamification che riteniamo possa migliorare dell'apprendimento

4. SERVIZI PROFESSIONALI E MODALITÀ DI ESECUZIONE

4.1. Project Management

L'offerente dovrà nominare un Project Manager e/o un Service Manager che fungerà da referente unico per la Stazione Appaltante. Il PM/SM sarà responsabile della stesura del piano di progetto (diagramma di GANTT), del coordinamento delle attività, della gestione dei rischi e della reportistica periodica sullo stato di avanzamento lavori (SAL).

Le seguenti attività sono esemplificative (non esaustive, si invita l'Offerente a indicare ogni ulteriore elemento di miglioramento per la corretta implementazione) dell'implementazione della completa infrastruttura HW / SW e servizi di sicurezza, come da scope di codesta gara. Si potrà descrivere l'attività di deploy, a seconda della preferenza dell'Offerente: in una singola ed esaustiva progettazione che raccoglie tutte le componenti descritte in precedenza o procedendo per singola componente tecnologica.

4.2. Fasi di Implementazione e integrazione

Il progetto dovrà seguire le seguenti macro-fasi per ciascuna componente tecnologica e quindi anche se non esplicitamente riportato conterrà riferimenti alla completa delivery della soluzione e pertanto si riferisce a SOC, PAM, e NG-FW.

1. **Analisi e Design:** workshop con il personale del Comune per definire l'architettura dettagliata, le policy di sicurezza e i casi d'uso. Produzione di un documento di High-Level Design (HLD) e Low-Level Design (LLD). Attività di design e setup del servizio SOC, PAM
2. **Installazione e Configurazione:** installazione fisica e/o virtuale degli apparati e del software, configurazione di base e di rete, raccolta dei log e setup del sistema di raccolta per l'integrazione con il SOC di tutte le componenti da monitorare.
3. **Implementazione Policy e Integrazione:** configurazione delle policy di sicurezza specifiche (regole firewall, policy NAC, policy PAM), integrazione tra le varie componenti, integrazioni e raccolta dei log, configurazioni delle notifiche e degli alert su tutta l'infrastruttura compresi SOC.

4. **Test e Tuning:** fase di test funzionale e di sicurezza, User Acceptance Test (UAT) con il personale del Comune e tuning delle configurazioni.
5. **Go-Live e Handover:** Messa in produzione della soluzione e passaggio delle consegne.

5. SERVIZI DI MANUTENZIONE E SUPPORTO TECNICO

Per tutta la durata contrattuale, l'Offerente dovrà fornire un servizio onnicomprensivo che includa:

5.1. Supporto Hardware (RMA)

- Per tutte le componenti hardware fornite, è richiesto un servizio di sostituzione anticipata delle parti guaste (Advanced Replacement) in coordinamento con il vendor.
- **SLA: Next Business Day (NBD)**. La parte sostitutiva deve essere consegnata presso la sede del Comune entro il giorno lavorativo successivo alla conferma del guasto.
- Tutto quanto necessario alla corretta sostituzione degli apparati e alla ripartenza del servizio.
- **Diagnostica remota** o on site per identificazione del guasto.
- Coordinamento della spedizione del nuovo apparato e dell'eventuale ritiro del guasto.

5.2. Supporto Software (Maintenance)

- Diritto a tutti gli aggiornamenti software (major, minor release) e patch di sicurezza rilasciati dai vendor (Forcepoint, CyberArk).
- Accesso alle firme di sicurezza aggiornate (IPS, Antivirus, Application Control, etc.).

6. FIGURE PROFESSIONALI E CERTIFICAZIONI RICHIESTE

L'offerente dovrà dimostrare di disporre di un team di progetto, e un team SOC con le seguenti figure e competenze, allegando i CV anonimizzati e il dettaglio degli ID delle certificazioni.

6.1. Project Manager / Service Manager

Principali responsabilità:

- Definisce con il personale della Committente il piano di lavoro, l'effort delle attività e il monitoraggio dei progressi mediante riunioni periodiche
- Analizza e definisce i flussi di lavoro per l'implementazione dei processi.
- Elabora le procedure operative per la gestione dei servizi.
- Analizza e definisce le metodologie per il calcolo degli indicatori di performance e di rischio (KPI / KRI).
- Pianifica e monitora lo stato del servizio sulla base delle attività pianificate.
- Coordina il personale tecnico in tutte le fasi del servizio.
- Responsabile del controllo e del reporting in merito alla qualità dei servizi erogati.
- Definisce le attività di servizio, comprese quelle relative ai processi e alle strutture interne (verbalizzazione delle riunioni, preparazione del materiale per i SAL periodici, ecc...).
- Responsabile di gestione dei rapporti anche con eventuali terze parti indicate dal cliente.

Conoscenze e competenze specifiche:

- Conoscenza approfondita delle metodologie di Project Management e Service Management, in particolare del Framework ITIL.
- Esperienza approfondita nello svolgimento di attività in progetti ICT, quali:
  - Analisi e definizione dei processi
  - Elaborazione delle procedure operative
  - Capacità di analizzare le esigenze funzionali dell'utente, redigendo documenti per la modellazione (es. UML, Data Flow), con i principali strumenti software (es. Visio, RUP, Argo, UML)
- Esperienza nella pianificazione, coordinamento e gestione di progetti SOC, Cybersecurity e/o SIEM e gestione dei servizi.

- Tecniche di controllo e gestione dei rischi.
- Esperienza di coordinamento e motivazione di gruppi di lavoro eterogenei.
- Gestione di grandi progetti, coordinamento e controllo delle attività.
- Pianificazione dei tempi e delle risorse.
- Gestione delle relazioni sullo stato di avanzamento.

6.2. Security Manager

Esperienza e competenze specifiche:

- Conoscenza degli Standard di sicurezza (ISO27001, NIST, ecc.).
- Conoscenza del quadro normativo sulla protezione dei dati personali.
- Conoscenza delle metodologie di Project Management.
- Conoscenza di architetture e soluzioni di sicurezza ICT.
- Conoscenza delle tecniche e tattiche di attacco in ambito cyber security

Certificazioni (almeno una, fortemente premiante):

- CISSP, CISM, OSCE, OSCP, L.A. ISO 27001, PMP, ITIL, ISO 22301

6.3. Security Architect

Conoscenze e competenze specifiche:

- Profonda conoscenza delle minacce informatiche e metodologie di attacco.
- Conoscenze degli strumenti di Vulnerability Assessment e Penetration Testing.
- Conoscenza approfondita dell'analisi degli incidenti di sicurezza e della gestione delle minacce.
- Conoscenza delle tecniche di hardening.
- Comprovata conoscenza dei sistemi operativi, protocolli di rete e infrastruttura di rete.
- Redazione specifiche tecniche di progetto.
- Definizione dei pattern architetturali.
- Conoscenza approfondita di architetture e soluzioni di sicurezza ICT.

- Conoscenza degli Standard di sicurezza (ISO27001, NIST, CoBIT, Common Criteria, ecc.).

Certificazioni (almeno una, fortemente premiante):

Security+, CEH, L.A. ISO 27001, ISO 22301, CISSP

6.4. Senior Security Engineer

- **Esperienza e competenze specifiche:** Almeno 7 anni di esperienza nel deployment di soluzioni di network security e identity management.
- **Certificazioni Tecniche (obbligatorie):**
  - Certificazione ufficiale Forcepoint a livello tecnico/amministrativo (es. Forcepoint Certified Technical Professional - NGFW).
  - Certificazione ufficiale CyberArk a livello tecnico/deployment (es. CyberArk Certified Delivery Engineer - CDE).
- **Certificazioni (almeno una, fortemente premiante):** CISSP, CISM, CompTIA Security+.

6.3. Security Specialist

Conoscenze e competenze specifiche:

- Conoscenza delle minacce informatiche e delle metodologie di attacco.
- Conoscenza dell'analisi degli incidenti di sicurezza e della gestione delle minacce.
- Conoscenza dei sistemi operativi, protocolli di rete e infrastruttura di rete.
- Conoscenza delle tecniche di bonifica.
- Almeno 5 anni di esperienza come analista in un SOC.

Certificazioni (almeno una, fortemente premiante):

- OSCP, CCNA, LPI, Security+ o specifiche certificazioni dei vendor.

7. MODALITÀ DI VERIFICA E COLLAUDO

Al termine delle attività di implementazione, si procederà con il **Collaudo Tecnico Funzionale**. Il collaudo sarà presieduto da una commissione nominata dalla Stazione Appaltante e verificherà la piena rispondenza della fornitura a tutti i requisiti espressi nel presente capitolato. L'Offerente dovrà produrre un piano di collaudo (test-case) da sottoporre ad approvazione. L'esito positivo del collaudo, formalizzato tramite apposito verbale, darà inizio alla decorrenza del contratto di manutenzione e servizio SOC.

8. COORDINAMENTO, MONITORAGGIO E VALUTAZIONE

L'Amministrazione comunale si riserva le funzioni di programmazione delle attività, nonché la facoltà di dettare istruzioni e direttive per il corretto svolgimento delle stesse. L'O.E. selezionato si impegna ad inviare la scheda di monitoraggio dei servizi erogati, la relazione intermedia e finale sull'attività svolta secondo i criteri e le modalità comunicate dalle linee guida PNRR di riferimento; ad aggiornare inoltre in maniera tempestiva la banca dati garantendone l'attendibilità e la veridicità dei dati inseriti, avendone designato un responsabile. A tal proposito dovrà aderire al-la rete informatica gestita dal Servizio Centrale assicurando, in conformità alla normativa vigente per la privacy, la disponibilità dei mezzi tecnici necessari al collegamento informatico. L'O.E. selezionato si obbliga, inoltre, in ottemperanza a decreti e circolari vigenti, alla gestione amministrativa del progetto, alla tenuta di ogni formalità di carattere amministrativo, contabile e fiscale; si impegna infine a trasmettere alla Città di Giugliano in Campania tutta la documentazione necessaria alla rendicontazione eco-nomica delle attività di progetto secondo i tempi, i criteri e le modalità comunicate dal Servizio Centrale.

9. OBBLIGHI DELL'AGGIUDICATARIO

L'ente che risulterà affidatario sarà obbligato a rendere immediatamente noto alla Amministrazione Comunale le seguenti situazioni in cui dovesse incorrere:

- eventuale ispezione in corso, sia ordinaria sia straordinaria, da parte degli Enti all'uopo deputati e i risultati delle stesse ispezioni, attraverso la trasmissione dello spe-

cifico verbale, con precisa notifica al Servizio Politiche di Integrazione e Nuove Citta-dinanze, in caso di contestazioni, di ogni tipo di irregolarità riscontrate ed eventuali conseguenti diffide;

- modifica della ragione sociale del soggetto; cessione dello stesso; cessazione dell'attività;
- concordato preventivo, fallimento; stato di moratoria e di conseguenti atti di sequestro o pignoramento.

L'ente affidatario dovrà provvedere successivamente all'affidamento:

- a depositare tutte le spese contrattuali, le quali cederanno per intero a suo cari-co;
- a depositare cauzione definitiva nella misura indicata al successivo art.12.

L'ente affidatario si impegna a:

- erogare il servizio sulla base di quanto stabilito nel contratto;
- svolgere le attività oggetto del contratto in coordinamento con la Città di Giugliano in Campania;
- rispettare la normativa comunitaria, nazionale e regionale vigente per le materie oggetto del presente appalto;
- garantire l'adempimento di tutti gli obblighi assicurativi e previdenziali previsti dalla normativa vigente a favore dei propri addetti alla realizzazione dell'attività;
- garantire che le strutture e le attrezzature messe a disposizione per lo svolgi-mento delle attività corrispondano ai requisiti delle vigenti normative in materia di idoneità e sicurezza;
- relazionare periodicamente e puntualmente sulle attività svolte;
- relazionare sulla conclusione delle attività evidenziando i servizi erogati, le problematiche emerse, le soluzioni adottate, e quant'altro necessario a quantificare e qualificare il servizio fornito;
- garantire che gli operatori siano idonei alle mansioni di cui al presente Capitolato;
- garantire per tutta la durata del progetto il contenimento del turn over, fornendo adeguate motivazioni e giustificazioni ad un eventuale avvicendamento e garantendo la

sostituzione con operatori in possesso dei titoli e delle esperienze di cui al presente capitolato;

- garantire l'immediata sostituzione dell'operatore assente per qualsiasi motivo;
- farsi esclusivo carico degli oneri assicurativi e previdenziali e quant'altro necessario all'impiego dell'operatore nelle attività di specie senza che possa null'altro opporsi all'Amministrazione Comunale in ordine alla normativa regolante il presente rapporto;
- farsi carico degli obblighi relativi alle vigenti disposizioni in materia di protezione dell'impiego e di condizioni di lavoro applicabili nel corso dell'esecuzione del con-tratto (sicurezza e protezione dei lavoratori, nonché delle condizioni di lavoro).

L'ente affidatario dovrà stipulare un'apposita polizza di assicurazione per la responsabilità civile del valore non inferiore a 500.000,00 euro a sinistro, con oneri a suo intero ed esclusivo carico, per la tutela degli utenti e di terzi, da eventuali danni provocati a persone e beni dal personale impiegato nell'espletamento del servizio, con ampia e totale liberazione dell'Amministrazione Comunale da ogni responsabilità.

10. MODALITÀ DI PAGAMENTO

I pagamenti relativi alle prestazioni finanziati con fondi trasferiti saranno subordinati all'effettivo introito delle somme finanziate. La Città di Giugliano in Campania provvederà alla liquidazione delle somme spettanti entro 30 giorni dalla presentazione della fattura elettronica corredata dalla documentazione attestante le spese effettivamente sostenute per la realizzazione dei servizi oggetto del presente appalto. Eventuali con-testazioni ed irregolarità sospenderanno tale termine. In caso di raggruppamento temporaneo d'impresa si richiede fatturazione separata sulla base delle quote di attività che ciascun ente dovrà svolgere così come dichiarato nell'istanza di partecipazione e indicato nell'atto costituivo del raggruppamento.

Sulla fattura dovrà essere specificato:

- l'oggetto dell'appalto;
- il codice identificativo gara (CIG **B904D9493C**);
- gli estremi della D.D. di impegno della spesa;

- il periodo di imputazione della spesa per la quale si chiede la liquidazione;
- il Codice Identificativo Univoco ……...

Il pagamento verrà disposto da parte dell'ufficio competente, a seguito di verifica di regolarità del/dei D.U.R.C. (documento unico di regolarità contributiva).

La Città di Giugliano in Campania potrà rivalersi, per ottenere la rifusione di eventuali danni contestati, il rimborso di spese ed il pagamento di penalità, mediante ritenuta da operarsi in sede di pagamento dei corrispettivi.

11. RAPPORTI CON L'ENTE LOCALE

Tra la Città di Giugliano in Campania e il soggetto attuatore selezionato sarà stipulato apposito contratto per disciplinare la realizzazione, gestione ed erogazione del servizio oggetto del presente capitolato e del disciplinare. Il contratto conterrà in dettaglio gli impegni e gli oneri intercorrenti tra le parti.

In ogni caso, il soggetto attuatore e gestore si impegna, nelle more dei controlli previsti dalle leggi vigenti, ad attivare i servizi di accoglienza integrata a far data dalla notifica dell'aggiudicazione, comunicando alla Città di Giugliano in Campania, con apposita nota, la data effettiva di avvio attività.

A seguito della comunicazione della proposta di aggiudicazione, è fatto obbligo di produrre garanzia definitiva, mediante polizza fideiussoria bancaria o assicurativa, ai sensi dell'art 117 del Codice.

Il contratto potrà essere revocato al venir meno dei requisiti indicati, sulla scorta di un processo di valutazione continua della qualità delle prestazioni rese.

La stipula di detto contratto sarà comunicata al soggetto attuatore con apposita comunicazione da parte della Città di Giugliano in Campania, dietro presentazione di idonea documentazione richiesta.

Qualunque danno dovesse derivare a persone, comprese quelle che operano presso la sede operativa, od a cose, causato dall'operatore afferente all'affidatario nell'espletamento delle attività del Progetto, dovrà intendersi, senza riserve o eccezioni, intera-mente a carico dell'affidatario medesimo.

In caso di danni arrecati a terzi, l'affidatario sarà comunque obbligato a darne immediata notizia al competente Servizio comunale, fornendo per iscritto dettagliati particolari.

12. TRATTAMENTO DEI DATI PERSONALI

L'O.E. aggiudicatario assume la qualifica di responsabile esterno del trattamento dati per le operazioni di trattamento connesse all'attuazione degli interventi di propria competenza. Il responsabile del trattamento (nel nuovo regolamento europeo data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR) e nel caso specifico è la Città di Giugliano in Campania, rappresentata dal Commissario in qualità di legale rappresentante dell'Ente.

Il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, para-grafo 2, GDPR).

Ha l'obbligo di garantire la sicurezza dei dati. Egli deve adottare tutte le misure di sicurezza adeguate al rischio (art. 32 GDPR), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, dovrà inoltre garantire la riservatezza dei dati, vincolando i dipendenti, dovrà informare il titolare delle violazioni avvenute, e dovrà occuparsi della cancellazione dei dati alla fine del trattamento.

Sia il titolare del trattamento che il responsabile, sono tenuti ad attuare le misure tecniche ed organizzative tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mediante le misure di sicurezza utili per ridurre i rischi del trattamento, quali la pseudonimizzazione e la cifratura dei dati personali, la capacità di as-sicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare

regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre, il responsabile ha l'obbligo di avvisare, assistere e consigliare il titolare. Dovrà, quindi, consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dal titolare del trattamento, dovrà avvisare il titolare se ritiene che un'istruzione ricevuta viola qualche norma in materia, dovrà prestare assistenza al titolare per l'evasione delle richieste degli interessati, dovrà avvisare il titolare in caso di violazioni dei dati, e assisterlo nella conduzione di una valutazione di impatto (DPIA). L'aggiudicatario si impegna a non utilizzare i dati personali oggetto dei trattamenti delegati per altro trattamento se non su richiesta scritta dell'Ente locale.

13. DEPOSITO CAUZIONALE

A garanzia dell'esatto adempimento degli obblighi assunti a seguito dell'aggiudicazione dell'appalto, l'O.E. aggiudicatario, prima della stipula del relativo contratto, dovrà prestare, ai sensi dell'art. 117 del Codice "garanzia definitiva" con le modalità di cui all'art. 106, commi 2 e 3 del Codice, nella misura stabilita dal richiamato art. 117. Alla garanzia definitiva si applicano le riduzioni previste dall'art. 106, comma 8 per la garanzia provvisoria.

Lo svincolo della cauzione avverrà ai sensi dell'art. 117 comma 8 del Codice e, in particolare, lo svincolo è automatico, senza necessità di nulla osta del committente, con la sola condizione della preventiva consegna all'istituto garante, da parte dell'appaltatore, degli stati di avanzamento dei lavori o di analogo documento, in originale o in copia autentica, attestanti l'avvenuta esecuzione. Tale automatismo si applica anche agli appalti di forniture e servizi.

14. CONTESTAZIONE DISSERVIZI E PROCEDURE DI ADDEBITO

Il Dirigente il VI Settore è deputato a contestare all'affidatario i disservizi che si verificassero durante il periodo contrattuale. Le contestazioni di detti disservizi dovranno

essere sempre comunicate per iscritto al rappresentante dell'affidatario che avrà cinque giorni di tempo dalla ricezione della contestazione per controdedurre.

Ove le controdeduzioni non fossero ritenute valide e giustificative dal responsabile sopra nominato, il medesimo provvederà all'applicazione di una penalità su ogni contestazione, non inferiore a € 200,00 (duecento euro) e non superiore a € 1.000,00 (mil-le euro), secondo la gravità dell'inadempienza.

Il soggetto affidatario ha l'obbligo, inoltre, di adottare nella realizzazione delle attività oggetto del presente Capitolato Speciale d'Appalto, tutte le cautele necessarie per garantire l'incolumità degli operatori, dei beneficiari e di terzi. In caso di danni a persone o cose, la responsabilità civile è a carico del soggetto affidatario, intendendosi integralmente sollevata la Città di Giugliano in Campania.

15. RECESSO UNILATERALE

L'Amministrazione comunale ha facoltà di recedere in qualunque momento dal contratto ai sensi dell'art.123 del Codice, *"purché tenga indenne l'appaltatore mediante il pagamento dei lavori eseguiti o delle prestazionirelative ai servizi e alle forniture eseguiti nonché del valore dei materiali utili esistenti in cantiere nel caso di lavori o in magazzino nel caso di servizi o forniture, oltre al decimo dell'importo delle opere, dei servizi o delle forniture non eseguite, calcolato secondo quanto previsto dell'allegato II.14."*

18. RISOLUZIONE DEL CONTRATTO, AFFIDAMENTO A TERZI

La risoluzione del contratto sarà disposta nei casi e secondo le modalità di cui all'art.122 del Codice. Oltre che nei casi di cui al richiamato articolo ed a quelli espressamente previsti nel presente capitolato, il contratto potrà essere risolto nei seguenti:

- grave violazione, negligenza nonché in caso di grave o reiterata inadempienza degli obblighi contrattuali da parte dell'O.E. aggiudicatario rispetto al Capitolato ed alla normativa in materia;
- sospensione, abbandono o mancata effettuazione da parte dell'ente affidatario del servizio affidato;

- impiego di personale inadeguato o insufficiente a garantire il livello di efficienza del servizio;
- gravi azioni a danno della dignità personale degli utenti da parte degli operatori.

L'Amministrazione Comunale potrà altresì ottenere la risoluzione del contratto in ca-so di cessione dell'ente affidatario, di cessazione di attività, oppure in caso di concordato preventivo, fallimento, stato di moratoria e di conseguenti atti di sequestro o di pignoramento, nonché, qualora venga modificata la ragione sociale dell'ente in modo tale da non contemplare più le prestazioni oggetto di codesto appalto.

La Città di Giugliano in Campania, previa comunicazione scritta all'ente attuatore, ha diritto di risolvere il contratto con tutte le conseguenze di legge che la risoluzione comporta, comprese l'incameramento della cauzione definitiva e la facoltà di affidare l'appalto a terzi in danno all'O.E. aggiudicatario e facendo salva l'applicazione delle penali previste dal Codice.

L'aggiudicatario riconosce alla Città di Giugliano in Campania, nei casi previsti nel presente articolo, di risolvere "ipso iure" il contratto mediante comunicazione da inviarsi a mezzo di lettera raccomandata con ricevuta di ritorno, al domicilio eletto dall'O.E. aggiudicatario, nonché di incamerare la cauzione definitiva presentata dalla stessa, a carico della quale resterà anche l'onere del maggior prezzo pagato dalla Città di Giugliano in Campania, rispetto a quello convenuto con l'O.E. inadempiente, per proseguire il servizio.

Per qualsiasi ragione si addivenga alla risoluzione del contratto, l'O.E. aggiudicatario, oltre alla immediata perdita della cauzione a titolo di penale, sarà tenuta al risarcimento di tutti i danni diretti e indiretti ed alle maggiori spese a carico dalla Città di Giugliano in Campania per il rimanente periodo contrattuale.

In caso di risoluzione del contratto, all'appaltatore sarà corrisposto il prezzo contrattuale del solo servizio effettuato fino al giorno della disposta risoluzione, fermo re-stando il recupero delle somme spettanti all'Amministrazione per applicazione di penali.

La risoluzione del contratto comporta, altresì, che la ditta non potrà partecipare a successive gare indette dall'Amministrazione Comunale.

In caso di risoluzione del contratto l'appaltatore si impegnerà a fornire alla Città di Giugliano in Campania tutta la documentazione tecnica e i dati necessari al fine di provvedere direttamente o tramite terzi all'esecuzione dello stesso. Ai sensi dell'art. 124 del Codice *"le stazioni appaltanti interpellano progressivamente i soggetti che hanno partecipato all'originaria procedura di gara, risultanti dalla relativa graduatoria, per stipulare un nuovo contratto per l'affidamento dell'esecuzione o del completa-mento dei lavori, servizi o forniture, se tecnicamente ed economicamente possibile."* Pertanto, l'Amministrazione Comunale, per il completamento del servizio oggetto dell'appalto, avrà la facoltà di affidare l'appalto alla seconda classificata alle medesime condizioni economiche già proposte in sede di offerta e, in caso di indisponibilità del-la seconda classificata, di interpellare i successivi OO.EE. utilmente collocatesi in graduatoria al fine di stipulare il nuovo contratto alle medesime condizioni economiche già proposte in sede di offerta.

19. OBBLIGHI DELL'APPALTATORE RELATIVI ALLA TRACCIABILITÀ DEI FLUSSI FINAN-ZIARI

L'appaltatore assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136 e successive modifiche. L'appaltatore si impegna a dare immediata comunicazione alla stazione appaltante ed alla Prefettura/Ufficio Territoriale di Governo della Provincia di Napoli della notizia dell'inadempimento della propria controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.

20. DEFINIZIONE DELLE CONTROVERSIE

Tutte le controversie derivanti dal contratto, previo esperimento dei tentativi di transazione e di accordo bonario ai sensi rispettivamente degli articoli 211 e 212 del D. Lgs. 36/2023, qualora non risolte, sono devolute alla giustizia ordinaria.

Il ricorso al Giudice Ordinario non esimerà per qualsiasi ragione l'assuntore dal dar corso, comunque, all'esecuzione dell'ordinativo.

L'assuntore sarà, pertanto, tenuto ad ottemperare a tutti gli obblighi derivanti dal presente Capitolato anche se la materia del contendere dovesse riflettere l'ordinativo e/o l'esecuzione dello stesso.

Le spese saranno anticipate dalla parte che intenderà ricorrere al Giudice Ordinario.

La competenza a dirimere qualsiasi controversia, devoluta alla giustizia ordinaria, fra la stazione appaltante e l'aggiudicataria spetta in via esclusiva al Foro di Napoli Nord.

21. NORMATIVE CONTRATTUALI

L'appalto sarà regolato dal presente Capitolato e sarà, inoltre, soggetto a tutte le vi-genti disposizioni in materia. L'ente affidatario è tenuto all'osservanza di tutte le leggi, i decreti ed i regolamenti in vigore o che saranno emanati durante il periodo del pro-getto e, quindi, si impegna anche a rispettare tutte le leggi vigenti in materia di assunzione ed impiego del personale e degli obblighi derivanti dai contratti collettivi di la-voro, nonché la normativa tutta regolante le specifiche prestazioni oggetto del presente rapporto.

La sottoscrizione del Contratto per l'ente/i selezionato/i sarà impegnativa per l'affidatario dalla data di affidamento mentre per la Città di Giugliano in Campania sarà subordinato alle approvazioni di legge.

A seguito di singoli ordinativi di spesa saranno stipulati tra le parti idonei contratti attuativi.

22. NORME DI RINVIO E ALTRE CLAUSOLE

Per quanto non previsto nel presente CSA e dagli atti di gara tutti si fa espresso riferimento alle disposizioni legislative e regolamentari in vigore al momento della gara o che saranno emanate nel corso di validità della convenzione, se e in quanto applicabili.

Responsabile del procedimento:

Ai sensi di quanto disposto dall'art. 15 del D. Lgs. n. 36/2023 il Responsabile Unico del Progetto è il dr. Michele Maria Ippolito, Responsabile Transizione Digitale.

Trattamento dati personali

Ai sensi della normativa vigente e del regolamento UE n. 2016/679 i dati forniti dalle società saranno trattati esclusivamente per le finalità connesse alla gara e per l'eventuale successiva stipulazione e gestione del contratto. Il titolare del trattamento è la Città di Giugliano in Campania rappresentata dal Commissario in qualità di legale rappresentante dell'Ente.

Comunicazioni

La Città di Giugliano in Campania provvederà a pubblicare l'esito della presente procedura di selezione secondo quanto previsto dalla normativa vigente.

Il Responsabile Transizione Digitale

Dott. Michele Maria Ippolito

MICHELE MARIA IPPOLITO
Dirig. Amm. Serv. Sociali\, Istruzione\, Sport\, Cult
10.11.2025 10:47:21 UTC