



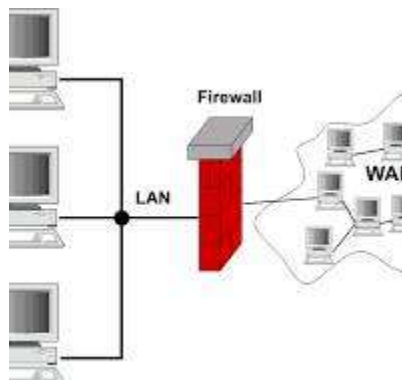
COMUNE DI OLBIA

Settore AA.GG. e Provveditorato - *Servizio ICT*

Project Area: Servizio IcT	Date: 10/04/2026
File: 2026.04.10-All_B-CT-FWaaS-Siportal.docx	Status: Definitivo

Affidamento del servizio FWaaS, migrazione e gestione di sistema Firewall in cluster ad alta affidabilità per infrastruttura fino a 10.000 utenze e 500 VPN Durata triennale

Capitolato Tecnico



Versione 1.0
Date: 10/04/2026



Indice

1	INTRODUZIONE	3
1.1	OBIETTIVO	3
1.2	A CHI È RIVOLTO	3
1.3	SEDI	3
1.4	ACRONIMI	4
1.5	ABBREVIAZIONI	4
1.6	DEFINIZIONI	4
1.7	RIFERIMENTI	4
1.8	ALLEGATI	4
2	OGGETTO DEL SERVIZIO	5
3	REVISIONE PREZZI	5
4	QUINTO D'OBBLIGO	5
5	SPECIFICHE TECNICHE MINIME OBBLIGATORIE	6
6	ULTERIORI REQUISITI MINIMI OBBLIGATORI	7
7	TEMPI DI ESPLETAMENTO E DURATA DEL SERVIZIO DI NOLEGGIO OPERATIVO	8
8	COLLAUDO	9
9	PAGAMENTO	9
10	DIRETTORE DELL'ESECUZIONE	9
11	CONTROLLO TECNICO-CONTABILE E AMMINISTRATIVO	10
12	GARANZIA DEFINITIVA	10
13	SVINCOLO DELLA GARANZIA DEFINITIVA	10
14	SUBAPPALTO	10
15	MANUTENZIONE, SLA E PENALI	10
15.1	LIVELLI DI GRAVITÀ DEI PROBLEMI:	11
15.2	INDICATORI TEMPORALI DI INTERVENTO	11
15.3	SLA E PENALI	11
15.3.1	Limiti di applicabilità dello SLA	12
16	VERBALE DI AVVIO DEL SERVIZIO	12
17	CLAUSOLA RISOLUTIVA ESPRESSA	12
18	DIRITTO DI RECESSO	13
19	TRATTAMENTO DEI DATI	13
20	TRACCIABILITÀ DEI FLUSSI FINANZIARI E ULTERIORI CLAUSOLE RISOLUTIVE ESPRESSE	13
21	ESTENSIONE DEGLI OBBLIGHI DI CONDOTTA PREVISTI DAL CODICE DI COMPORTAMENTO DEI DIPENDENTI PUBBLICI	14
22	INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI	14
23	RISERVATEZZA	15
24	CONTROVERSIE	16
25	NORME APPLICABILI	16
26	NORMATIVA DI RINVIO	16

Document History:

<i>Version</i>	<i>Date</i>	<i>Prepared/Modified by</i>	<i>Changes comparing to previous versions</i>
1.0	10.04.2026	Dott. Sebastiano Bellu	Draft

Review & Approval

<i>Review Name</i>	<i>Date</i>	<i>Approved</i>
1.0	10.04.2026	Dott. Sebastiano Bellu

1 Introduzione

1.1 Obiettivo

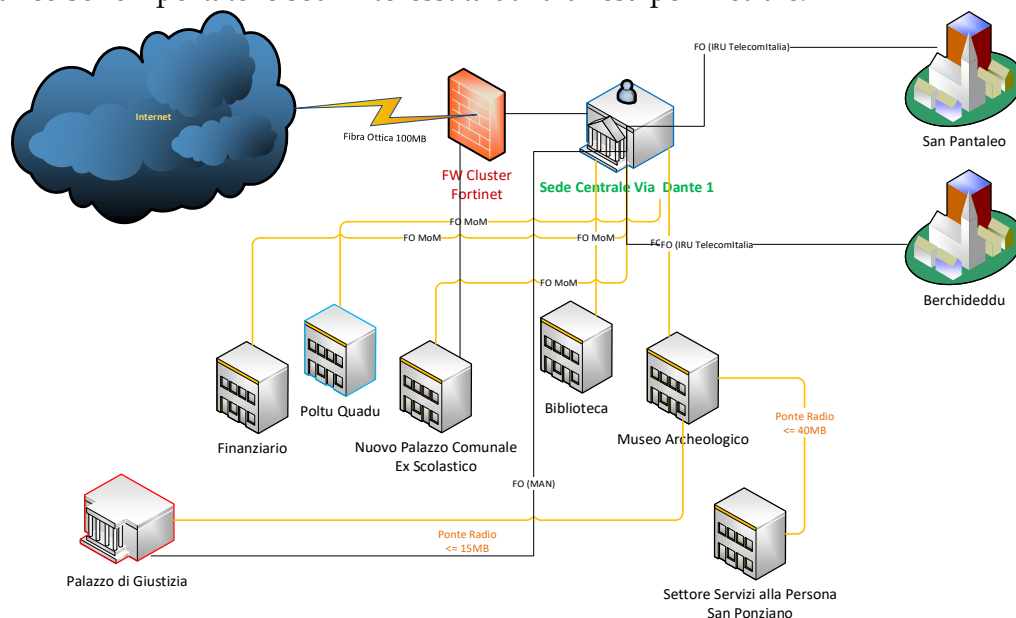
Capitolato Tecnico per il servizio di difesa perimetrale ICT con 2 Firewall in cluster HA, per una infrastruttura fino a 10.000 utenti (Uffici Comunali e Scuole Comunali e alcune Scuole Secondarie di Secondo ordine), con la possibilità di garantire fino a 500 VPN. I Firewall dovranno gestire una **banda di 10Gbps**. Il Servizio dovrà comprendere una attività Una Tantom per migrare l'attuale configurazione dei FW Fortigate 1100e presenti nel Data Center dell'Ente, in particolare tutte le policy definite ad oggi. Non dovranno essere presenti le policy disabilitate.

1.2 A chi è rivolto

Il seguente documento è finalizzato a fornire il dettaglio tecnico di quanto necessario per l'affidamento del servizio di firewalling.

1.3 Sedi

In questo grafico sono riportate le sedi interessate dalla difesa perimetrale:



1.4 Acronimi

SI	Sistema Informativo
ICT	Information and Communication Technology (<i>Tecnologie dell'informazione e della comunicazione</i>)
HW	Hardware
SW	Software
PdL	Postazione di Lavoro
SSD	Solid-State Drive (<i>memoria di massa a stato solido</i>)
OS	Operating System (<i>SO Sistema Operativo</i>)
SLA	Service Level Agreement (<i>accordo sul livello del servizio</i>)
NGFW	Next Generation Firewall
FQDN	Fully Qualified Domain Name
SOC	Security Operations Center
ZTNA	Zero Trust Network Access
SASE	Secure Access Service Edge

1.5 Abbreviazioni

--	--

1.6 Definizioni

La seguente tabella contiene la definizione di alcuni termini usati nel documento.

Nome	Definizione

1.7 Riferimenti

[1] Sito ufficiale Comune di Olbia: www.comune.olbia.ot.it

1.8 Allegati

[1] Misure di sicurezza ICT

[2]

2 Oggetto del Servizio

Configurazione, migrazione e manutenzione di un FWaaS:

- n. 2 firewall di fascia enterprise (architettura Next Generation Firewall – NGFW);
- configurazione in **cluster ad alta affidabilità (HA Active/Passive o Active/Active)**;
- migrazione completa delle configurazioni dall'attuale infrastruttura firewall on-premise;
- supporto specialistico e formazione operativa.

I firewall messi a disposizione devono essere opportunamente dimensionati per rispondere alle esigenze dell'Amministrazione in termini di protezione della rete da minacce esterne, controllo degli accessi, segmentazione del traffico e implementazione di policy di sicurezza personalizzate, il tutto in coerenza con le recenti normative in tema di sicurezza e resilienza informatica, dettate dalle Autorità competenti (AGID, ACN, GDPR).

La soluzione FWaaS verrà erogata in modalità Unmanaged da parte del Fornitore. Ciò implica che L'Ente intende mantenere la piena titolarità del management della soluzione FWaaS oggetto della fornitura, riservandosi l'autonomia operativa nella definizione, implementazione e modifica delle policy di sicurezza e delle configurazioni di sistema.

A tal fine, il fornitore dovrà garantire all'Ente l'accesso completo all'interfaccia di gestione della piattaforma firewall, con profilo amministrativo di livello superiore (super-admin o equivalente), senza limitazioni di natura tecnica o contrattuale all'operatività dell'Ente stesso.

Il fornitore è tenuto a:

- **Predisporre e mantenere l'infrastruttura** su cui è erogata la soluzione FWaaS, garantendo la continuità del servizio secondo i livelli concordati (SLA); la continuità del servizio deve essere garantita anche nell'operatività del firewall in HA nel suo ruolo funzionale di sicurezza perimetrale.
- **Fornire accesso amministrativo dedicato all'Ente**, con credenziali nominali e profilazione dei ruoli coerente con le esigenze operative dell'amministrazione;
- **Non interferire con le configurazioni** impostate dall'Ente, salvo esplicita richiesta scritta da parte del Responsabile Tecnico dell'amministrazione o in caso di emergenza documentata che richieda un intervento urgente a tutela dell'integrità del servizio;
- **Garantire la tracciabilità** di ogni operazione svolta dal proprio personale tecnico sull'apparato, mediante log di audit accessibili all'Ente in tempo reale o su richiesta.
- **Affiancare i tecnici dell'Ente** per le attività di supporto specialistiche necessarie.
- **Intervenire sistemisticamente per eventuali configurazioni successive richiesta dei tecnici dell'Ente.**

3 Revisione Prezzi

Qualora nel corso di esecuzione del contratto, al verificarsi di particolari condizioni di natura oggettiva, si determina una variazione, in aumento o in diminuzione, del costo del servizio superiore al cinque per cento, dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione, in relazione alle prestazioni da eseguire. Ai fini del calcolo della variazione dei prezzi si utilizza l'indice di Variazione % rispetto allo stesso mese dell'anno precedente pari a +0,8, ai sensi dell'articolo 60, comma 3, lettera b del Codice.

4 Quinto D'obbligo

Non è previsto il quinto d'obbligo.

5 Specifiche Tecniche Minime Obbligatorie

Nel presente Capitolato Tecnico sono riportate le Specifiche Tecniche Minime che dovranno essere soddisfatte, per tutti gli elementi componenti il servizio di FWaaS e per tutte le attività necessarie per l'erogazione dei servizi.

Tutte le specifiche e le caratteristiche tecniche, indicate nel presente documento con i tag [*SpecTech. xx*], sono da intendersi specifiche tecniche minime obbligatorie.

[SpecTech 1.]

La ditta fornitrice dovrà fornire un servizio di difesa perimetrale ICT con 2 Firewall in cluster HA, per una infrastruttura fino a **10.000** utenti (Uffici Comunali e Scuole Comunali e alcune Scuole Secondarie di Secondo ordine), con la possibilità di garantire fino a **500** VPN. I Firewall dovranno gestire una **banda di 10Gbps**.

Il Servizio dovrà comprendere una attività Una Tantum per migrare l'attuale configurazione dei FW Fortigate 1100e presenti nel Data Center dell'Ente, in particolare tutte le policy definite ad oggi. Non dovranno essere presenti le policy disabilitate. Sarà cura dei sistemisti messi a disposizione dal Fornitore, rendere correttamente funzionali i firewall forniti a partire da tale configurazione e risolvere eventuali problematiche di compatibilità legate al passaggio verso i nuovi apparati.

Sarà cura dell'Ente fornire il file di configurazione degli attuali firewall in dotazione.

Il Fornitore dovrà provvedere alla messa in opera dei firewall, collegamento alla rete dati dell'Amministrazione, test, messa in esercizio e collaudo.

[SpecTech 2.]

Il fornitore si impegna a notificare all'Ente ogni significativo incidente di sicurezza che riguardi l'infrastruttura e i servizi erogati all'Ente, entro **24** ore dalla rilevazione, fornendo supporto tecnico per la successiva segnalazione al CSIRT Italia (ACN).

[SpecTech 3.]

Logging da conservare criptato e con copia di sicurezza nascosta (*per l'autorità giudiziaria*).

[SpecTech 4.] **Requisiti architetturali generali**

Il sistema dovrà:

1. Essere basato su appliance hardware dedicate di classe data center enterprise.
2. Essere configurato in cluster HA con:
 - sincronizzazione stato sessioni;
 - sincronizzazione configurazione automatica;
 - failover automatico ≤ 5 secondi (*in configurazione Active-Passive (A-P)*).
3. Supportare minimo:
 - **10.000** utenti concorrenti autenticati;
 - **500** VPN (*SSL/IPsec*) attive contemporanee; si gestirà **IAM/MFA** con un sistema esterno, pertanto, il firewall dovrà delegare l'autenticazione;
 - Firewall throughput ≥ 10 Gbps;
 - routing inter-VLAN a livello firewall.

[SpecTech 5.] **Caratteristiche del servizio FWaaS**

Il servizio in modalità FWaaS deve garantire:

- che i firewall, forniti in modalità FWaaS, siano ospitati presso il Data Center del Fornitore;
- continuità operativa con configurazione ridondante (cluster in HA) per eliminare singoli punti di guasto;
- nessun investimento hardware da parte dell'Amministrazione e gestione operativa demandata al Fornitore;
- supporto professionale con **team specializzato e certificato dalla casa madre per i firewall** messi a disposizione, per la gestione e il monitoraggio, per **8 ore/mese**;

- conformità NIS2: piattaforme di management e analisi per garantire autonomia gestionale nel rispetto del decreto legislativo sulla sicurezza delle reti (*D.Lgs. 4 settembre 2024 n.138*);
- protezione avanzata da minacce, IPS, antivirus, web-filtering, antispam;
- supporto tecnico prioritario e aggiornamenti continui;
- piattaforme di gestione che garantiscano all'Amministrazione piena visibilità e controllo sulla propria postura di sicurezza, facilitando la conformità normativa e l'audit:
 - a. piattaforma centralizzata per la configurazione, gestione delle policy e orchestrazione dei firewall;
 - b. piattaforma avanzata per analisi dei log, reportistica e monitoraggio della sicurezza in tempo reale.

[SpecTech 6.] Compliance ad ACN dei Firewall e certificazioni.

I firewall in cluster devono essere conformi alle specifiche ACN e il fornitore è tenuto a documentare tale compliance.

I tecnici messi a disposizione dal fornitore, per l'intera durata del contratto, devono essere in possesso della certificazione rilasciata dalla casa madre del firewall messo a disposizione, per garantire un'alta competenza tecnica e capacità di configurare, gestire e risolvere problemi su firewall di fascia enterprise (NGFW), in grado di proteggere l'infrastruttura dell'Ente da minacce informatiche avanzate. Il possesso del suddetto requisito di certificazione dovrà essere dimostrato in fase di collaudo dei servizi FWaaS.

[SpecTech 7.]

Il fornitore dovrà garantire che i 2 (due) firewall in cluster siano sempre aggiornati a nuove release sia firmware che di OS.

[SpecTech 8.]

Uptime: il fornitore deve garantire una disponibilità del servizio $\geq 99,95\%$ su base mensile e un supporto tecnico 12x6.

[SpecTech 9.] Aggiornamenti delle Firme (IPS, Antivirus, Web Filtering, etc.)

Garanzia da parte del fornitore di "Zero-Day patching": le protezioni contro una nuova minaccia devono essere distribuite, se rese disponibili dal produttore del Firewall entro cinque giorni lavorativi dalla disponibilità della patch.

Il fornitore si impegna, laddove particolari esigenze di sicurezza lo richiedessero, a **proporre** e a **supportare** l'Ente per l'**applicazione delle suddette patch coerentemente ad eventuali esigenze temporali più ristrette**.

[SpecTech 10.] Portabilità delle Policy

A chiusura del contratto il fornitore del FWaaS deve garantire l'esportazione delle policy in formati standard o tramite API.

6 Ulteriori Requisiti Minimi Obbligatori

[SpecTech 11.]

I Firewall messi a disposizione devono essere prodotti originali recanti il marchio del produttore. Tutti gli oggetti dovranno essere nuovi.

Il Fornitore si impegna a utilizzare licenze software originali rilasciate. Il Fornitore non potrà mettere a disposizione prodotti usati o rigenerati.

[SpecTech 12.]

I FW, oggetto del servizio, dovranno essere derivati da produzioni di primarie marche presenti sul mercato e non essere prodotti dall'assemblaggio di componenti non soggetti a controllo industriale.

[SpecTech 13.]

Come caratteristica generale, valida per tutti i componenti hardware e software degli elementi oggetti del presente contratto, si richiede che:

- la tecnologia di tutti i componenti sia di ultima generazione;
- per nessun componente sia stata annunciata, al momento della presentazione dell'offerta, la messa fuori produzione dello stesso o la sospensione del relativo supporto da parte del produttore;
- per quei componenti che dovessero essere dichiarati fuori produzione dalla casa madre prima della attivazione del sistema di firewalling, deve essere fornita in sostituzione la nuova release del prodotto stesso;
- i firewall messi a disposizione non devono uscire fuori produzione durante il periodo contrattuale.

[SpecTech 14.]

I Firewall richiesti nell'ambito del presente Capitolato Tecnico dovranno presentare caratteristiche intrinseche di robustezza ed affidabilità tali da limitare le possibilità di malfunzionamento delle apparecchiature stesse, ed in maniera più generale, dell'intera infrastruttura.

[SpecTech 15.]

I Firewall messi a disposizione devono essere marcati CE, devono essere corredati di informazioni utili al loro smaltimento integrale o di parti di esse, in conformità con la vigente normativa in materia.

[SpecTech 16.] [SpecTech 16.] Requisiti ambientali DNSH Scheda 8

Relativamente ai requisiti ambientali DNSH, per i firewall il Fornitore deve essere in possesso della Registrazione Emas / UNI EN ISO 14001 / CLC/TR 50600-99-1, oppure sia iscritto al Code of Conduct for energy efficiency of data centers (rispetti le best practices).

In alternativa, il fornitore deve dare evidenza di rispettare congiuntamente i seguenti requisiti:

1. EPA ENERGY STAR / ISO/IEC 30134-4:2017 [*standard di efficienza energetica per nuovo HW*]
2. EN 50625 [Gestione Rifiuti]
3. UNI EN ISO IEC 50001 / EN 50600/ISO IEC 22237 / ANSI TIA-942 pertinente [*Potenziale di riscaldamento Globale GWP*];
4. EN IEC 63000:2018 [*Sostanze pericolose*]

In aggiunta ai suddetti 4 requisiti bisognerà presentare evidenza anche di uno tra i requisiti per la gestione ambientale dei Data Center:

- a. ISO 55000/ISO 14040/ISO 14044/ EN 15978
- b. ISO 30134:2016

[SpecTech 17.]

Il servizio di firewalling deve essere eseguito direttamente dalla ditta fornitrice, ossia l'Ente avrà rapporti esclusivamente con il Fornitore.

[SpecTech 18.]

GDPR: la società deve garantire una tutela ai massimi livelli dei "dati personali" eventualmente presenti sulle memorie dei firewall e nel flusso dei pacchetti IP, in particolare rispettando le misure di sicurezza ICT allegate al presente Capitolato Tecnico.

7 Tempi di espletamento e durata del servizio di noleggio operativo

Il servizio di firewalling dovrà essere attivato entro il termine massimo di **60 (sessanta) giorni (lavorativi e consecutivi)** dalla stipula del contratto.

La durata del servizio di firewalling è stabilita in anni 3 (tre).

8 Collaudo

Il collaudo dovrà iniziare non prima della data di comunicazione, da parte del fornitore, di avvenuta messa in produzione dei firewall in HA, di verifica funzionale positiva e di verifica di tutte le **SpecTech richieste dal presente capitolato**. Sarà espletato dal Responsabile del Servizio ICT del Comune, alla presenza di un tecnico del Fornitore, e terminerà non oltre **5 (cinque) giorni** dalla predetta data. Nel caso in cui il collaudo abbia un esito negativo, anche parziale, sarà ripetuto entro **7 (sette) giorni**.

Il collaudo dovrà prevedere:

- Test failover cluster;
- Test banda;
- Test VPN multipla;

9 Pagamento

Il corrispettivo comprende:

- a) Il pagamento U.T. dell'attività di migrazione dall'attuale sistema e configurazione dei nuovi firewall, a collaudo positivo;
- b) il pagamento del servizio di firewalling, che verrà effettuato sotto forma di **canone semestrale anticipato**.

Con tale corrispettivo la ditta si intende compensata di qualsiasi suo avere o pretendere dall'Amministrazione Comunale per il servizio di che trattasi, senza alcun diritto a nuovi o maggiori compensi.

Il pagamento verrà eseguito mediante bonifico bancario/postale previa presentazione di regolare fattura che dovrà pervenire obbligatoriamente in modalità elettronica mediante l'utilizzo del sistema informatico messo a disposizione sul sito www.fatturapa.gov.it.

La fattura, intestata al Comune di Olbia – Via Dante 1, 07026 Olbia – P.I. 00920660909, potrà essere emessa successivamente agli adempimenti descritti al successivo art. 13.

Sull'importo netto del servizio di manutenzione l'Ente applicherà una ritenuta dello **0,50** per cento. Tale ritenuta potrà essere svincolata soltanto in sede di liquidazione finale dopo l'approvazione del certificato di regolare esecuzione da parte del RUP e previo rilascio del DURC con esito positivo.

La fattura dovrà contenere i seguenti dati:

1. descrizione dettagliata del servizio;
2. numero e data della determinazione del Dirigente di Settore che verrà comunicata al momento dell'aggiudicazione definitiva ex 90, comma 1 lett.b del D.Lgs. 36/2023;
3. il codice univoco ufficio: **J65OW6**;
4. la dicitura "scissione dei pagamenti – art. 17 ter del DPR n. 633/1972".

I pagamenti verranno effettuati, entro i termini di legge decorrenti dalla data di protocollazione della fattura, tramite bonifico su conto corrente bancario/postale.

In caso di fattura irregolare il termine di pagamento verrà sospeso dalla data di contestazione dell'Amministrazione. Dalle fatture saranno detratte le eventuali penalità applicate.

10 Direttore dell'esecuzione

Il direttore dell'esecuzione (DEC) sarà nominato dal RUP entro 5 giorni dalla stipula del contratto.

11 Controllo tecnico-contabile e amministrativo

Il DEC deve provvedere al coordinamento, alla direzione e al controllo tecnico-contabile dell'esecuzione del contratto stipulato dalla stazione appaltante secondo le competenze che gli vengono assegnate dalla vigente normativa di settore.

In caso di regolarità del DURC, il RUP emetterà lo stato di avanzamento del servizio ed il certificato di pagamento nel quale verrà indicato l'importo che dovrà essere riportato in fattura. Il S.A.S. ed il C.P. verranno trasmessi alla ditta aggiudicataria la quale entro 5 giorni dal ricevimento dovrà restituirli firmati. All'atto della firma la Ditta aggiudicataria potrà aggiungere le eventuali contestazioni che ritiene opportune, rispetto alle operazioni di verifica.

12 Garanzia Definitiva

Prima della stipula del contratto, l'affidatario è tenuto a costituire apposita garanzia definitiva, a norma dell'art. 53 del d.lgs. n. 36/2023. La garanzia può essere costituita mediante cauzione, come precisato nell'art. 106 del codice dei contratti, al quale si formula espresso rinvio, o con garanzia fideiussoria, anche in questo caso con le modalità specificate dal citato articolo 106, purché contenga la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, preveda espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, preveda l'operatività entro 15 giorni, a semplice richiesta della stazione appaltante. Non verrà accettata altra forma di costituzione della garanzia definitiva.

La ditta affidataria è obbligata a reintegrare la cauzione su cui l'Amministrazione si sia rivalsa, in tutto o in parte, durante l'esecuzione del contratto.

In caso di inadempienza la cauzione potrà essere reintegrata d'ufficio a spese della ditta affidataria, prelevandone l'importo dal corrispettivo ancora dovuto alla stessa ditta.

Resta salvo per l'Amministrazione l'esperimento di ogni altra azione nel caso in cui la cauzione risultasse insufficiente.

La mancata costituzione della garanzia di cui al presente articolo determinerà la decadenza dell'affidamento.

13 Svincolo della Garanzia Definitiva

La garanzia definitiva è progressivamente svincolata in funzione dell'avanzamento dell'esecuzione del contratto, nel limite massimo dell'80 per cento dell'importo garantito.

L'ammontare residuo della garanzia definitiva permane fino alla data di emissione del certificato di regolare esecuzione, o comunque fino a dodici mesi dalla data di ultimazione del servizio risultante dal relativo certificato.

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, dello stato di avanzamento del servizio, in originale o in copia autentica, attestanti l'avvenuta esecuzione.

14 Subappalto

Vista la particolare attività specialistica del servizio di FWaaS, non è ammesso il subappalto!

15 Manutenzione, SLA e Penali

I servizi di manutenzione ordinaria e straordinaria sono tutti a carico del Fornitore senza alcun onere da parte dell'Ente.

15.1 Livelli di gravità dei problemi:

Nella tabella di seguito riportata, sono definiti i livelli di gravità delle possibilità criticità:

Livello	Descrizione
Liv_01*	anomalia bloccante: i FW in HA è indisponibile o gravemente degradato.
Liv_02*	anomalia grave: funzioni critiche del FW in HA, sono indisponibili o gravemente degradate.
Liv_03	anomalia media: funzioni non critiche FW in HA sono indisponibili o gravemente degradate, oppure funzioni critiche sono lievemente degradate.
Liv_04	anomalia lieve: funzioni non critiche dei FW in HA sono lievemente degradate.
Liv_05	manutenzione adeguativa: criticità dei FW in HA comportano la necessità di aggiornamenti firmware o di release.

*In caso di indisponibilità riconducibile a vulnerabilità “zero-day” non ancora soggetta a patch ufficiale da parte del vendor, il livello di gravità è mantenuto, ma i termini di ripristino sono estesi fino a disponibilità di remediation ufficiale o applicazione di workaround certificato. Le penali previste sono sospese per la durata dell'evento zero-day documentato.

15.2 Indicatori temporali di intervento

Di seguito si riportano in tabella le definizioni degli indicatori temporali, che saranno utilizzati per la definizione degli SLA e delle penali.

Indicatore	Descrizione
TPC: Tempo di Presa in Carico	Intervallo di tempo intercorrente fra la richiesta di intervento a fronte di un malfunzionamento e la conferma del Fornitore di aver recepito la richiesta e attivato le procedure necessarie per l'effettuazione dell'intervento; richiesta di intervento e conferma devono avvenire tramite mail, PEC o telefonata, con caricamento sul sistema di Trouble Ticketing dell'Ente.
TR: Tempo Risoluzione	Intervallo di tempo intercorrente fra la conferma del Fornitore di aver preso in carico la chiamata e l'effettiva risoluzione del malfunzionamento segnalato mediante invio da parte del Fornitore tramite chiusura sul sistema di Ticketing messo a disposizione dall'Ente e contestuale e-mail di un messaggio di chiusura intervento. Nel caso in cui l'Ente non ritenga il malfunzionamento risolto (e non emetta quindi il relativo certificato di accettazione, inviando al fornitore contestazione dell'intervento effettuato), l'intervento si riterrà non concluso e il tempo di risoluzione verrà nuovamente calcolato al momento in cui il Fornitore darà nuova segnalazione di chiusura intervento a cui segua l'accettazione da parte dell'Ente.

15.3 SLA e Penali

Livello	SLA (ore consecutive)				Penali (‰ per mille)		Importo Aggiudicazione
	TPC		TR		TPC + TR	Perc. Appl.	
Liv_01	≤	6	≤	6	> 12	0,40‰	
Liv_02	≤	6	≤	10	> 16	0,38‰	
Liv_03	≤	8	≤	72	> 80	0,35‰	
Liv_04	≤	8	≤	96	> 106	0,32‰	
Liv_05	≤	24	≤	336	> 360	0,30‰	

*La percentuale si applica per ogni giorno successivo al superamento dello SLA.

V giorno ritardo * si intende che superato il limite **TPC+TC**, si applicherà la penale indicata per il giorno in cui avviene tale superamento e per ogni giorno successivo, fino al giorno in cui il problema viene risolto.

Nel caso di ritardo della fornitura del servizio, per ogni giorno di ritardo si applica una penale giornaliera pari a **1‰ (uno per mille)** dell'importo di aggiudicazione. Resta inteso che l'ammontare delle penali applicate non potrà superare l'**1% (uno per cento)** dell'importo della fornitura.

Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali di cui ai precedenti commi, verranno contestati al Fornitore contraente dal RUP per iscritto. Il Fornitore contraente dovrà comunicare in ogni caso le proprie deduzioni al RUP nel termine massimo di 5 (cinque) giorni dalla stessa contestazione. Qualora dette deduzioni non siano accoglibili a giudizio del RUP ovvero non vi sia stata risposta o la stessa non sia giunta nel termine indicato potranno essere applicate al Fornitore contraente le penali come sopra indicate a decorrere dall'inizio dell'inadempimento.

Tutte le penali di cui al presente articolo sono contabilizzate in detrazione in occasione del pagamento immediatamente successivo al verificarsi della relativa condizione.

La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore contraente dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale, fatta salva la facoltà per il RUP di risolvere il Contratto nei casi in cui questo è consentito.

15.3.1 Limiti di applicabilità dello SLA

Qui di seguito sono riportate le condizioni in presenza delle quali, nonostante il verificarsi di eventuali disservizi, non si prevedono penali nei confronti del fornitore a seguito del non rispetto degli SLA:

- a. cause di Forza Maggiore e cioè eventi che, oggettivamente, impediscano ai tecnici del Fornitore di intervenire per eseguire le attività di intervento richieste (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani etc);
- b. Interventi Straordinari da effettuarsi con urgenza, atti ad evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità del servizio. L'eventuale esecuzione di tali interventi sarà, comunque, comunicata al Fornitore via PEC da parte del CED dell'Ente, con contestuale chiamata telefonica, con preavviso minimo di 1 ora;
- c. Indisponibilità o Blocchi al Servizio imputabili a:
 - c.1) errato utilizzo, errata configurazione o comandi volontariamente o involontariamente eseguiti dal cliente;
 - c.2) anomalie e malfunzionamenti dei software applicativi/gestionali forniti da terze parti;
 - c.3) inadempimento o violazione del Contratto imputabile all'Ente;
 - c.4) cause che determinano l'inaccessibilità, imputabili a guasti nella rete internet esterna al perimetro del fornitore e, comunque, fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

16 Verbale di avvio del Servizio

Il giorno successivo alla data di stipula del contratto verrà redatto un verbale di avvio del servizio.

17 Clausola risolutiva espressa

Oltre a quanto previsto dagli artt. 1453 e seguenti del Codice Civile, la Stazione Appaltante potrà risolvere di diritto il Contratto ai sensi dell'art. 1456 c.c., previa dichiarazione da comunicarsi al Fornitore contraente per iscritto, e senza bisogno di assegnare previamente alcun termine per l'adempimento, nei seguenti casi:

- a. qualora fosse accertato il venir meno dei requisiti morali richiesti dall'art.94 all'art.98 del D.lgs. 36/2023;
- b. inosservanza delle leggi in materia di rapporti di lavoro, correttezza contributiva;
- c. inosservanza delle leggi in materia di sicurezza;
- d. inadempimento rispetto agli obblighi di riservatezza e di trattamento dei dati personali;
- e. nel caso in cui le transazioni finanziarie siano eseguite senza l'utilizzo del bonifico bancario o postale ovvero di altri strumenti idonei a consentire la piena tracciabilità delle stesse, così come previsto dall'art. 3, comma 8, della legge n. 136/2010;
- f. dopo la terza diffida scritta circa la puntuale esecuzione delle prestazioni contrattuali, qualora il fornitore non abbia risposto per ciascuna di esse fornendo risoluzioni idonee al superamento delle inadempienze contestate.

In caso di risoluzione del Contratto, il Fornitore contraente si impegna comunque a porre in essere ogni attività necessaria per assicurare il servizio a favore della Stazione Appaltante.

18 Diritto di Recesso

Ai sensi dell'art. 123 del d.lgs 36/2023 l'Amministrazione può recedere dal contratto in qualunque momento purché tenga indenne l'appaltatore mediante il pagamento delle prestazioni eseguite 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 del servizio non eseguito, calcolato secondo quanto previsto dell'allegato II.14 del codice.

In detta circostanza l'Amministrazione indennizzerà l'appaltatore mediante il pagamento delle prestazioni eseguite nonché del valore dei materiali utili esistenti in magazzino, oltre al decimo dell'importo del servizio non eseguito.

L'esercizio del diritto di recesso è manifestato dalla stazione appaltante mediante una formale comunicazione all'appaltatore da darsi per iscritto con un preavviso non inferiore a venti giorni, decorsi i quali la stazione appaltante prende in consegna il servizio e verifica la regolarità delle prestazioni.

19 Trattamento dei Dati

Ai sensi del D.lgs n° 196/2003, si informa che i dati comunicati dalla ditta saranno oggetto di trattamento nel rispetto dei principi della vigente normativa.

20 Tracciabilità dei flussi finanziari e ulteriori Clausole risolutive espresse

1. Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136 e s.m.i., l'aggiudicatario si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.
2. Ferme restando le ulteriori ipotesi di risoluzione previste nel presente capitolato si conviene che, in ogni caso, il Comune, in ottemperanza a quanto disposto dall'art. 3, comma 9 *bis*, della Legge 13 agosto 2010 n. 136 e s.m.i., senza bisogno di assegnare previamente alcun termine per l'adempimento, risolverà di diritto, ai sensi dell'art. 1456 c.c., nonché ai sensi dell'art. 1360 c.c., previa dichiarazione da comunicarsi all'aggiudicatario, i singoli contratti nell'ipotesi in cui le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri documenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora "**Autorità Nazionale Anticorruzione**", di seguito "**A.N.AC.**") n. 4 del 7 luglio 2011.
3. In ogni caso, si conviene che il Comune, senza bisogno di assegnare previamente alcun termine per l'adempimento, si riserva di risolvere di diritto il Contratto, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'aggiudicatario con PEC, nell'ipotesi di reiterati inadempimenti agli obblighi di cui al precedente comma.
4. L'aggiudicatario, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136 e s.m.i., ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136 e s.m.i.
5. L'aggiudicatario, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui all'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i., è tenuto a darne immediata comunicazione al Comune e alla Prefettura - Ufficio Territoriale del Governo della Provincia ove ha sede la stazione appaltante.
6. L'aggiudicatario, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari. Il Comune verificherà che nei contratti sottoscritti con i subappaltatori e i subcontraenti, sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla su richiamata Legge.

7. L'aggiudicatario sarà tenuto a comunicare al Comune, entro e non oltre 7 giorni dalla stipula del Contratto, i dati afferenti al Conto Bancario o Postale dedicato, anche non in via esclusiva, alla ricezione dei flussi finanziari relativi al contratto stipulato nonché le generalità e il codice fiscale del/i soggetto/i delegato/i ad operare sul conto/i corrente del Fornitore dedicato/i.
8. L'aggiudicatario è tenuto a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i, qualsivoglia variazione intervenuta in ordine ai dati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il Codice Fiscale delle persone delegate ad operare su detto/i conto/i.
9. Con riferimento ai contratti di subappalto, l'aggiudicatario si obbliga a trasmettere al Comune, oltre alle informazioni di cui all'art. 119, comma 2, quinto periodo, del D. Lgs. n. 36/2023 e s.m.i., anche apposita dichiarazione resa ai sensi del DPR 445/2000, attestante che nel relativo sub-contratto, ove predisposto, sia stata inserita, a pena di nullità assoluta, un'apposita clausola con la quale il subcontraente assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge, restando inteso che il Comune, si riserva di procedere a verifiche a campione sulla presenza di quanto attestato, richiedendo all'uopo la produzione degli eventuali sub-contratti stipulati, e, di adottare, all'esito dell'espletata verifica ogni più opportuna determinazione, ai sensi di legge e di contratto.
10. Ai sensi della Determinazione dell'Autorità per la Vigilanza sui contratti pubblici (ora A.N.A.C.) n. 4 del 7 luglio 2011, l'aggiudicatario, in caso di cessione dei crediti, si impegna a comunicare il CIG al cessionario affinché lo stesso venga riportato sugli strumenti di pagamento utilizzati. Il cessionario è tenuto a utilizzare conto/i corrente/i dedicato/i nonché ad anticipare i pagamenti all'aggiudicatario mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i dell'aggiudicatario medesimo riportando il CIG dallo stesso comunicato e, in generale, al rispetto delle prescrizioni stabilite dalla normativa applicabile e dall'A.N.A.C.

21 Estensione degli obblighi di condotta previsti dal codice di comportamento dei dipendenti pubblici

Gli obblighi di condotta previsti dal "Regolamento comunale recante il codice di comportamento dei dipendenti pubblici", approvato con deliberazione della Giunta comunale n. 452 del 22/11/2023, ai sensi e per gli effetti del d.P.R. 16 aprile 2013, n. 62, vengono estesi, per quanto compatibili, anche ai collaboratori a qualsiasi titolo dell'impresa affidataria dell'appalto (imprese fornitrici di beni o servizi in favore del comune di Olbia).

Il rapporto si risolverà di diritto o decadrà nel caso di violazioni da parte dei collaboratori dell'impresa contraente del suindicato "Regolamento". L'indirizzo URL del sito comunale in cui il menzionato "Regolamento" è pubblicato è:

<https://servizi.comune.olbia.ot.it/L190/?idSezione=15201&id=&sort=&activePage=&search=>

22 Informativa sul Trattamento dei Dati Personali

L'aggiudicatario dichiara di aver ricevuto prima della sottoscrizione del contratto di fornitura/servizio le informazioni di cui agli artt. 13 e 14 del regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione del contratto stesso e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa. Tale informativa è contenuta nella lettera di richiesta conferma preventivo, che deve intendersi in quest'ambito integralmente trascritto.

Con la sottoscrizione del contratto, il rappresentante legale del fornitore acconsente espressamente al trattamento dei dati personali come sopra definito, si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione del contratto per le finalità descritte nel disciplinare di gara e sopra richiamate;

La S.A. acconsente espressamente al trattamento da parte dell'aggiudicatario dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione del contratto.

Inoltre, in adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 20 D.Lgs. 36/2023), il fornitore prende atto della pubblicazione e diffusione dei dati e/o della documentazione che la legge impone di pubblicare, tramite il sito internet www.comune.olbia.ot.it sezione amministrazione trasparente.

Con la sottoscrizione del contratto il fornitore acconsente espressamente al trattamento dei dati personali e si impegna a improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente (Regolamento UE 2016/679), ivi inclusi gli ulteriori provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la protezione dei dati personali.

In particolare, si impegna ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non compatibili con le finalità per cui i dati sono stati raccolti.

L'aggiudicatario si impegna ad adottare le misure di sicurezza di natura fisica, logica, tecnico ed organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi compresa quelle specificate nel contratto, unitamente ai suoi allegati; si impegna, altresì ad osservare le vigenti disposizioni in materia di sicurezza e privacy ed a farle osservare ai relativi dipendenti e collaboratori, opportunamente autorizzati al trattamento dei Dati personali.

L'aggiudicatario prende atto che l'ente potrà operare verifiche periodiche, ispezioni ed audit, anche tramite soggetti terzi autorizzati dallo stesso, volti a riscontrare l'applicazione e l'adeguatezza delle misure di sicurezza dei dati personali applicate.

23 Riservatezza

- a. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del contratto e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
- b. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del contratto; tale obbligo non concerne i dati che siano o divengano di pubblico dominio.
- c. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza anzidetti.
- d. In caso di inosservanza degli obblighi di riservatezza, l'Amministrazione ha la facoltà di dichiarare risolto di diritto il contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare all'Amministrazione.
- e. Il Fornitore potrà citare i contenuti essenziali del contratto, nei casi in cui ciò fosse condizione necessaria per la partecipazione del Fornitore medesimo a gare e appalti.
- f. Il Fornitore si impegna, altresì, a rispettare quanto previsto dalla normativa sul trattamento dei dati personali (Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e ulteriori provvedimenti in materia.

24 Controversie

Per le controversie di qualsiasi natura e genere che dovessero sorgere in ordine al Capitolato Tecnico è competente il Foro di Tempio Pausania.

25 Norme Applicabili

La presente procedura è regolata dal presente capitolato speciale e quindi dalle disposizioni ivi contenute o espressamente richiamate, dalla legislazione vigente in materia di appalti pubblici, dal Codice Civile e da altre disposizioni in quanto compatibili.

26 Normativa di rinvio

Per quanto non espressamente previsto nelle condizioni contenute nel presente documento, trovano applicazione le norme di Legge vigenti in materia di affidamento di contratti pubblici, con particolare riferimento al D.Lgs. 36/2023.

Olbia, 10/04/20266



Il RUP
Dott. Sebastiano Bellu