

FRONTESPIZIO DETERMINAZIONE

AOO: ASL_BO

REGISTRO: Determinazione

NUMERO: 0002484

DATA: 06/10/2026 14:58

OGGETTO: Procedura aperta PI 433695-26 per la fornitura in SERVICE DI SISTEMI ANALITICI DI CITOFLUORIMETRIA PER LE ESIGENZE DELLE AZIENDE DELL' AREA VASTA EMILIA CENTRO (AVEC). Approvazione parziale modifica documentazione di gara.

SOTTOSCRITTO DIGITALMENTE DA:

Antonia Crugliano

ADOTTATO DA:

Servizio Acquisti di Area Vasta - SAAV (SC)

CLASSIFICAZIONI:

- [08-02]

DESTINATARI:

- Collegio sindacale: collegio.sindacale@aosp.bo.it; collegio.sindacale@ausl.bologna.it; collegio.sindacale@ospfe.it
- Servizio Acquisti di Area Vasta - SAAV (SC)

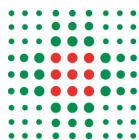
DOCUMENTI:

File	Firmato digitalmente da	Hash
DETE0002484_2026_determina_firmata.pdf	Crugliano Antonia	5F2E5501F53C5D17DC4BDF0E0BA1133B 9BFE2095350D9982A2205AFE5374834F
DETE0002484_2026_Allegato1.pdf:		CB057B434C2A5FF282DEEF7F29A5E43E DB39C273BD31DE8474CC64A32C84A1C8



L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.

Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.



Servizio Acquisti di Area Vasta - SAAV (SC)

DETERMINAZIONE

OGGETTO: Procedura aperta PI 433695-26 per la fornitura in SERVICE DI SISTEMI ANALITICI DI CITOFLUORIMETRIA PER LE ESIGENZE DELLE AZIENDE DELL'AREA VASTA EMILIA CENTRO (AVEC). Approvazione parziale modifica documentazione di gara.

IL DIRETTORE

Vista la delibera n.115 del 13.06.2011 di unificazione di servizi amministrativi in ambito metropolitano con la quale è stato istituito il Servizio Acquisti Metropolitano;

Viste le delibere n. 268 del 29.06.2022 dell'Azienda USL di Bologna, n.204 del 29.06.2022 dell'IRCCS Azienda Ospedaliero-Universitaria di Bologna Policlinico di Sant'Orsola, n.193 del 30.06.2022 dell'IRCCS – Istituto Ortopedico Rizzoli, n.149 del 29.06.2022 dell'Azienda USL di Imola, n.129 del 29.06.2022 dell'Azienda Ospedaliero Universitaria di Ferrara, n.179 del 01.07.2022 dell'Azienda USL di Ferrara con le quali è stato costituito il Servizio Acquisti di Area Vasta Emilia Centrale (SAAV) ed è stata contestualmente approvata la convenzione attuativa per lo svolgimento delle relative funzioni unificate con decorrenza dall'1 luglio 2022;

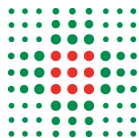
Considerato che con le sopra citate delibere sono state altresì individuate le funzioni delegate al SAAV e quelle di competenza esclusiva delle Aziende deleganti;

Richiamata la delibera n.404 del 08.11.2022 di conferimento dell'incarico dirigenziale di Direttore del SAAV;

Richiamati altresì gli atti deliberativi n.62 del 12 febbraio 2024 dell'Azienda Usl di Bologna, n.53 del 15 febbraio 2024 dell'IRCCS Azienda Ospedaliero-Universitaria di Bologna Policlinico di Sant'Orsola, n.69 del 22 marzo 2024 dell'IRCCS- Istituto Ortopedico Rizzoli, n.41 del 26 febbraio 2024 dell'Azienda Usl di Imola, n.41 del 19 febbraio 2024 dell'Azienda Ospedaliero Universitaria di Ferrara, n.61 del 20 febbraio 2024 dell'Azienda Usl di Ferrara con i quali è stata approvata la nuova convenzione attuativa per lo svolgimento delle funzioni unificate del SAAV;

Richiamata la determinazione n. 2148/2026 adottata dal Direttore del Servizio Acquisti di Area Vasta, con la quale si è provveduto, ai sensi del D.Lgs 36/23, all'indizione della procedura di gara:

- procedura aperta per la fornitura in "SERVICE DI SISTEMI ANALITICI DI CITOFLUORIMETRIA PER LE ESIGENZE DELLE AZIENDE DELL'AREA VASTA EMILIA CENTRO (AVEC)", suddivisa in 2 lotti, della durata di 5 (cinque) anni, eventualmente rinnovabile di ulteriori anni 2 (due) anche



singolarmente considerati, per un importo complessivo per 5 (cinque) anni di € 5.868.370,00 IVA esclusa, di cui € 5.870,00 quali oneri di sicurezza non soggetti a ribasso IVA esclusa;

- scelta del contraente mediante procedura aperta ai sensi dell'art.71 del D.lgs 36/2023, criterio di aggiudicazione basato sull'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo ai sensi dell'art.108, del D.lgs 36/2023;

Vista la richiesta di un Operatore Economico di chiarimenti e precisamente:

1) *“Spettabile Ente, Con riferimento al paragrafo 7 “Requisiti informatici – Cybersecurity” del Capitolato Speciale Normativo Prestazionale, si chiede di chiarire se il requisito secondo cui qualsiasi apparato hardware e software deve essere conforme alle politiche aziendali in materia debba intendersi riferito alle politiche della Committente. In caso affermativo, si chiede di specificare quali siano tali politiche. In alternativa, si chiede di confermare che l’offerente debba descrivere le proprie politiche di sicurezza proposte”.*

2) *“Spettabile Ente. Con riferimento al paragrafo 7 “Requisiti informatici – Politiche di sicurezza” del Capitolato Speciale Normativo Prestazionale, si chiede di fornire la documentazione relativa alle politiche di sicurezza e privacy della Committente, richiamate dal requisito che prevede la coerenza della security policy del fornitore con l’analogo documento della Committente”.*

Considerato che per i quesiti richiesti dall'Operatore Economico si è proceduto ad una verifica a seguito della quale:

per la risposta al quesito n. 1)

Le politiche a cui conformarsi sono quelle dell'azienda committente; si allega il documento di politiche di sicurezza a cui il fornitore dovrà essere adeguato

In allegato il documento che richiama l'ICT.

per la risposta al quesito n. 2)

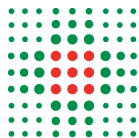
Le politiche a cui conformarsi sono quelle dell'azienda committente; si allega il documento di politiche di sicurezza a cui il fornitore dovrà essere adeguato .

In allegato il documento che richiama l'ICT.

Evidenziato che alle risposte suindicate è allegato il documento denominato “Politiche di sicurezza” che sarà pubblicato e reso noto a tutti i concorrenti;

Preso atto che le suddette risposte ai chiarimenti unitamente al documento “Politiche di sicurezza” saranno pubblicate e rese note in ossequio ai principi della concorrenza, massima partecipazione, parità di condizioni, pubblicità, trasparenza;

Considerato necessario:



1) modificare i termini di presentazione dell'offerta dal giorno 15/10/2026 ore 16:00 al giorno **22/10/2026 ore 16:00** per consentire agli operatori economici di prendere visione delle risposte e del documento "Politiche di sicurezza" allegato e tenerne conto in sede di formulazione dell'offerta;

2) posticipare la seduta virtuale per l'apertura delle buste amministrative al **23/10/2026 alle ore 10:00**, in luogo del 16/10/2026 alle ore 10:00

Dato atto che, in seguito a quanto sopra esposto, verrà data comunicazione sul portale Sater di Intercenter, dove si sta svolgendo la procedura di gara, e sul profilo del committente di questa Azienda USL;

Ritenuto pertanto di modificare i documenti di gara come sopra riportato e di procrastinare il termine di scadenza;

Viste le funzioni unificate del SAAV;

Determina

per le motivazioni espresse in premessa, da intendersi qui richiamate:

1) di approvare relativamente alla procedura fornitura in "SERVICE DI SISTEMI ANALITICI DI CITOFLUORIMETRIA PER LE ESIGENZE DELLE AZIENDE DELL'AREA VASTA EMILIA CENTRO (AVEC)", la modifica parziale della documentazione di gara e precisamente:

per la risposta al quesito n. 1)

Le politiche a cui conformarsi sono quelle dell'azienda committente; si allega il documento di politiche di sicurezza a cui il fornitore dovrà essere adeguato

In allegato il documento che richiama l'ICT.

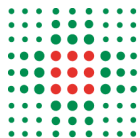
per la risposta al quesito n. 2)

Le politiche a cui conformarsi sono quelle dell'azienda committente; si allega il documento di politiche di sicurezza a cui il fornitore dovrà essere adeguato .

In allegato il documento che richiama l'ICT.

2) di dare atto che il documento denominato "Politiche di sicurezza" sarà pubblicato e reso noto a tutti i concorrenti unitamente alle risposte ai chiarimenti in parola;

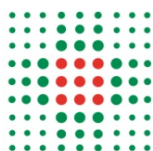
3) di modificare il termine di presentazione dell'offerta economica dal 15/10/2026 ore 16:00 al giorno **22/10/2026 ore 16:00** e la seduta virtuale di apertura delle offerte dal 16/10/2026 ore 10:00 al **23/10/2026 ore 10:00**;



- 4) di pubblicare sia sul profilo del committente dell'Azienda USL di Bologna sia su Piattaforma SATER le suddette variazioni, per consentire alle ditte di formulare correttamente l'offerta;
- 5) di dare atto che la presente determinazione sarà pubblicata, ai sensi dell'art.28 del D.lgs 36/2023, sul profilo del committente, sezione Amministrazione Trasparente dell'Azienda USL di Bologna;
- 6) di dare inoltre atto che la presente determinazione sarà pubblicata all'Albo Informatico consultabile sul sito istituzionale dell'Azienda USL di Bologna;
- 7) di dare infine atto che il redattore del presente atto è la Sig.ra Silvia Mingardi del SAAV.

Responsabile del procedimento ai sensi della L. 241/90:
Anna Maria Testa

Firmato digitalmente da:
Antonia Crugliano



Politiche Di Sicurezza

Data	Versione.	Descrizione della revisione		Paragrafi rev.
23/09/2026	02	Aggiornamento del documento		tutti
DATA ultima revisione: 23/09/2026	NUMERO ultima revisione: 02	Redatta da:	Gruppo Aziendale sulla Sicurezza Informatica dell'Azienda USL di Bologna	
		Verificata da:	Gruppo Aziendale sulla Sicurezza Informatica dell'Azienda USL di Bologna	
		Approvata da:	Direzione aziendale	

Politica di Sicurezza.....	1
Principi generali, governance e framework di riferimento	1
Controllo degli accessi e identità degli utilizzatori dei sistemi.....	2
Protezione dei dati, degli asset e supporto alla ricerca	2
Sicurezza operativa e delle reti	3
Consapevolezza e risposta agli incidenti	3
Sicurezza fisica e della catena di fornitura (third-party risk).....	3
Distribuzione del presente documento	4

Politica di Sicurezza

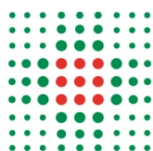
Principi generali, governance e framework di riferimento

P1: La sicurezza è responsabilità di tutti: ogni dipendente, collaboratore o fornitore con accesso ai sistemi aziendali è responsabile della protezione del patrimonio informativo.

P2: Approccio basato sul rischio: le misure di sicurezza sono implementate e aggiornate in base all'analisi periodica dei rischi al fine di garantire, prioritariamente, la sicurezza dei pazienti (Patient Safety Risk) e degli operatori sanitari.

P3: Conformità normativa e standard: l'azienda si impegna a rispettare le leggi vigenti in materia di protezione dei dati personali trattati nell'ambito dell'attività istituzionale resa e le normative di settore, con specifico riferimento ai requisiti della Direttiva NIS2.

P4: Governance e Comitato di Sicurezza: è istituito il Gruppo Aziendale di Sicurezza delle Informazioni. Questo garantisce un modello di governance in cui la sicurezza supporta direttamente



la salute del paziente, la compliance e l'operatività clinica proteggendola senza bloccarla. Gli obiettivi di sicurezza vengono riesaminati annualmente dalla direzione.

Controllo degli accessi e identità degli utilizzatori dei sistemi

P5: Principio del minimo privilegio: gli utenti ricevono i permessi di accesso alle informazioni strettamente necessari a svolgere le proprie mansioni lavorative.

P6: Autenticazione forte: l'accesso a qualsiasi sistema o informazione richiede una fase di autenticazione. In ragione della valutazione del rischio, bilanciata da criteri di opportunità ed usabilità si adotta una strategia a più fattori, MFA – Multi Factor Authentication -, per la mitigazione dei rischi individuati.

P7: Gestione delle credenziali: è vietato condividere le password aziendali o utilizzarle per account personali esterni all'Azienda.

P8: Revoca tempestiva: gli accessi logici e fisici vengono revocati immediatamente al momento della cessazione del rapporto di lavoro o della collaborazione.

Protezione dei dati, degli asset e supporto alla ricerca

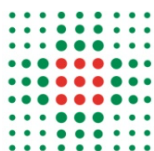
P9: Ciclo di vita delle informazioni: l'azienda gestisce le informazioni in tutto il loro ciclo di vita, dal momento in cui esse nascono o vengono acquisite, al momento in cui vengono gestite nel rispetto dei vincoli di conoscibilità secondo un principio di minimo privilegio (least privilege), avendo cura di preservarne l'integrità e la correttezza; le informazioni vengono eliminate nel rispetto delle politiche di conservazione definite dall'azienda;

P10: Classificazione delle informazioni e impatto clinico: tutti i dati aziendali devono essere classificati in base al rischio e protetti secondo il loro livello di sensibilità.

P11: Crittografia obbligatoria: i dati personali e i dati particolari (quindi anche i dati sanitari) devono essere cifrati sia quando sono memorizzati ("at rest", cioè quando risiedono nelle banche dati) sia quando vengono trasmessi ("in transit", cioè quando vengono trasmessi in rete).

P12: Data Masking e Ricerca Sicura: il supporto alle attività di ricerca scientifica deve avvenire in modo sicuro attraverso l'impiego obbligatorio di strumenti di Data Masking e pseudonimizzazione, consentendo l'analisi dei dati senza esporre le identità dei pazienti o dati personali o particolari in genere.

P13: Uso dei dispositivi aziendali e divieto di Shadow IT: i computer e i dispositivi di comunicazione forniti dall'azienda devono essere utilizzati solo per scopi professionali e non possono essere modificati senza autorizzazione. È vietato utilizzare software, servizi cloud o strumenti hardware non esplicitamente approvati dalle Tecnologie Informatiche e di Comunicazione.



Sicurezza operativa e delle reti

P14: Gestione delle vulnerabilità: tutti i sistemi, i software e i dispositivi devono essere mantenuti aggiornati con adeguate politiche di patching e sicurezza applicativa.

P15: Architettura Zero Trust e Isolamento dei dispositivi medici: la rete aziendale deve essere segmentata secondo un approccio "Zero Trust" in cui la rete interna non è considerata a priori sicura. La rete dei dispositivi medici deve essere isolata dalla rete amministrativa e da quella pubblica (ospiti) per ridurre la superficie di attacco.

P16: Continuità operativa e Disaster Recovery: tutti i dati personali aziendali devono essere sottoposti a backup regolari e testati periodicamente per il ripristino. Il piano di Business Continuity (BC) deve garantire un livello accettato di continuità operativa. Il piano di Disaster Recovery (DR) deve essere predisposto e testato periodicamente, misurando la capacità di recuperare tutti i dati pregressi e i tempi di ripristino dei sistemi critici rispetto alle specifiche soglie massime accettate.

Consapevolezza e risposta agli incidenti

P17: Cultura della Sicurezza (Security Awareness): tutto il personale aziendale o che comunque utilizza i sistemi aziendali deve partecipare ai corsi di formazione continua e alle simulazioni di sicurezza. La formazione deve esplicitare chiaramente quali siano le conseguenze per la sicurezza e l'operatività dell'azienda in caso di adozione di comportamenti non corretti.

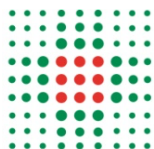
P18: Segnalazione tempestiva e monitoraggio (SOC 24/7): qualsiasi evento sospetto, anomalia o potenziale violazione deve essere segnalata immediatamente al team di sicurezza, per il tramite dell'Help Desk aziendale. È attivo un servizio SOC (Security Operations Center) 24/7 di monitoraggio continuo degli eventi di sicurezza per intercettare e bloccare tempestivamente le minacce prima che si trasformino in un blocco totale dei sistemi.

P19: Piano di Risposta agli Incidenti: l'azienda mantiene attivo un piano di risposta agli incidenti che integra procedure di continuità operativa e di recupero da disastro. Qualora il sistema informatico non sia disponibile, il personale deve essere addestrato e sapere come passare alla modalità di emergenza per non interrompere le cure, tutelare la salute del paziente e la sicurezza degli operatori.

Sicurezza fisica e della catena di fornitura (third-party risk)

P20: Protezione fisica: l'accesso ai locali aziendali e in particolare alle aree critiche, come le *server room* eventualmente presenti in Azienda, è limitato e monitorato.

P21: Gestione del Rischio dei Fornitori (Third-Party Risk): i fornitori terzi e i collaboratori esterni (inclusi manutentori di apparecchiature, fornitori di software, di servizi di telemedicina, di telecomunicazioni, di servizi cloud e di servizi informatici indispensabili) che trattano dati aziendali o accedono ai sistemi devono garantire standard di sicurezza equivalenti a quelli stabiliti da questa politica. È indispensabile l'inserimento di requisiti stringenti di cybersecurity nei bandi di gara e l'esecuzione di audit periodici sui livelli di sicurezza garantiti dalle terze parti.



Distribuzione del presente documento

Il presente documento è condiviso con tutti i dipendenti ed in via generale mantenuto all'interno della Intranet aziendale all'indirizzo

https://intranet.internal.ausl.bologna.it/servizi/dip/dip_tecn_patr/serv_ced/cy-se