U.O.C. Sistemi informativi e Controllo di Gestione

CONDIZIONI PARTICOLARI DI FORNITURA

Oda 9174188

Periodo: 01.01.2027-31.12.2029

SAT-3 - Sistema Informatico per la gestione trasporti.

Sommario

Art 1. OGGETTO DELLA FORNITURA 3
Art 2. DESCRIZIONE DEL SERVIZIO 3
2.1. LICENZE 3
2.2. MANUTENZIONE TECNICA E CONDUZIONE 3
2.3. SERVIZIO DI ASSISTENZA 5
2.4. AVVICENDAMENTO CONTRATTUALE 7
2.5. SERVIZIO OPZIONALE DI SUPPORTO SPECIALISTICO / MANUTENZIONE EVOLUTIVA 8
Art 3. LIVELLI DI SERVIZIO RICHIESTI 8
Art 4. DURATA DEL CONTRATTO 10
Art 5. VALORE DEL CONTRATTO 10
Art 6. MODALITÀ DI FATTURAZIONE 12
Art 7. RESPONSABILITÀ DEL FORNITORE 13
Art 8. PENALI 14
Art 9. RISERVATEZZA E TRATTAMENTO DATI PERSONALI 17
Art 10. MISURE DI SICUREZZA INFORMATICA 18
Art 11. BREVETTI INDUSTRIALI E DIRITTO D'AUTORE 19
Art 12. RESPONSABILE DEL SERVIZIO 19
Art 13. GARANZIA DEFINITIVA 19
Art 14. DOCUMENTAZIONE AMMINISTRATIVA 19
Art 15. RISOLUZIONE DEL CONTRATTO E CLAUSOLE RISOLUTIVE ESPRESSE 20
Art 16. FORO COMPETENTE 21
Art 17. TRATTAMENTO DATI PERSONALI DEL FORNITORE 21
ALLEGATO A "NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI " 22
ALLEGATO B "PATTO DI INTEGRITA' " ..... **Errore. Il segnalibro non è definito.**

ALLEGATO C “DISCIPLINARE TECNICO PER L’INTEGRAZIONE DI SISTEMI CON L’INFRASTRUTTURA IT DELL’AZIENDA USL UMBRIA 1 “..... **Errore. Il segnalibro non è definito.**

Art 1. OGGETTO DELLA FORNITURA

Il presente documento disciplina i rapporti tra l'Azienda USL Umbria 1 (in seguito denominata anche "Azienda" o "Stazione appaltante" o "S.A.") e l'operatore economico aggiudicatario dell'appalto (in seguito denominato anche "Fornitore" o "Appaltatore" o "Affidatario"), per l'affidamento dei servizi di conduzione, manutenzione, gestione ed assistenza tecnica di tutte le componenti, nessuna esclusa, del sistema in oggetto:

- Evoluzione dei programmi applicativi software di gestione dei trasporti sanitari aziendali effettuati con mezzi propri "SAT1" o mediante servizi in convenzione "SAT2" in unico programma denominato SAT per aderire ai nuovi standard di sicurezza NIS2 ed a nuove implementazioni;

Art 2. DESCRIZIONE DEL SERVIZIO

2.1. LICENZE

Le licenze per l'uso del sistema in oggetto sono di proprietà dell'USL Umbria per numero illimitato di utenti.

2.2. MANUTENZIONE TECNICA E CONDUZIONE

In relazione all'oggetto del presente documento, il Fornitore si obbliga ad effettuare le seguenti tipologie di prestazioni:

- Manutenzione PREVENTIVA: messe a punto, controllo e supervisione dei sistemi, dei database e degli applicativi, per prevenire l'insorgenza di guasti e mantenere il sistema in condizioni funzionali adeguate all'uso e regolarmente operativo.
- Manutenzione CORRETTIVA (su chiamata): verifica e risoluzione di eventuali malfunzionamenti segnalati dagli Utenti, consistente in un numero illimitato di interventi per l'eliminazione di malfunzionamenti e/o guasti che si verificassero durante il corretto utilizzo dei sistemi.
- Manutenzione ORDINARIA: piccole migliorie di carattere ordinario, adeguamento delle tabelle di configurazione dei database (es.: prestazioni, utenti, filtri, …), delle 'intestazioni pagina' delle stampe (es.: logo ospedaliero; recapiti, indirizzi e nominativi di Reparto). Adeguamenti a norma di legge compresi requisiti di sicurezza e riservatezza e ottimizzazione del database.

Nell'ambito dei servizi di manutenzione devono essere svolte, a titolo esemplificativo e non esaustivo, le seguenti principali attività:

- **Servizio di conduzione**
  Assistenza e riparazione ordinaria di guasti e anomalie segnalate dagli operatori.

Qualora esistente, l'ambiente di test dovrà essere allineato con l'ambiente di produzione in termini di configurazioni di prodotto ed infrastrutturali come il sistema operativo.

- **Assistenza e formazione**

  Con particolare riferimento all'introduzione di nuove significative revisioni software poste in essere nel periodo di validità del Servizio, l'operatore erogherà adeguate sessioni di aggiornamento formativo, concordate di volta in volta con il DEC.

- **Amministrazione del database**

  Il Fornitore deve svolgere tutte le attività di amministrazione del database e pertanto ne è responsabile per la creazione, configurazione, dimensionamento, monitoraggio e piena efficienza.

  La proprietà dei dati rimane in capo all'USL Umbria 1 a cui, su richiesta, deve essere data la possibilità di accedere all'intero database.

  Il Fornitore è responsabile della corretta descrizione ed implementazione delle procedure di salvataggio degli archivi e/o dati.

  Il Fornitore è altresì tenuto a comunicare tempestivamente tutte le modifiche necessarie alla corretta implementazione della procedura di backup.

- **Monitoraggio e reporting**

  Il Fornitore deve effettuare costanti controlli sul sistema (ad esempio: dimensioni del database, utilizzo delle risorse di elaborazione, analisi dei log, etc..) e monitorare il corretto funzionamento e la corretta parametrizzazione dello stesso.

  Il Fornitore è tenuto a mettere in atto le azioni migliorative necessarie al mantenimento dell'efficienza del sistema al variare delle condizioni e dei carichi di lavoro, dandone ove necessario comunicazione qualora sia indispensabile l'aumento di "risorse fisiche" come spazio HDD, RAM, CPU, Network, ecc…

  Il Fornitore deve effettuare il monitoraggio preventivo e periodico del sistema, anche mediante strumenti di monitoring automatico. Il Fornitore dovrà produrre un report sul monitoraggio effettuato, evidenziando eventuali anomalie e le azioni correttive intraprese. La produzione dei predetti report deve avvenire con periodicità trimestrale (o altra periodicità concordata) e comunque ogni qualvolta vengano richieste dalla USL Umbria1 per specifiche necessità (ad esempio in caso di blocchi totali/parziali del sistema o di integrazioni con altri sistemi informatici, verifica delle performance o delle vulnerabilità) entro i termini stabiliti dalla SA.

  Il Fornitore si impegna a comunicare repentinamente alle Aziende Sanitarie eventi che possono presupporre rischi per l'integrità, affidabilità e riservatezza dei dati e collaborare nel caso di Data Breach.

- **Aggiornamento del software:**

Sono ricompresi nel contratto tutti gli aggiornamenti del software necessari alle correzioni di anomalie rilevate, alle vulnerabilità legate alla sicurezza informatica e agli adeguamenti agli obblighi di legge.

Il Fornitore è tenuto inoltre a rendere disponibili senza ulteriori aggravi economici le evoluzioni del prodotto e/o nuove funzionalità o comunque nuove versioni, ivi comprese le attività di installazione, configurazione e migrazione eventualmente necessarie.

Gli aggiornamenti e/o le nuove funzionalità devono essere sempre effettuati concordando con l'Azienda Usl le modalità operative. Rimane facoltà dell'Azienda decidere se accettare/installare o meno tali release sulla base di specifiche valutazioni tecniche.

Qualora le attività sopracitate non siano possibili in teleassistenza, il Fornitore è tenuto ad intervenire sul luogo. L'intervento viene concordato preventivamente con le Aziende Sanitarie che garantisce la disponibilità del sistema e la presenza di un proprio referente.

- Supporto tecnico per attività sistemistiche

Il Fornitore deve garantire supporto tecnico in caso di:

- riavvio di server o di servizi della soluzione;
- migrazioni o modifiche/aggiornamenti dei componenti dell'infrastruttura, inclusa l'eventuale reinstallazione e configurazione dell'applicativo su nuovi ambienti nel caso in cui l'attuale ambiente non rispetti più le norme in ambito di sicurezza informatica e trattamento dei dati, per disposizioni aziendali/regionali, per la corretta esecuzione dell'applicativo in modo da non bloccare o rallentare l'operatività giornaliera del servizio Trasfusionale/centri raccolta sangue;
- qualunque eventualità sopraggiunta e strettamente necessaria/obbligatoria (es: sistemi operativi obsoleti ecc.)
- effettuazione di simulazioni di ripristino dell'intero sistema (utile per simulare ripristini da backup in cloud).

In caso di eventuale restore da backup, dovrà garantire pieno supporto tecnico fino al completo ripristino del servizio/sistema.

Il supporto tecnico per attività sistemistiche dovrà essere pianificato in modo da ridurre al minimo l'impatto del disservizio e comunque in accordo con l'Azienda.

2.3. SERVIZIO DI ASSISTENZA

Il servizio viene erogato, mediante richiesta della Usl Umbria1 sia in forma verbale o scritta e sarà inviata al 'Servizio Assistenza Clienti MICRA', ai recapiti alternativi indicati:

UBICAZIONE Via Gramsci, 6, Corciano (Pg)

RECAPITI Tel.: +39 075 9288501

e-Mail: micra@micra.it
nei seguenti orari: dal lunedì al venerdì, dalle 09.00 alle 13.00 e dalle ore 14.00 alle 18.00.

Il servizio comprende le seguenti attività:

a) Ricevimento delle segnalazioni di guasti, anomalie, blocchi o malfunzionamenti del sistema;
b) Diagnosi del guasto o dell'anomalia, verifica dell'eventuale coinvolgimento di sistemi e fornitori terzi con i quali il Fornitore è tenuto a collaborare direttamente, per la definizione della corretta diagnosi;
c) Ripristino delle funzionalità a seguito di segnalazioni di anomalie, malfunzionamenti o blocco del sistema;
d) Superamento di situazioni bloccanti e malfunzionamenti;
e) Indicazione di eventuali operazioni o accorgimenti utili all'eliminazione dell'anomalia;
f) Aggiornamento e configurazione ad hoc dei modelli/strutture delle stampe quotidianamente utilizzate dal servizio;
g) Attività di creazione, configurazione e profilatura degli utenti;
h) Attività di creazione, configurazione e gestione della reportistica;
i) Assistenza e supporto tecnico in caso di gravi anomalie o malfunzionamenti del sistema che, pur non derivanti da malfunzionamenti del software oggetto della fornitura, possono compromettere la continuità dell'utilizzo del sistema;
j) Assistenza e supporto tecnico in caso di riavvio dei server o di servizi, determinati da attività sistemistiche programmate o da sinistri che hanno impatto sull'infrastruttura;
k) Supporto all'Azienda per lo svolgimento delle attività richieste dal GDPR in relazione ai diritti dell'interessato, come descritte nel successivo art. 9;
l) Estrazione dei log di sistema per i dovuti controlli, come descritti nel successivo 0.

Nel caso di anomalie del software, la risoluzione potrà essere fornita mediante correzione della versione corrente del software oltre che mediante l'aggiornamento di versione;

Le chiamate al servizio saranno effettuate dai Referenti designati dall'Azienda Usl che ha in carico il 1° Livello di assistenza;

Per segnalazioni non critiche e pianificabili (livello 5 della successiva classificazione) le richieste potranno essere segnalate via email ad apposita casella di posta elettronica o apposito sistema di gestione dei ticket che dovrà essere reso disponibile dal Fornitore. Il Fornitore, qualora la Usl Umbria 1 ne facesse espressa richiesta, si renderà disponibile ad utilizzare il sistema di gestione dei ticket della Usl.

Il Customer Service è tenuto a classificare tutte le segnalazioni pervenute dall'Azienda, sulla base dei parametri impatto ed urgenza, in base ai seguenti 5 LIVELLI DI PRIORITÀ di intervento, dal più grave al meno grave:

- Livello 1 Emergency: l'intero sistema è indisponibile agli utenti;
- Livello 2 Critical: almeno una delle funzionalità critiche del sistema è indisponibile a tutti gli utenti;
- Livello 3 Normal: una o più funzionalità non critiche sono indisponibili agli utenti, oppure una funzionalità critica non è disponibile ad una parte degli utenti o solo per specifici episodi;
- Livello 4 Low: una o più funzionalità non critiche del sistema sono indisponibili, ma senza impatto sulla operatività degli utenti;
- Livello 5 Planned: nessuna funzionalità del sistema è indisponibile.

Il Fornitore è tenuto a comunicare all'Azienda l'orario di presa in carico della segnalazione ed il relativo livello di priorità assegnato. In assenza della specifica identificazione di funzionalità critica o non critica, le segnalazioni riguardanti funzionalità bloccanti saranno considerate critiche.

2.4. AVVICENDAMENTO CONTRATTUALE

In caso di passaggio di esecuzione del servizio dall'appaltatore del presente contratto ("appaltatore uscente") a un nuovo appaltatore ("appaltatore entrante"), deve essere garantito dall'appaltatore uscente piena collaborazione e supporto per la continuità operativa.
Il servizio include almeno:

- Trasferimento di tutte le conoscenze necessarie a garantire la fluida transizione nell'erogazione e la continuità operativa per l'utenza dei servizi in fornitura del Committente;
- Fornitura delle specifiche ed i protocolli di interfaccia per il trasferimento dei dati e il supporto per la migrazione di tutti i dati;
- quanto altro ritenuto funzionale e necessario alla gestione complessiva del servizio in continuità operativa.

La consegna di quanto sopra previsto da parte dell'Appaltatore uscente alla Stazione Appaltante, sarà attestata con apposito verbale di accertamento redatto congiuntamente da Stazione Appaltante, Appaltatore uscente e Appaltatore entrante. Il verbale evidenzierà qualità e grado di completezza dei dati e delle informazioni consegnate e della documentazione ad essi associata.
La realizzazione della strategia di uscita non deve essere subordinata a nessuna condizione e garantita, da un punto di vista tecnico, fin da subito attraverso chiare specifiche di progetto.

Il Fornitore si impegna in caso di passaggio ad un nuovo Fornitore a supportare l'Azienda nella migrazione del sistema per un periodo massimo di 6 mesi dalla conclusione del presente contratto.
Il pagamento dell'ultima fattura è subordinato alla conclusione del servizio in questione.
Quanto soggetto a trasferimento e le attività conseguenti, potranno essere rimodulati in funzione delle peculiarità logistico-organizzative del nuovo servizio contrattualizzato con il Fornitore entrante, e all'uopo, l'Azienda fornirà per tempo le indicazioni necessarie.
L'Appaltatore uscente deve garantire l'esecuzione di ogni attività conclusiva, anche non prevista nel presente contratto, se necessaria all'efficace avvicendamento con il Fornitore entrante, anche in conformità a quanto previsto dal Manuale Applicativo N. 7 relativo al Governo dei Contratti ICT ex CNIPA (cfr. par.4.2.5 "Gestire l'avvicendamento contrattuale").

2.5. SERVIZIO OPZIONALE DI SUPPORTO SPECIALISTICO / MANUTENZIONE EVOLUTIVA

Sono richiesti servizi applicativi da effettuarsi mediante giornate professionali di tecnico specialista di prodotto, finalizzate ad attività di manutenzione evolutiva, parametrazione, formazione ed integrazione con altri applicativi aziendali. l'Azienda si riserva di richiedere o meno le giornate professionali sulla base di esigenze che insorgeranno nel periodo contrattuale fino ad un massimo di n. 6 gg complessive.

Per l'espletamento delle attività previste al presente paragrafo L'Azienda richiederà le giornate professionali sulla base di specifici progetti condivisi con il Fornitore. La conclusione delle attività dovrà essere sempre certificata da rapporti di intervento e verbale di accettazione sottoscritto dal Direttore di Esecuzione del Contratto o dal Responsabile Unico del Procedimento.

Art 3. LIVELLI DI SERVIZIO RICHIESTI

Il Fornitore si impegna a gestire con tempestività e professionalità tutte le segnalazioni di problemi, anomalie o richieste riguardanti il software, che giungono alla sua attenzione e, comunque, nel rispetto dei livelli di servizio definiti dal presente contratto.
Tutte le segnalazioni devono essere classificate in base all'impatto e all'urgenza che hanno sulla Stazione Appaltante, e viene loro assegnato un livello di priorità corrispondente. Al momento dell'invio della richiesta di assistenza, la Stazione Appaltante stabilisce il livello di priorità iniziale. Successivamente, tale livello può essere modificato in base alla valutazione del problema effettuata da un tecnico dell'Appaltatore, previa approvazione della Stazione Appaltante.

I fini della valutazione della qualità del servizio si definiscono i seguenti indicatori:

- TEMPO DI PRESA IN CARICO: tempo che intercorre tra la segnalazione all'Help Desk da parte dell'Utente via telefono e/o via e-mail) e la presa in carico dello stesso con comunicazione all'Azienda della registrazione dell'evento e dell'assegnazione del livello di priorità.
- TEMPO DI RISOLUZIONE: tempo che intercorre tra la presa in carico e la relativa risoluzione, che può avvenire anche mediante applicazione di una soluzione temporanea che permette di ripristinare l'operatività del servizio pur non risolvendo la causa che ha scatenato il problema.

Il Fornitore dovrà garantire i seguenti tempi di presa in carico e di risoluzione dell'anomalia da computarsi a far tempo dall'ora di ricevimento della richiesta al Call Center/ invio della richiesta via email/sistema di gestione dei ticket, per la determinazione dell'orario di risoluzione, in caso di contestazione potranno essere utilizzati i log di sistema;

GUASTO o ANOMALIA	PRESA IN CARICO	RISOLUZIONE
guasti o anomalie di livello 1 e 2	entro 4 ore* dalla chiamata	entro 1 gg lavorativi dalla presa in carico
guasti o anomalie di livello 3	entro 1 giorno lavorativo dalla chiamata	entro 2 gg lavorativi dalla presa in carico
guasti o anomalie di livello 4 e 5	entro 2 giorno lavorativo dalla richiesta	Entro 5 gg lavorativi dalla presa in carico

*per il conteggio si considerano le ore lavorative negli orari e nei giorni indicati al punto "2.5 modalità di erogazione".

In caso di ritardi nella risoluzione di una segnalazione, il Fornitore è tenuto a informare tempestivamente la Stazione Appaltante, indicando le cause del ritardo e i tempi previsti per la soluzione del problema.

Il Fornitore è tenuto a tracciare e documentare tutte le segnalazioni, dalle fasi di presa in carico alla risoluzione finale. A tal fine, è auspicabile un sistema di trouble ticketing

In caso di ritardi nella risoluzione di una segnalazione, il Fornitore è tenuto a informare tempestivamente la Stazione Appaltante, indicando le cause del ritardo e i tempi previsti per la soluzione del problema.

Il Fornitore è tenuto a tracciare e documentare tutte le segnalazioni, dalle fasi di presa in carico alla risoluzione finale.

La Stazione Appaltante potrà chiedere periodicamente report sulle segnalazioni aperte, la loro tipologia e i relativi tempi di risoluzione.

Per la determinazione degli orari in questioni, in caso di contestazione potranno essere utilizzati i log di sistema.

In caso d'inadempienza dell'Appaltatore, resta ferma la facoltà della Stazione Appaltante di ricorrere a terzi per l'esecuzione dei servizi di cui al presente capitolato addebitando all'Appaltatore i relativi costi sostenuti maggiorati del 25%.

Art 4. DURATA DEL CONTRATTO

La durata dell'appalto è di n. 36 mesi a decorrere dalla data del 1.1.2027.

E' ammessa la facoltà di rinnovo del servizio per ulteriori n. 12 mesi ai sensi dell'art.120, comma 1 lett. a) del D.Lgs 36/2023 alle medesime condizioni. La facoltà di esercitare l'opzione di ripetizione del contratto è in capo all'USL UMBRIA 1.

La durata del contratto potrà essere prorogata, in corso di esecuzione, per non oltre 12 mesi e comunque per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione del nuovo contraente ai sensi dell'art. 120, comma 10 del Dlgs 36/2023. In tal caso il contraente è tenuto all'esecuzione delle prestazioni oggetto del contratto agli stessi prezzi patti e condizioni o più favorevoli.

È ammessa l'esecuzione del contratto anticipata delle prestazioni contrattuali, nelle more della sottoscrizione del relativo contratto, nelle ipotesi e secondo le prescrizioni di cui all'art. 17, c.8 del D.lgs. n. 36/2023.

L'USL Umbria 1 si riserva la facoltà di recesso qualora nel periodo di esecuzione intervenga l'attivazione di uno strumento contrattuale offerto da CONSIP SpA (convenzione, accordo quadro, sistema dinamico di acquisizione) o da CRAS/PuntoZero Scarl, o da nuovi strumenti contrattuali previsti nell'ambito del PNRR o comunque per mutate esigenze dell'Azienda ovvero in caso di mutamenti di carattere organizzativo aventi incidenza sull'esecuzione della fornitura.

Il Fornitore, qualora richiesto dall' Azienda Usl Umbria 1, si obbliga a garantire una proroga dell'espletamento del servizio alle medesime condizioni al fine di consentire la conclusione della nuova procedura di affidamento.

Art 5. VALORE DEL CONTRATTO

L'importo complessivo massimo presunto per ciascun applicativo per ogni anno è

€ 48.000,00	SAT Implementazione
€ 5.500,00	SAT assistenza annuale

Pertanto l'importo complessivo massimo presunto per l'intera durata dell'appalto è

Importo	Periodo
€53.500,00	I anno (servizi per l'avvio del nuovo sistema e canoni assistenza annuale)
€ 5.500,00	II anno manutenzione
€ 5.500,00	III anno manutenzione
€5.500,00	n.12 mesi proroga ai sensi dell'art. 120, comma 10 del D.lgs. 36/2023 *[eventuale-opzione]*
€ 70.000,00	Totale oltre iva

Il suddetto importo, calcolato ai sensi dell'art. 14 comma 4 del D. Lgs. 36/2023, comprende:

- i costi della manodopera e gli oneri aziendali per l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro. Nell'offerta economica l'operatore indica, a pena di esclusione, i predetti costi eccetto che nelle forniture senza posa in opera e nei servizi di natura intellettuale *(art.108 c.9 del D. Lgs. 36/2023);*
- i costi di sicurezza di natura interferenziale che ammontano complessivamente ad € 0,00 (IVA esclusa) per tutta la durata dell'appalto trattandosi di fornitura di beni senza messa in opera;
- i costi, espressi e non, derivanti per adempiere a tutto quanto richiesto dal servizio oggetto dall'appalto e necessari per assicurare la perfetta esecuzione del servizio;
- i costi delle licenze dei prodotti software necessari all'esecuzione dell'applicativo offerto (con particolare riguardo a DBMS, application server, ecc.):
- *[eventuale-opzione]* il valore del costo per eventuale proroga ai sensi art. 120, comma 10 del Dlgs 36/2023 n.12 mesi;

Il Fornitore è tenuto ad eseguire tutte le prestazioni oggetto di fornitura a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel presente documento e nell'offerta, pena la risoluzione di diritto del contratto medesimo.

In ogni caso, il Fornitore si obbliga ad osservare nell'esecuzione delle prestazioni contrattuali tutte le norme e tutte le prescrizioni tecniche e di sicurezza in vigore, nonché quelle che dovessero essere emanate in corso di esecuzione del contratto.

Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula del contratto, resteranno ad esclusivo carico del Fornitore, intendendosi in ogni caso remunerati con il corrispettivo fissato contrattualmente.

Art 6. MODALITÀ DI FATTURAZIONE

L'emissione della fattura potrà avvenire solo successivamente al completamento della fornitura dei servizi ed alla verifica della corretta esecuzione accertata con apposito verbale della stazione appaltante.

La fatturazione dei servizi a canone seguirà una periodicità semestrale posticipata.

La liquidazione e il conseguente pagamento delle somme dovute avverranno entro 60gg dal ricevimento della fattura (ai sensi dell'art. 4 c.5 lett. b) del D.Lgs 231/2002 e s.m.i.) previo:

- esito positivo della verifica di conformità, diretta a certificare che le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni del contratto, nonché nel rispetto delle vigenti normative e delle eventuali leggi di settore;
- esito positivo della verifica contabile, diretta a verificare che gli importi fatturati siano rispondenti alle prestazioni erogate;
- esito positivo della verifica di regolarità contributiva (DURC) dell'appaltatore, dei subappaltatori e delle imprese ausiliarie;
- *(in caso di subappalto)* certificazione dell'avvenuto pagamento di quanto dovuto dall'Appaltatore al subappaltatore (anche secondo le disposizioni della tracciabilità dei flussi finanziari di cui alla Legge 136/2010); resta ferma quanto previsto dall'art.105 del D.Lgs n.50/2016;
- *(in caso di avvalimento)* certificazione dell'avvenuto pagamento di quanto dovuto dall'Appaltatore all'impresa ausiliaria secondo quanto previsto dal relativo contratto di avvalimento;
- rispetto di ulteriori eventuali obblighi normativi.

I termini di pagamento decorrono dalla data di ricevimento della fattura da parte dell'ufficio protocollo della USL, ovvero dalla data di accertamento da parte del direttore dell'esecuzione della rispondenza alle

prescrizioni contrattuali della prestazione effettuata nel mese di riferimento, se la fattura è ricevuta in epoca antecedente.

In caso si verificasse almeno una delle perdette condizioni, il termine di pagamento si intende sospeso dall'invio della contestazione fino al 30° giorno dopo la ricezione da parte della Azienda USL della comunicazione del Fornitore, di accettazione della contestazione o delle notizie aggiuntive che consentano di dichiarare la fornitura "regolarmente eseguita" e/o la fattura conforme alle disposizioni contrattuali.

L'Azienda, in fase di liquidazione delle prestazioni contrattuali, opererà le ritenute obbligatorie per legge sull'importo netto delle prestazioni secondo quanto previsto dalle normative vigenti o che entreranno in vigore durante l'esecuzione del contratto.

Le fatture dovranno contenere le seguenti informazioni:

- "Tripletta" (art.3 del DM 7.12.2018):
  - Numero di Ordine NSO (esempio 0500XXXXX/A0A/001): campo <DatiOrdineAcquisto> <IdDocumento>
  - codice univoco di fatturazione: UF9FAJ campo <DatiOrdineAcquisto> <CodiceCommessaConvenzione>;
  - data ordine: campo <DatiOrdineAcquisto> <Data>;
- Codice CIG (campo <DatiOrdineAcquisto><CodiceCIG>);
- PIVA Committente: 03301860544;
- Codice Fiscale Committente: 03301860544;
- Applicazione della scissione dei pagamenti ai sensi dell'art. 17- ter del D.P.R. n. 633/1972 (c.d. split payment);
- Descrizione della prestazione eseguita, imponibile e IVA.

La Stazione Appaltante si riserva la possibilità di accogliere modifiche alle modalità di fatturazione proposte dall'Appaltatore.

Art 7. RESPONSABILITÀ DEL FORNITORE

Il Fornitore dichiara di possedere tutte le autorizzazioni e le competenze necessarie per l'espletamento dei servizi oggetto del presente contratto e si impegna a svolgere i propri compiti in modo diligente, professionale e in conformità alle leggi applicabili.

Il Fornitore risponde di tutti i danni diretti, indiretti e consequenziali di qualsiasi natura causati alla Stazione Appaltante, ai suoi dipendenti e ai terzi, per la propria responsabilità anche derivante da atti, fatti o omissioni dolose o colpose commessi dalle persone di cui deve rispondere il Fornitore, nell'esecuzione delle attività oggetto del presente contratto. Il Fornitore garantisce inoltre di adottare

tutte le misure necessarie per evitare danni ai dati, alle applicazioni e ai sistemi informatici della Stazione Appaltante e dei terzi, conseguenti allo svolgimento dell'attività ai sensi del presente contratto.

Art 8. PENALI

In caso di riscontrata irregolarità nell'esecuzione del servizio o di mancato rispetto delle disposizioni contenute nel presente documento e nelle eventuali parti integrative e migliorative contenute nell'Offerta Tecnica, l'Appaltatore è tenuto al pagamento di una penale calcolata in rapporto alla gravità dell'inadempienza e alla recidiva fatta salva la risoluzione del contratto.

Le penalità saranno precedute da regolare contestazione dell'inadempienza. L'Appaltatore è tenuto a fornire giustificazioni scritte e documentate, se richieste dalla Stazione Appaltante, in relazione alle contestazioni mosse. Se entro il termine previsto dalla Stazione Appaltante, di massimo 5 gg – termine ridotto in casi di urgenza, in base al caso specifico -, l'Appaltatore non produce alcuna comprovata giustificazione, la Stazione Appaltante applicherà le penali previste dal presente capitolato.

Le penali non si applicano nel caso in cui l'inesatto o mancato adempimento dell'Appaltatore sia determinato da cause di forza maggiore o impossibilità sopravvenuta alla stessa non addebitabili. Gli inadempimenti che l'Appaltatore ritiene ascrivibili a tali eventi devono essere segnalati, per iscritto, alla Stazione Appaltante entro 3 giorni lavorativi dall'inizio del loro avverarsi sotto pena di decadenza dal diritto al risarcimento.

In ogni caso per forza maggiore si intende ogni situazione o evento imprevedibile ed eccezionale, indipendente dalla volontà delle parti e non attribuibile ad una loro colpa o negligenza, che impedisca ad una delle parti di adempiere ad uno degli obblighi derivanti dal contratto, senza possibilità di ovviare a tale impedimento nonostante tutta la diligenza dispiegata. Se una delle parti si trova in caso di forza maggiore, ne avvisa senza indugio e nel più breve tempo possibile l'altra parte, precisando la natura, la durata possibile e gli effetti prevedibili di tale avvenimento.

In caso di recidiva nell'arco di 30 giorni, la penalità già applicata potrà essere aumentata fino al raddoppio.

Per gli inadempimenti di seguito elencati, la Stazione Appaltante potrà applicare, anche in maniera additiva, le seguenti penali:

In caso di riscontrata irregolarità nell'esecuzione del servizio o di mancato rispetto delle disposizioni contenute nel presente documento e nelle eventuali parti integrative e migliorative contenute nell'Offerta Tecnica, l'Appaltatore è tenuto al pagamento di una penale calcolata in rapporto alla gravità dell'inadempienza e alla recidiva fatta salva la risoluzione del contratto.

Le penalità saranno precedute da regolare contestazione dell'inadempienza. L'Appaltatore è tenuto a fornire giustificazioni scritte e documentate, se richieste dalla Stazione Appaltante, in relazione alle contestazioni mosse. Se entro il termine previsto dalla Stazione Appaltante, di massimo 5 gg – termine

ridotto in casi di urgenza, in base al caso specifico -, l'Appaltatore non produce alcuna comprovata giustificazione, la Stazione Appaltante applicherà le penali previste dal presente capitolato.

Le penali non si applicano nel caso in cui l'inesatto o mancato adempimento dell'Appaltatore sia determinato da cause di forza maggiore o impossibilità sopravvenuta alla stessa non addebitabili. Gli inadempimenti che l'Appaltatore ritiene ascrivibili a tali eventi devono essere segnalati, per iscritto, alla Stazione Appaltante entro 3 giorni lavorativi dall'inizio del loro avverarsi sotto pena di decadenza dal diritto al risarcimento.

In ogni caso per forza maggiore si intende ogni situazione o evento imprevedibile ed eccezionale, indipendente dalla volontà delle parti e non attribuibile ad una loro colpa o negligenza, che impedisca ad una delle parti di adempiere ad uno degli obblighi derivanti dal contratto, senza possibilità di ovviare a tale impedimento nonostante tutta la diligenza dispiegata. Se una delle parti si trova in caso di forza maggiore, ne avvisa senza indugio e nel più breve tempo possibile l'altra parte, precisando la natura, la durata possibile e gli effetti prevedibili di tale avvenimento.

In caso di recidiva nell'arco di 30 giorni, la penalità già applicata potrà essere aumentata fino al raddoppio.

Per gli inadempimenti di seguito elencati, la Stazione Appaltante potrà applicare, anche in maniera additiva, le seguenti penali:

Tabella 2 – Penali

EVENTO	INDICATORE	IMPORTO PENALE
Presa in carico per anomalie/segnalazioni di livello 1 e 2	Numero di ore oltre il livello di servizio richiesto (Tabella 1)	50 € per ciascuna ora di ritardo
Ripristino per anomale/segnalazioni di livello 3	Numero di ore oltre il livello di servizio richiesto (Tabella 1)	30 € per ciascuna ora di ritardo
Ripristino per anomale/segnalazioni di livello 4 e 5	Giorni di ritardo oltre il livello di servizio richiesto (Tabella 1)	100 € per ciascun giorno di ritardo
Blocco, anche parziale, dei servizi dovuto ad errata gestione del database o per carenza di monitoraggio del sistema	Verificarsi di un evento di blocco	500 € per ciascun evento bloccante occorso, l'importo è da sommare alle penali di eventuali ritardi di presa in carico e ripristino
Mancata assegnazione del livello di priorità o mancata comunicazione della presa in carico	Numero di ticket aperti privi di comunicazione della presa	100 € per ciascun evento aperto al call center

	in carico e/o del livello di criticità	mancante della comunicazione
Ottemperanza alle prescrizioni impartite dell'USL Umbria 1	Numero giorni di ritardo rispetto a quanto prescritto dalla stazione appaltante	200€ per ciascun giorno di ritardo
ciascuna violazione di norme contenute nel presente documento o nell'Offerta Tecnica dell'Appaltatore, non espressamente previste nelle penalità di cui sopra		un valore definito a discrezione della Stazione Appaltante in rapporto alla gravità dell'inadempimento.

In assenza della specifica identificazione di funzionalità critica o non critica, le segnalazioni riguardanti funzionalità bloccanti saranno considerate critiche.

In caso di ritardi nella risoluzione di una segnalazione, il Fornitore è tenuto a informare tempestivamente la Stazione Appaltante, indicando le cause del ritardo e i tempi previsti per la soluzione del problema.

Il Fornitore è tenuto a tracciare e documentare tutte le segnalazioni, dalle fasi di presa in carico alla risoluzione finale. A tal fine, dovrà essere utilizzato un sistema di trouble ticketing, messo a disposizione del Fornitore, che permetta la tracciabilità e la consultazione da parte della Stazione Appaltante delle segnalazioni, l'assegnazione delle priorità e la gestione dei tempi di risoluzione. Il Fornitore è tenuto a comunicare all'Azienda via mail o con altre eventuali modalità da concordare preventivamente, l'orario di presa in carico della segnalazione ed il relativo livello di priorità assegnato, nonché la risoluzione della segnalazione stessa.

La Stazione Appaltante potrà chiedere periodicamente report sulle segnalazioni aperte, la loro tipologia e i relativi tempi di risoluzione.

Per la determinazione degli orari in questioni, in caso di contestazione potranno essere utilizzati i log di sistema.

L'imposizione delle penali non impedisce l'applicazione delle norme di risoluzione contrattuale.

L'Azienda potrà compensare i crediti derivanti dall'applicazione delle penali di cui al presente articolo con quanto dovuto al fornitore a qualsiasi titolo ovvero in difetto avvalersi della cauzione senza bisogno di diffida ulteriore, accertamento o procedimento giudiziario.

La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso l'Appaltatore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

L'Appaltatore prende atto che l'applicazione delle penali previste dal presente articolo non preclude il diritto dell'Azienda a richiedere il risarcimento degli eventuali maggior danni.

In caso d'inadempienza dell'Appaltatore, resta ferma la facoltà della Stazione Appaltante di ricorrere a terzi per l'esecuzione dei servizi di cui al presente capitolato addebitando all'Appaltatore i relativi costi sostenuti maggiorati del 25%.

Art 9. RISERVATEZZA E TRATTAMENTO DATI PERSONALI

Con la stipula del contratto il Fornitore accetta la nomina come Responsabile esterno del trattamento dei dati personali necessari per svolgere le attività oggetto della fornitura ai sensi dell'art. 28 del GDPR, come da apposito allegato che costituisce parte integrante e sostanziale.

Rientrano tra questi trattamenti le attività di lettura, scrittura, modifica, verifica e controllo di tutti i dati gestiti nei sistemi oggetto di fornitura, svolte per le finalità di gestione e manutenzione del sistema informatico stesso.

Pur non essendo preposto ordinariamente ad operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), il Fornitore è responsabile di tutte le specifiche fasi lavorative oggetto del contratto che possono comportare elevate criticità rispetto alla protezione dei dati ed è tenuto ad adottare misure idonee volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali effettuati dai propri incaricati, in specie quelli realizzati con abuso della qualità di amministratore di sistema.

Tenuto conto del contesto operativo che potrebbe rendere tecnicamente possibile l'accesso, anche fortuito, a dati personali ed in particolare a dati sensibili, il Fornitore, in qualità di responsabile dei trattamenti, è tenuto a nominare, quali incaricati, soggetti in possesso di adeguate qualità tecniche, professionali e di condotta.

Il Fornitore ha altresì l'obbligo di mantenere riservati tutti i dati e tutte le informazioni, di cui venga in possesso o 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, anche successivamente alla cessazione di efficacia del rapporto contrattuale.

Il Fornitore è responsabile dell'esatta osservanza da parte dei propri incaricati degli obblighi di segretezza anzidetti. In caso di inosservanza degli obblighi di riservatezza, l'Azienda USL ha la facoltà di dichiarare risolto di diritto il contratto di fornitura, fatto salvo il diritto ad agire per via giudiziale per ottenere il risarcimento di eventuali maggiori danni e/o oneri subiti, fermo restando le eventuali responsabilità civili e penali a carico del Fornitore del servizio.

Il Fornitore è tenuto ad adottate tutte le misure di sicurezza informatiche ed organizzative richieste dall'Azienda USL, e riportate nel successivo articolo 10, atte a garantire la completa integrità e riservatezza dei dati personali trattati nell'ambito del contratto;

In particolare, le figure professionali addette alla manutenzione di sistemi o di componenti dei sistemi informatici sono assimilabili alla definizione di "Amministratore di sistema", come individuato dal

provvedimento del garante privacy 27 novembre 2008 e modificato con provvedimento del 25 giugno 2009, in quanto le attività tecniche comportano un'effettiva capacità di azione su informazioni (ovvero un trattamento di dati personali) anche quando l'addetto non consulti "in chiaro" le informazioni medesime.
Il Fornitore è tenuto a mantenere un elenco aggiornato di queste figure e di renderlo disponibile all'Azienda quando ne faccia richiesta.
Dovrà inoltre attivare un servizio di tracciatura atto a registrare e conservare i log di tutti gli accessi agli applicativi/sistemi/DB e dovrà conservare per la durata minima di un anno come pregresso durante il contratto e per almeno sei mesi oltre la durata del contratto stesso. I log dovranno essere resi disponibili all'Azienda USL per i dovuti controlli, su richiesta della stessa e senza oneri aggiuntivi.
Il Software oggetto del presente contratto deve consentire all'Azienda USL il rispetto dei diritti dell'interessato introdotti con il GDPR, pertanto il Fornitore, in assenza di strumenti automatizzati che consentano all'Azienda di agire in autonomia, dovrà garantire, senza oneri aggiuntivi, il pieno supporto all'Azienda USL per ottemperare senza ritardo, alle seguenti richieste degli utenti i cui dati sono registrati all'interno del software oggetto del presente affidamento:

1. Richiesta di portabilità dei dati: estrazione in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali del cittadino che ne fa richiesta;
2. Richiesta di rettifica e integrazione: modifica ed integrazione dei dati personali su richiesta dell'interessato
3. Diritto alla cancellazione all'oblio: cancellazione dei dati personali su richiesta dall'interessato.

Qualora nello svolgimento delle attività di gestione e manutenzione il Fornitore rilevi una violazione della riservatezza dei dati personali è tenuto a comunicarlo tempestivamente all'Azienda Usl Umbria1 per permetterne la notifica all'Autorità Garante nei termini di legge.
Per quanto non espressamente previsto all'interno del presente articolo si rimanda all'allegato documento di Nomina in qualità di Responsabile esterno del trattamento ai sensi dell'art 28 del GDPR.

Art 10. MISURE DI SICUREZZA INFORMATICA

Con la sottoscrizione delle seguenti condizioni di fornitura il Fornitore accetta tutte le prescrizioni contenute nel documento "*Disciplinare tecnico per l'integrazione di sistemi informatici con l'infrastruttura IT dell'Azienda Usl Umbria1*" che si allega, quale parte integrante e sostanziale al presente documento, in particolare dichiara la conformità e l'accettazione integrale dell'Allegato "*Requisiti di conformità in ambito security*". Lo scenario di riferimento per il sistema in oggetto è lo scenario 1 descritto nel disciplinare tecnico.
Con la sottoscrizione delle seguenti condizioni di fornitura il Fornitore si impegna inoltre al pieno rispetto delle prescrizioni stabilite dalle normative.

Art 11. BREVETTI INDUSTRIALI E DIRITTO D'AUTORE

Il Fornitore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui e pertanto, si obbliga a manlevare Azienda, per quanto di propria competenza, dalle pretese che terzi dovessero avanzare in relazione a vantati diritti di privativa.

Art 12. RESPONSABILE DEL SERVIZIO

Il Fornitore ha l'onere di nominare un Responsabile del contratto che assumerà l'incarico di referente responsabile nei confronti dell'Azienda per l'esecuzione del contratto.

Art 13. GARANZIA DEFINITIVA

Il Fornitore, a seguito dell'aggiudicazione e ove sia obbligatoria da normativa, dovrà costituire apposita garanzia definitiva, a sua scelta sotto forma di cauzione o fideiussione, ai sensi dell'art.103 del D.Lgs n.50/2016, per un importo pari al 10% dell'importo contrattuale di aggiudicazione. La fidejussione bancaria o la polizza assicurativa dovrà espressamente prevedere la clausola di pagamento a semplice richiesta, prevedendo espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, di cui all'art. 1944 c.c. La fidejussione dovrà altresì contenere la rinuncia da parte del fideiussore, ad eccepire la decorrenza del termine di cui all'art. 1957 del Codice Civile, nonché alla rinuncia all'eccezione di compensazione, ai sensi dell'art. 1247 del c.c. La cauzione dovrà avere validità di pari alla durata del contratto come definita all'Art 4 delle presenti condizioni di fornitura. Sarà restituita alla scadenza del contratto. Nei casi di riduzione dell'importo della garanzia, il concorrente avente diritto dovrà produrre la documentazione in originale o copia autenticata ai sensi degli art. 18 o 19 del DPR 445/2000 che comprova il diritto alla riduzione medesima.

Art 14. DOCUMENTAZIONE AMMINISTRATIVA

Il Fornitore dovrà trasmettere contestualmente all'offerta, la seguente documentazione:

- Documento di gara unico europeo – DGUE, approvato in allegato alla Circolare del Ministero delle Infrastrutture e dei Trasporti n. 3 del 18 luglio 2016 "*Linee guida per la compilazione del modello di formulario di Documento di gara unico europeo (DGUE) approvato dal Regolamento di esecuzione (UE) 2016/7 della Commissione del 5 gennaio 2016. (16A05530)*" - Gazzetta Ufficiale – Serie Generale n. 174 del 27-7-2016. Il modello è reso disponibile, in formato word compilabile, in allegato alla presente lettera invito;
- Condizioni di fornitura (presente documento) - sottoscritto per accettazione – comprensivo di:
    - Allegato A - Nomina quale Responsabile esterno al trattamento dati;
    - Allegato B - Patto di integrità

- Allegato C - Disciplinare tecnico per l'integrazione di sistemi con l'infrastruttura IT - sottoscritto per accettazione;
- Modulo di richiesta accesso remoto;

Ai sensi del DPR n. 642/1972, l'atto di stipula è soggetto all'imposta di bollo pari a € 16,00; ai fini dell'assolvimento il Fornitore è tenuto al pagamento mediante utilizzo del modello F23 da trasmettere tramite PEC: aslumbria1@postacert.umbria.it, riportando il n. di CIG della presente fornitura.

Art 15. RISOLUZIONE DEL CONTRATTO E CLAUSOLE RISOLUTIVE ESPRESSE

Oltre a quanto previsto dalle Condizioni Generali di Contratto, il Punto Ordinante potrà risolvere di diritto il contratto ai sensi dell'art. 1456 del codice civile, nei seguenti casi:

- abbandono, sospensione (anche parziale) o rifiuto di esecuzione delle prestazioni previste nel Contratto;
- cumulo di penali per un importo complessivo pari o superiore al 10% dell'ammontare netto contrattuale;
- concessione e/o esecuzione di subappalti, in tutto o in parte, delle attività oggetto del Contratto, senza la previa autorizzazione scritta dell'Azienda Usl;
- violazione degli obblighi di riservatezza dei dati personali;
- violazione degli obblighi e disposizioni relative alla sicurezza sul lavoro;
- inadempimento degli obblighi concernenti il pagamento degli oneri assicurativi, assistenziali e di qualsiasi specie in conformità alle leggi, ai regolamenti e alle norme vigenti;
- impossibilità di procedere nella esecuzione delle attività oggetto del Contratto, per fatti di mafia riguardanti amministratori e/o rappresentanti dell'Appaltatore o di altri soggetti, così come previsto dalla vigente legislazione antimafia;
- sentenza di condanna passata in giudicato per frode nei confronti di subappaltatori, fornitori, lavoratori dipendenti, Enti e/o Autorità quali INPS, INAIL, ecc. e per mancata osservanza dello Statuto dei lavoratori;
- reiterato inadempimento nei pagamenti dovuti a fornitori e/o subappaltatori;
- mancanze che abbiano causato almeno tre verbalizzazioni di penale nell'arco di un trimestre;
- mancato rispetto dei termini di intervento in condizioni di emergenza;
- frode da parte dell'appaltatore nello svolgimento delle prestazioni, accertata con qualsiasi mezzo dall'Azienda Usl.

In presenza di uno qualsiasi dei casi sopraindicati, l'Azienda sanitaria notifica al Fornitore del servizio gli addebiti e gli concede, mediante comunicazione a mezzo lettera raccomandata con ricevuta di ritorno, un termine, salvo casi di particolare urgenza, non inferiore a dieci giorni di tempo per presentare le proprie controdeduzioni ed argomentazioni.

Nel caso che le controdeduzioni ed argomentazioni del Fornitore del servizio siano valutate negativamente dall'Azienda sanitaria oppure che il termine assegnato sia scaduto senza risposta data a mezzo di lettera raccomandata con ricevuta di ritorno, l'Azienda sanitaria procede alla risoluzione del Contratto fatto salvo il diritto ad agire per via giudiziale per ottenere il risarcimento di eventuali maggiori danni e/o oneri subiti, fermo restando le eventuali responsabilità civili e penali a carico del Fornitore del servizio.

Art 16. FORO COMPETENTE

Il foro competente per le controversie che dovessero insorgere tra l'Azienda USL ed il Fornitore sarà in ogni caso quello di Perugia.

Art 17. TRATTAMENTO DATI PERSONALI DEL FORNITORE

Ai sensi della vigente normativa in materia di protezione dei dati personali, in ordine alla fornitura oggetto del presente capitolato, si informa che:

- le finalità cui sono destinati i dati raccolti sono inerenti strettamente allo svolgimento della procedura di gara, fino alla stipulazione del contratto;
- il conferimento dei dati si configura come onere del concorrente per partecipare alla gara;
- i soggetti o le categorie di soggetti i quali possono venire a conoscenza dei dati sono: il personale interno dell'Azienda USL addetto agli uffici che partecipano al procedimento;

I diritti spettanti all'interessato in relazione al trattamento dei dati sono quelli di cui previsti dagli artt 12 e seguenti del GDPR.
Il titolare del trattamento dei dati è l'Azienda Usl Umbria1, per quanto concerne i dati conferiti dall'impresa aggiudicataria ai fini dell'esecuzione del contratto.

LEGALE RAPPRESENTANTE
(Firmato digitalmente per accettazione)

ALLEGATO A "

ALLEGATO A "NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI "

Di seguito l'AZIENDA USL UMBRIA 1 viene indicata come "Azienda" ed il Fornitore viene indicato come "Fornitore/Responsabile".

DISPOSIZIONI A CARATTERE GENERALE

1. Con la sottoscrizione del presente documento il Fornitore accetta la nomina a Responsabile del trattamento (di seguito *Responsabile*) ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche *"Regolamento UE"*), per tutta la durata del contratto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE e delle istruzioni nel seguito fornite;

2. I trattamenti consistono in attività di lettura, verifica, copia, analisi dei dati personali degli utenti e dei dipendenti per le finalità di assistenza e manutenzione del sistema in oggetto, così come descritto nelle allegate condizioni di fornitura, al fine di garantire la sicurezza, l'integrità e la disponibilità dei dati trattati e supportare l'Azienda in tutte le attività previste nelle condizioni contrattuali mantenendo il sistema in perfetta efficienza;

3. Trattandosi di dati inseriti nel documentale aziendale possono essere trattati in ragione delle attività oggetto del contratto i seguenti tipi di dati: i) dati comuni (anagrafici, di contatto, ecc…); ii) dati sensibili (dati sanitari/clinici);

4. Le categorie di interessati sono pazienti, utenti e dipendenti dell'Azienda Usl.

5. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

   a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

   b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

   c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni

di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

   - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - ricevano la formazione necessaria in materia di protezione dei dati personali;
   - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE;

OBBLIGHI DI PROTEZIONE DEI DATI

6. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio e il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre:

- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la 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 testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

7. In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati.

SUB- RESPONSABILE

8. Il Responsabile del trattamento può avvalersi di subappaltatori o subcontraenti (di seguito "sub-Responsabili del trattamento") per delegargli attività specifiche del Contratto che comportano il trattamento di dati personali solo previa richiesta scritta di autorizzazione da parte del Titolare del trattamento. Nella richiesta di autorizzazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.

9. Nel caso si ricorra a subappaltatori o a subcontraenti, il Fornitore/ Responsabile è obbligato a nominare con specifico contratto o atto di nomina tali operatori quali sub-Responsabili del trattamento ai sensi dell'art 28 del Regolamento UE sulla base delle specifiche indicate al Titolare. In particolare, il sub-Responsabile del trattamento deve rispettare gli stessi obblighi a quelli forniti dal Titolare al Responsabile del trattamento con il presente documento.

   Spetta al Responsabile del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti.

   L'Azienda potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi che avverranno con le medesime modalità di cui ai successivi punti 19 e 20. Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Azienda diffiderà il Responsabile a far adottare al sub-Responsabile del trattamento tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, l'Azienda potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

10. Il Responsabile Iniziale del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno di reputazione) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori;

ESERCIZIO DEI DIRITTI DELL'INTERESSATO

11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti;

SUPPORTO IN CASO DI VIOLAZIONE DEI DATI PERSONALI, DATA BREACH E/O VERIFICHE DA PARTE DEL GARANTE

12. Il Responsabile dovrà collaborare con il Titolare per eseguire la valutazione d'impatto sulla protezione dei dati (art 35 del Regolamento) e la messa in atto delle misure idonee alla mitigazione del rischio;

13. Ai sensi dell'art 33 del regolamento, il Responsabile deve informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di qualsiasi violazione di dati personali (cd. *data breach*). La comunicazione dovrà essere accompagnata da ogni documentazione utile per permettere al Titolare di valutare la natura della violazione, la categoria dei dati e le probabili conseguenze e consentire l'adozione delle misure necessarie alla risoluzione delle cause che hanno provocato la violazione del dato.

    Il Responsabile è tenuto ad affiancare il Titolare in tutte le fasi gestione del data breach da quelle iniziali di indagine e verifica fino all'adozione delle misure volte alla mitigazione del rischio. Dovrà supportare il titolare anche nelle comunicazioni agli interessati ai sensi dell'art 34 del regolamento;

14. Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare nel caso in cui riceva richieste di informazioni e di documentazione o di ispezioni da parte dell'Autorità Garante per la protezione dei dati personali. Dovrà, inoltre, assistere il Titolare nel caso di richieste formulate dall'Autorità Garante al Titolare stesso;

DESIGNAZIONE RESPONSABILE DELLA PROTEZIONE DEI DATI

15. Il Responsabile esterno del trattamento deve comunicare al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare;

AMMINISTRATORI DI SISTEMA

16. Il Responsabile si impegna ad attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema".*

    In particolare, dovrà procedere alla designazione formale degli amministratori di sistema nella quale dovranno essere elencati in modo analitico gli ambiti di operatività consentiti in base al profilo autorizzato.

    Sarà inoltre tenuto ad effettuare una verifica del loro operato con cadenza almeno annuale in modo da controllare il rispetto di tutte le misure di organizzative, tecniche e di sicurezza riguardo al trattamento dei dati personali;

LOCALIZZAZIONE DEI DATI

17. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare;

VERIFICHE DA PARTE DEL TITOLARE

18. Sarà obbligo del Titolare del trattamento vigilare per tutta la durata del contratto, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento da parte del Responsabile, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento;

19. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso.

    Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Azienda diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato;

20. Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzioni del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati" e/o non si sia adeguato a seguito di diffida, l'Azienda potrà risolvere il contratto, salvo il risarcimento del maggior danno;

ADEGUAMENTI ALLA NORMATIVA

21. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di

Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

22. Durante l'esecuzione del Contratto, qualora la normativa lo richieda, il responsabile dovrà adottare un codice di condotta approvato o un meccanismo di certificazione così come specificato agli articoli 40 e 42 del Regolamento

LEGALE RAPPRESENTANTE

(Firmato digitalmente per accettazione)

ALLEGATO B "PATTO DI INTEGRITA' "

Questo patto d'integrità stabilisce la reciproca, formale obbligazione dell'Azienda USL Umbria 1 e l'operatore economico di conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza nonché l'espresso impegno anti-corruzione di non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio, sia direttamente che indirettamente tramite intermediari, al fine dell'assegnazione del contratto e/o al fine di distorcerne la relativa corretta esecuzione.

Il personale, i collaboratori ed i consulenti dell'Azienda USL Umbria 1 impiegati ad ogni livello nell'espletamento della gara e nel controllo dell'esecuzione del contratto in oggetto, sono consapevoli del presente Patto d'Integrità, il cui spirito condividono pienamente, nonché delle sanzioni previste a loro carico in caso di mancato rispetto del presente Patto.

Il sottoscritto Operatore economico si impegna a segnalare all'Azienda USL Umbria 1 qualsiasi tentativo di turbativa, irregolarità o distorsione nella fase di esecuzione del contratto, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative all'affidamento in oggetto.

Il sottoscritto operatore economico dichiara di non trovarsi in situazioni di controllo o di collegamento (formale e/o sostanziale) con altri concorrenti e che non si è accordato e non si accorderà con altri partecipanti alla gara.

Il sottoscritto Operatore economico si impegna a non conferire incarichi di collaborazione al personale dipendente di questa Azienda USL coinvolto nell'appalto, od ai loro familiari, ivi compresi gli affini entro il secondo grado, durante la fase di esecuzione del contratto e nei tre anni successivi alla conclusione del contratto stesso.

I dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto dell'Azienda USL non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della stessa Azienda USL svolta attraverso i medesimi poteri. I contratti conclusi e gli incarichi conferiti in violazione di quanto previsto dal presente comma sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni con obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti.

Il sottoscritto Operatore economico prende nota e accetta che nel caso di mancato rispetto degli impegni assunti con il presente Patto di Integrità comunque accertato dall'Amministrazione, potranno essere applicate le seguenti sanzioni:

- risoluzione o perdita del contratto;
- escussione della cauzione di validità dell'offerta;
- escussione della cauzione di buona esecuzione del contratto;
- responsabilità per danno arrecato all'Azienda USL Umbria 1 nella misura dell'8% del valore del contratto, impregiudicata la prova dell'esistenza di un danno maggiore;
- responsabilità per danno arrecato agli altri concorrenti della gara nella misura dell'1% del valore del contratto per ogni partecipante, sempre impregiudicata la prova predetta;
- esclusione del concorrente dalle gare d'appalto indette dall'Azienda USL Umbria 1 per 5 anni.

Il presente Patto di Integrità e le relative sanzioni applicabili resteranno in vigore sino alla completa esecuzione del contratto in oggetto.

Ogni controversia relativa all'interpretazione, ed esecuzione del presente patto d'integrità fra Azienda USL Umbria 1 ed i concorrenti e tra gli stessi concorrenti sarà risolta dall' Autorità Giudiziaria competente.

LEGALE RAPPRESENTANTE

(Firmato digitalmente per accettazione)

ALLEGATO C "DISCIPLINARE TECNICO PER L'INTEGRAZIONE DI SISTEMI CON L'INFRASTRUTTURA IT DELL'AZIENDA USL UMBRIA 1 "

Art. 1.C. SCOPO

La presente procedura definisce le specifiche e le regole che i sistemi installati da ditte/fornitori esterni dovranno rispettare relativamente agli aspetti inerenti l'infrastruttura IT (Information Technology).

Art 2.C. TERMINI E ABBREVIAZIONI

ACCOUNT: insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in determinati contesti operativi, come siti web, determinati servizi su Internet ma anche per accedere alle più disparate applicazioni software.

ACTIVE DIRECTORY: Insieme di servizi di rete, adottati dai sistemi operativi Microsoft e gestiti da un domain controller. Esso si fonda sui concetti di dominio e di directory (che in inglese sta a significare "elenco telefonico"), ovvero la modalità con cui vengono assegnate agli utenti tutte le risorse della rete attraverso i concetti di: account utente, account computer, cartelle condivise, stampanti ecc... secondo l'assegnazione da parte dell'amministratore di sistema.

AGID (Agenzia per l'Italia digitale): è una agenzia pubblica italiana che svolge le funzioni ed i compiti ad essa attribuiti dalla legge al fine di perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della pubblica amministrazione e al servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

BACKUP: replicazione su un qualunque supporto di memorizzazione di materiale informativo archiviato nella memoria di massa dei computer, siano essi personal computer, workstation o server, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. Si tratta dunque di una misura di ridondanza fisica dei dati.

CLIENT: componente che accede ai servizi o alle risorse di un'altra componente detta server.

DHCP: protocollo di rete di livello applicativo che permette ai dispositivi o terminali di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso a una rete la configurazione necessaria per stabilire una connessione.

DNS: sistema utilizzato per la risoluzione di nomi dei nodi della rete in indirizzi IP.

Indirizzo IP: etichetta numerica che identifica univocamente un dispositivo detto *host* collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete.

LAN: una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

NIS: Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi

RDBMS: Sistema per la gestione di database relazionali.

SERVER: componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate *clients*, cioè *clienti*) che ne fanno richiesta attraverso una rete di computer.

SINGLE SIGN ON: sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato.

SISTEMA: qualsiasi apparecchiatura informatica, elettromedicale o dispositivo che si dovrà interfacciare/Integrare con l'infrastruttura IT di USL Umbria 1

VLAN: insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale.

VPN: rete di telecomunicazioni privata aziendale sicura, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

WSUS: Windows Server Update Services (WSUS) fornisce un servizio di aggiornamenti per i sistemi operativi Microsoft Windows e altri software Microsoft. E' un sistema di gestione locale che lavora combinato con Windows Update per dare agli amministratori dei sistemi la possibilità di gestire la distribuzione delle hotfix e degli aggiornamenti distribuiti, attraverso gli aggiornamenti automatici nei computer degli ambienti aziendali.

Art. 3.C. MODALITA' ESECUTIVE / CONTENUTI

I sistemi oggetto di fornitura dovranno essere coerenti con le politiche del presente documento nonché essere rispondenti alle normative in essere, o emanate in vigenza del presente contratto, in materia di sicurezza e privacy con particolare riguardo:

- alla Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi);
- alle Misure Minime di Sicurezza ICT per la Pubblica Amministrazione diramate da AGID con circolare 18 aprile 2017;
- ai principi derivanti dal CAD-Codice dell'amministrazione digitale (con particolare riguardo all'art. 51 del D.lgs 82/05);
- al Regolamento europeo 2016/679 sulla protezione dei dati personali (GDPR) in virtù del quale il titolare del trattamento deve mettere in atto tutte le misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali.

Art. 3.1.C. ADEMPIMENTI DELL'AGGIUDICATARIO

L'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'Azienda USL Umbria 1 è chiamata a redigere in ottemperanza alla vigente normativa in materia di sicurezza ICT e di privacy.

La fornitura dovrà essere sempre oggetto di apposito collaudo corredato dalla documentazione attestante la rispondenza del sistema alle presenti prescrizioni.

In particolare, per quanto riguarda dispositivi e sistemi medici/elettromedicali il collaudo sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un accordo di responsabilità (responsibility agreement) redatto secondo i dettami della norma IEC 80001.

Tale documento dovrà fare riferimento allo scenario individuato nel contratto e alle specifiche configurazioni ed installazioni del sistema presso l'Azienda USL Umbria 1. Dovrà inoltre riportare i riferimenti alla "marcatura CE" dei dispositivi offerti ed al fatto che i requisiti essenziali di sicurezza non saranno inficiati dalla specifica installazione.

Art. 3.2.C. INTEGRAZIONE CON L'INFRASTRUTTURA IT DI USL UMBRIA 1

I sistemi oggetto di fornitura dovranno essere interfacciati o integrati con l'infrastruttura IT dell'Azienda USL Umbria 1 rispettando le direttive riportate di seguito e basate sullo specifico scenario di utilizzo.

I dispositivi dotati di connettività di rete (host) e che necessitano di collegamento alla rete dati per svolgere le proprie funzioni, potranno essere collegati solo se riconducibili ad uno dei seguenti scenari, mutuamente esclusivi:

- **Scenario 1:** Sistemi e/o dispositivi da integrare con la rete LAN o con i sistemi già presenti nell'Azienda USL Umbria 1 (es: integrazione con Active Directory o con altri

software/sistemi già attivi) utilizzando in alcuni casi anche le risorse hardware preesistenti (es: hypervisor, infrastrutture cluster, ecc...).

- **Scenario 2:** Sistemi e/o dispositivi forniti dall'assegnatario che possono essere confinati ad una rete VLAN dedicata (isolamento totale dai sistemi dell'Azienda USL Umbria 1) e che prevedono l'utilizzo di hardware dedicato e non condiviso con quello preesistente.

L'aggiudicatario dovrà garantire la piena compatibilità dei sistemi forniti con l'infrastruttura descritta e in caso di incompatibilità completa dovrà proporre soluzioni analoga a quanto richiesto con il presente documento, in caso di incompatibilità parziale dovrà proporre un piano di adeguamento da attivare entro 3 mesi dal collaudo.

In entrambi i casi le soluzioni proposte dovranno essere presentate per iscritto ed essere validate dall'Azienda Sanitaria USL Umbria 1.

Art. 4.C. SCENARIO 1

In questo scenario i sistemi oggetto della fornitura sono strettamente integrati con l'infrastruttura IT dell'Azienda USL Umbria 1, sia dal punto di vista della rete che dei server, facendo affidamento in generale sulle infrastrutture di virtualizzazione e sui servizi di rete preesistenti.

Tale scenario è applicabile per esempio nel caso dell'implementazione di sistemi la cui fornitura non preveda l'installazione di hardware dedicato e può usufruire di sistemi di autenticazione basati su Active Directory.

Di seguito vengono riportate le caratteristiche peculiari dell'infrastruttura informatica dell'Azienda USL Umbria 1, definendo inoltre le specifiche di interfacciamento all'infrastruttura esistente alle quali i sistemi oggetto di fornitura dovranno adeguarsi.

SCENARIO 1 - Infrastruttura esistente

L'Azienda USL Umbria 1 dispone di un directory service aziendale basato su dominio Active Directory (AD).

Ogni account del directory service aziendale è associato ad almeno un gruppo di dominio (gruppi locali al dominio, domain local) corrispondente alla struttura amministrativa Azienda USL Umbria 1 di appartenenza.

Gli aggiornamenti di sistema per i client e per i server con sistema operativo Microsoft vengono distribuiti tramite il servizio WSUS.

Il protocollo di rete in uso nelle reti LAN dell'Azienda USL Umbria 1 è IPv4.

La risoluzione dei nomi è basata esclusivamente sul servizio DNS (Domain Name Service), integrato in AD, che accetta solo registrazioni sicure.

I backup dei sistemi, dei database, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi saranno effettuati dai tecnici dell'Azienda USL Umbria 1 secondo specifici accordi con il fornitore ed in relazione alla specificità dei sistemi forniti.

Le postazioni di lavoro client dispongono di sistema operativo client Microsoft Windows di varie versioni.

L'applicativo antivirus aziendale è Sophos versione Central Intercept X Advanced.

Il controllo del traffico è realizzato tramite l'implementazione di apposite regole sui firewall aziendali redatte sulla base delle sole necessità di navigazione. Qualora la soluzione proposta necessiti di specifiche configurazioni, il fornitore dovrà collaborare con i tecnici dell'Azienda in fase di configurazione e fino al raggiungimento di adeguati livelli di sicurezza.

SCENARIO 1 – Virtualizzazione server

Gli eventuali server virtuali oggetto della fornitura dovranno essere compatibili con il sistema di virtualizzazione Nutanix versione 6.5.2 LTS.

Tutte le configurazioni relative ai sistemi e ai software in esse presenti dovranno rispecchiarne le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, di backup e di disaster recovery.

In relazione alle necessità potranno essere messe a disposizione dell'aggiudicatario una o più VM (macchine virtuali) rispecchiando l'architettura proposta, assegnando sufficienti risorse hardware in base alle specifiche necessità.

Dal punto di vista dei sistemi operativi, l'assegnatario potrà proporre al servizio informatico dell'Azienda USL Umbria 1 un ventaglio di possibili scelte al fine di selezionare la più opportuna sia in termini di compatibilità con la piattaforma di virtualizzazione in uso, che in termini di omogeneità con i sistemi operativi già presenti nell'infrastruttura.

In tutti i casi le licenze dei sistemi operativi (es: Windows Server) necessarie al funzionamento del sistema non sono da intendersi a carico del fornitore e non dovranno essere in alcun caso di tipo OEM, bensì licenze Retail/VLK intestate all'Azienda USL Umbria1.

In linea generale laddove si debbano implementare VM con sistema operativo Windows Server, sarà opportuno legare tali VM al dominio uslumbria1.it e conseguentemente al sistema di aggiornamento WSUS dell'Azienda USL Umbria 1.

Tali macchine verranno inserite in una apposita Organizational Unit (OU) relativa ai server oppure in una OU dedicata al fine di definire ed applicare su di esse le Group Policy di sicurezza ed autorizzazione concordate con l'Azienda USL Umbria 1.

Verrà applicata in ogni caso su tutte le OU la default domain policy.

Per quanto concerne la connettività di rete, ai server verrà assegnato un range di indirizzi IP statici nella rete della LAN aziendale o, se necessario, una subnet di rete dedicata.

SCENARIO 1 - Sistemi database RDBMS

Nel presente scenario, i dati acquisiti e generati dal sistema e/o i loro riferimenti, nonché tutti quelli direttamente o indirettamente necessari al funzionamento degli applicativi forniti, dovranno essere organizzati in uno o più RDBMS, che potranno essere istanziati sugli attuali server Microsoft SQL e Oracle di cui già dispone l'Azienda USL Umbria 1 o in nuovi RDBMS basati su altre piattaforme a discrezione dell'aggiudicatario, sempre previa valutazione con il servizio informatico al fine di stabilire l'eventuale conformità con le attuali politiche di sicurezza e compatibilità/sostenibilità con l'attuale sistema di backup e disaster recovery.

In quest'ultimo caso l'aggiudicatario dovrà farsi carico di fornire le licenze d'uso per gli RDBMS forniti e della gestione delle politiche di backup se non integrabili con l'attuale sistema di backup e disaster recovery.

SCENARIO 1 - Applicativi client/server o web-based

Nel presente scenario, gli applicativi destinati all'utilizzo da parte degli utenti dovranno essere basati su tecnologia client/server o web-based.

Gli eventuali applicativi destinati all'installazione lato client dovranno essere adeguati alle caratteristiche software e hardware delle postazioni di lavoro e dovranno garantire piena compatibilità con le policy del dominio Active Directory e con i software già installati nelle postazioni di lavoro.

.

Nel caso in cui non fosse possibile effettuare il deployment centralizzato di tali applicativi, l'installazione verrà effettuata – con analoghe caratteristiche qualitative e di risultato – da parte dell'aggiudicatario.

Per quanto concerne gli applicativi web, sarà necessario analizzarne e verificarne la compatibilità con i browser web e relativi plugin approvati dal servizio informatico per l'utilizzo dalle varie postazioni di lavoro dell'Azienda USL Umbria 1.

Gli applicativi web dovranno obbligatoriamente avere connessione protette tramite certificato fornito dall'Azienda (porta 443).

SCENARIO 1 – Sistemi client

Eventuali PC o apparati oggetto di fornitura, qualora dispongano di sistema operativo Microsoft Windows, dovranno essere configurati come membri del dominio uslumbria1.it in modo da essere conformi con le policy di dominio applicate ai computer dell'Azienda USL Umbria 1.

Nel presente scenario, se non diversamente comunicato dall'aggiudicatario, i sistemi operativi Microsoft Windows verranno aggiornati tramite WSUS installando tutte le patch rilasciate da Microsoft che verranno approvate dagli amministratori.

Le configurazioni di rete dei PC/apparati oggetto della fornitura dovranno garantire la compatibilità con il sistema di indirizzamento IP dinamico (DHCP) attivo in generale sui client dell'Azienda USL Umbria 1. Nel caso in cui l'architettura e le caratteristiche tecniche dei sistemi forniti impedissero tale configurazione, l'aggiudicatario sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza e sulla base della quale l'Azienda USL Umbria 1 si riserva di create sul servizio DHCP opportune e specifiche configurazioni (reservation).

Sulle postazioni dovrà essere installato l'antivirus Aziendale in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'Azienda USL Umbria 1, a meno di eccezioni concordate con il servizio informatico.

Eventuali PC/apparati non Windows che non siano compatibili con l'Active Directory e che necessitano di connettività con la rete dati Azienda USL Umbria 1, verranno connessi alla stessa con specifici indirizzi IP statici assegnati dal servizio informatico dell'Azienda USL Umbria 1. La gestione del patching di tali sistemi è comunque obbligatoria ed è a carico dell'aggiudicatario.

SCENARIO 1 – VPN

In caso di necessità di interventi in teleassistenza da remoto da parte del personale tecnico dell'aggiudicatario durante il periodo di validità del contratto, l'accesso agli host oggetto di assistenza sarà garantito esclusivamente per mezzo dei sistemi VPN dell'Azienda USL Umbria 1.

Il personale tecnico potrà ottenere l'accesso al sistema VPN solo a fronte della compilazione del modulo specifico che dovrà essere inviato per validazione al servizio informatico dell'Azienda USL Umbria 1.

La connessione VPN dovrà essere di tipo client-to-site ed effettuata necessariamente utilizzando credenziali personali.

Nel caso in cui l'aggiudicatario non fosse in condizione di poter garantire tale configurazione per valide ragioni tecniche, sarà tenuto a redigere una relazione che giustifichi tale evenienza sulla base della quale l'Azienda USL Umbria 1 si riserverà di attivare connessioni di tipo site-to-site (es: tunnel IPSec). L'aggiudicatario dovrà garantire la tracciatura interna degli accessi effettuati da parte degli operatori che svolgono interventi in assistenza remota. L'Azienda USL Umbria 1 si riserva inoltre la facoltà di richiedere in qualsiasi momento il report di tali accessi.

Per rispondere ad eventuali esigenze di monitoraggio continuativo da remoto dello stato dei sistemi che sono oggetto della fornitura, lo strumento messo a disposizione dall'Azienda USL Umbria 1, a fronte di specifica configurazione, consentirà all'aggiudicatario di tenere costantemente sotto controllo lo stato dei servizi e dei dispositivi oggetto della fornitura.

SCENARIO 1 – Single Sign-On (SSO)

Tutti gli applicativi software forniti devono essere integrabili con l'LDAP messo a disposizione dal servizio Active Directory con livello di funzionalità minima 2012. Il collegamento dovrà passare tramite canale cifrato TLS/SSL debitamente autenticato tramite credenziali di sola lettura. L'integrazione del software oggetto della fornitura con il servizio LDAP di Active Directory andrà discussa di volta in volta con il servizio informatico al fine di fornire tutte le specifiche necessarie all'implementazione.

Altre soluzioni di SSO, autenticazione e account/identity management saranno consentite valutate dal Servizio informatico dell'Azienda USL Umbria 1.

Art. 5.C. SCENARIO 2

Questo scenario fa riferimento a tutti quei sistemi che, seppur installati all'interno dei locali dell'Azienda USL Umbria 1, non si interfacciano con la rete aziendale

SCENARIO 2 – CASISTICA A

I sistemi che non necessitano di connettività di rete (airgapped) dovranno essere comunque conformi alle disposizioni di legge in materia di sicurezza informatica e alla normative privacy vigenti.

La gestione del patching e della manutenzione di tali sistemi andrà esclusivamente gestita in locale, escludendo qualsivoglia sistema di gestione remota. Sarà pertanto onere del fornitore provvedere all'aggiornamento periodico dei sistemi tramite interventi on site in conformità alle misure minime indicate nell'Allegato n.1 – "Requisiti di conformità in ambito security"

SCENARIO 2 - CASISTICA B

I sistemi che non si devono integrare con la rete di USL Umbria 1 ma che necessitano di connettività di rete per svolgere le loro funzioni, verrà assegnata una specifica classe di indirizzi IP statici coerente con il piano di indirizzamenti dell'Azienda USL Umbria 1 e tali dispositivi verranno inseriti in una VLAN dedicata dalla quale potranno effettuare solo il traffico necessario per svolgere le funzioni richieste e il traffico relativo all'assistenza remota da parte del fornitore.

La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall.

Gli host forniti saranno soggetti a filtraggio della navigazione Internet. Potranno essere implementate specifiche eccezioni all'autenticazione basate su IP sorgente che consentiranno il traffico esclusivamente verso IP e porte specifiche. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'Azienda USL Umbria 1 per la definizione delle suddette eccezioni.

Nel presente scenario l'aggiudicatario è responsabile in toto delle prescrizioni in ambito di sicurezza informatica e privacy, secondo quanto previsto dal quadro legislativo e normativo vigente, nonché dal presente documento; in particolare per quanto riguarda le politiche di: autenticazione, autorizzazione e accounting (AAA), di backup e disaster recovery, sugli aggiornamenti di sicurezza di tutti i software installati sugli host oggetto di assistenza, di protezione antivirus e da altre tipologie di cyber attacco.

Si specifica infine che, eventuali PC client o qualsivoglia dispositivo necessario al corretto e sicuro funzionamento dei sistemi oggetto di fornitura, dovranno essere gestiti interamente dal fornitore cui competerà il rispetto dei requisiti di legge in materia di sicurezza ICT.

I server o dispositivi di storage forniti dovranno essere conformi con gli standard per l'installazione a rack 19"; dovranno inoltre essere dotati di requisiti di ridondanza sufficienti a garantirne almeno la continuità operativa (es: doppio alimentatore, doppio storage controller, ecc...) e laddove possibile anche l'alta affidabilità (HA). Non dovranno infine essere utilizzati per alcun motivo come postazioni di lavoro da parte degli operatori.

Per quanto concerne l'accesso remoto tramite VPN ai dispositivi oggetto della fornitura, a fronte della connessione VPN effettuata tramite i sistemi messi a disposizione dall'Azienda USL Umbria 1, il collegamento ai singoli host oggetto di assistenza potrà avvenire con strumenti scelti dall'aggiudicatario, nel rispetto delle modalità previste dal quadro legislativo e normativo vigente, previa validazione degli strumenti stessi e della loro specifica configurazione da parte del servizio informatico dell'Azienda USL Umbria 1.

Qualora compatibile con i sistemi del fornitore, l'Azienda USL Umbria 1 può mettere a disposizione del fornitore uno strumento per consentire il monitoraggio continuativo da remoto dello stato di tali sistemi.

Art. 6.C. REQUISITI DI CONFORMITÀ IN AMBITO SECURITY

In entrambi gli scenari appena descritti sarà compito dell'aggiudicatario adeguare le specifiche dei sistemi oggetto della fornitura (e le relative modalità di gestione da parte degli amministratori) ai principi generali di sicurezza delle infrastrutture IT, garantendo la piena conformità alle prescrizioni indicate in questo documento, con particolare riferimento a quelle relative all'ambito della IT Security.

L'aggiudicatario dovrà garantire che sia l'architettura che gli elementi forniti vengano progettati, implementati e manutenuti nel tempo in modo da risultare conformi disposizioni previste dalla Direttiva NIS (Direttiva 2016/1148) e dalle misure minime di sicurezza ICT per la Pubblica

Amministrazione, al fine di minimizzare il rischio informatico residuo sia di "attacchi ai sistemi" che di "attacchi dai sistemi".

Qui di seguito vengono esposte le indicazioni relative ai requisiti di conformità con le misure minime di sicurezza AGID applicabili al contesto delle forniture da parte di aziende esterne:

Inventario dei dispositivi: Nel caso in cui i dispositivi oggetto della fornitura vadano connessi alla rete (Scenario 1 o 2B) i dispositivi oggetto della fornitura andranno inventariati e tali dati di inventario andranno mantenuti aggiornati seguendo un processo formale di approvazione (vedi Allegato n.3). L'aggiudicatario dovrà compilare il modulo in allegato fornendo tutte le informazioni tecniche necessarie all'implementazione della fornitura in oggetto ed inviarlo al servizio informatico per l'approvazione e la valutazione di eventuali "non conformità". Sarà compito dell'aggiudicatario provvedere a comunicare tempestivamente eventuali modifiche o sostituzioni seguendo di volta in volta lo stesso iter di approvazione.

Laddove i dispositivi siano raggiungibili via rete, l'assegnatario sarà inoltre tenuto a comunicare al servizio informatico le modalità di scansione remota delle informazioni inerenti l'hardware e il software installati nel dispositivo (es: SNMP, WMI) e relative credenziali.

Elenco software autorizzati: il fornitore dovrà indicare preventivamente i sistemi operativi e i software che intenderà utilizzare nei propri dispositivi/sistemi sia come prima installazione che in caso di necessità di aggiornamenti a "major release" o in caso di sostituzione con altro software, seguendo anche in questo caso il processo formale di approvazione. I software non presenti nella lista di quelli autorizzati potranno essere installati solo a fronte di specifica richiesta e validazione da parte del servizio informatico.

Configurazioni sicure standard: le configurazioni dei dispositivi e dei software devono rispettare le configurazioni sicure standard, implementate nei clients tramite immagini di installazione preconfigurate e/o mediante group policies, le quali vengono applicate ai sistemi operativi Microsoft Windows sia server che client.

Nel caso di sistemi operativi non Microsoft o non agganciati al dominio, sarà cura del fornitore effettuare l'hardening ad-hoc dei propri sistemi tramite procedure che dovranno essere formalmente validate dal servizio informatico.

Connessioni protette per l'amministrazione remota: l'aggiudicatario dovrà configurare opportunamente i dispositivi o i software oggetto della fornitura affinché le operazioni di amministrazione da remoto possano avvenire per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri), utilizzando protocolli cifrati (es: https/SSH/RDP) che dovranno essere formalmente validati dal servizio informatico.

Verifica vulnerabilità: L'aggiudicatario deve verificare la presenza di eventuali vulnerabilità sia prima dell'installazione che dopo l'eventuale modifica/aggiornamento dei dispositivi e dei software oggetto della fornitura. I sistemi collegati alla rete dell'Azienda USL Umbria 1 sono sottoposti periodicamente a verifica di vulnerabilità tramite appositi strumenti, pertanto, l'Azienda USL Umbria 1 verificherà che le vulnerabilità emerse dalle scansioni vengano risolte per mezzo di patch, o implementando opportune contromisure.

Patching dei dispositivi e degli OS: La politica di gestione degli aggiornamenti/patching dei dispositivi e dei sistemi operativi è naturalmente legata alla piattaforma in uso dallo specifico dispositivo fornito. In linea generale, nel caso in cui si tratti di sistemi basati su piattaforma Microsoft Windows sarà opportuno fare in modo che essi possano ricevere gli aggiornamenti dal server WSUS centralizzato già presente nell'Azienda USL Umbria 1, concordando con il servizio informatico dell'Azienda USL Umbria 1 dei time-slot periodici per consentire l'applicazione degli aggiornamenti sui propri sistemi e verificarne l'esito. In tutti gli altri casi, ovvero per le applicazioni proprietarie, per i sistemi Windows non legati al dominio, per i sistemi operativi non Windows o per tutti gli altri dispositivi, l'aggiudicatario si dovrà far carico della verifica della disponibilità ed installazione manuale delle patch, concordando con il servizio informatico dell'Azienda USL Umbria 1 dei time-slot periodici per consentirne l'esecuzione e la successiva verifica di funzionamento.

In linea generale le patch andranno installate entro 90gg dal rilascio, salvo la necessità di installarle con la massima urgenza nei casi in cui le patch vadano ad indirizzare e correggere bug o vulnerabilità ad alto livello di criticità.

Patching dei sistemi separati dalla rete (es: airgapped): In caso della fornitura di sistemi separati dalla rete, in particolare di quelli "airgapped", l'aggiudicatario dovrà farsi carico di assicurare l'aggiornamento tempestivo degli stessi. Anche in questo caso, in linea generale le patch andranno installate entro 90gg dal rilascio, salvo la necessità di installarle con la massima urgenza nei casi in cui le patch vadano ad indirizzare e correggere bug o vulnerabilità ad alto livello di criticità.

Strumentazione hardware: non è autorizzato l'uso di strumentazione in cui siano presenti sistemi in end of life. Nel caso in cui, nel corso del contratto, si verifichi una tale condizione il fornitore dovrà attivare tutte le misure necessarie affinché tale criticità venga risolta: sia che questo comporti la configurazione di una nuova macchina sia che richieda l'adeguamento dell'applicativo in uso;

Manutenzione del software: le applicazioni fornite devono rispondere ai requisiti previsti dalla normativa vigente e utilizzare sempre le ultime realise.

Gestione account privilegiati: L'Azienda USL Umbria 1 utilizza un software per la gestione e il tracciamento delle autorizzazioni a livello applicativo, compreso l'inventario degli amministratori di sistema.

I privilegi amministrativi vengono concessi solo ad utenti dotati delle competenze necessarie e di un incarico/contratto relativo alla configurazione dei sistemi, solo per consentire lo svolgimento di attività che richiedano specifici livelli di privilegi.

Le utenze personali devono essere formalmente autorizzate seguendo una specifica procedura di validazione da parte del servizio informatico.

Gli accessi amministrativi vengono tracciati nei registri di auditing e conservati su piattaforma di Log Management, sia per quanto concerne i sistemi federati con Active Directory che per i sistemi standalone. Al fine di consentire la corretta acquisizione dei log dai sistemi/dispositivi oggetto della fornitura l'aggiudicatario sarà tenuto a fornire al servizio informatico le relative specifiche tecniche.

Gestione account locali: Prima di collegare alla rete un nuovo dispositivo o prima di mettere in produzione un software, l'aggiudicatario dovrà provvedere a sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso. L'Azienda USL Umbria 1 si riserva la facoltà di effettuare periodicamente delle verifiche a campione al fine di verificare che le credenziali predefinite non siano ancora in uso.

System hardening: Le password delle utenze amministrative devono rispondere a criteri di elevata robustezza: devono essere soggette a limiti minimi di lunghezza (es: 14 caratteri), rotazione (password history > 10) e durata (password aging <90gg). NB: tale prescrizione dovrà essere applicata a tutte le utenze con privilegi amministrativi, coinvolte nella fornitura, indipendentemente dal fatto che siano locali, legate all'Active Directory o definite in qualsiasi altra piattaforma software.

Gestione account privilegiati: L'aggiudicatario dovrà fare distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali distinte. Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso. L'aggiudicatario dovrà inoltre conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

Endpoint Protection: l'aggiudicatario dovrà provvedere ad installare l'antivirus centralizzato messo a disposizione dall'Azienda USL Umbria 1 (Sophos Endpoint Security) in tutti i dispositivi oggetto della fornitura, al fine di garantire adeguati livelli di protezione antivirus, firewall, IPS, controllo dei dispositivi USB, controllo web e controllo delle applicazioni. Le politiche di configurazione della suite antivirus sono gestite centralmente e rispondono ai requisiti delle misure minime AGID ai punti sopraindicati; pertanto, eventuali eccezioni antivirus potranno essere create solo a fronte della verifica da parte del servizio informatico della conformità alle stesse. Non sarà inoltre possibile attivare l'utilizzo di servizi di posta elettronica esterni a quelli dell'Azienda USL Umbria 1.

Data Protection: In base allo scenario di rischio al quale potrà essere ricondotta la fornitura, dovrà essere garantita l'esecuzione di un backup periodico contenente le informazioni strettamente necessarie per il completo ripristino del sistema. Le modalità di esecuzione e la relativa pianificazione andranno concordate con il servizio informatico dell'Azienda USL Umbria 1 sulla base dello scenario applicabile. La riservatezza delle informazioni contenute nelle copie di sicurezza dovrà essere assicurata mediante adeguata protezione fisica dei supporti. Sarà inoltre necessario assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

Crittografia dati rilevanti: L'aggiudicatario dovrà effettuare un'analisi dei dati manipolati dalla propria applicazione o dal sistema oggetto della fornitura al fine di individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e quelli ai quali va applicata la protezione crittografica, al fine di concordare con il servizio informatico di USL Umbria 1 le modalità più opportune per l'adempimento di tale direttiva

RIFERIMENTI

- Regolamento UE 2016/679 (GDPR) – Regolamento generale sulla protezione dei dati
- Decreto Legislativo 30 giugno 2003, n° 196: "Codice in materia di protezione dei dati personali" e ss.mm.ii
- CAD Decreto Legislativo 82/2005 e ss.mm.ii
- Circolare Agid 18 Aprile 2017 n° 2: “Misure minime di sicurezza ICT per la PA”
- Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi)
- Ulteriori norme in materia che dovessero essere emanate in corso di esecuzione del contratto

Art. 7 – Scenario 3 - Affidamenti servizi Cloud

In caso di affidamenti di servizio in Cloud il fornitore dovrà essere presente e/o dovrà avvalersi di un fornitore presente all’interno del market Place ACN (ex AGID).

Il livello minimo di sicurezza, capacità elaborativa, risparmio energetico e affidabilità deve rispondere alle disposizioni normative vigenti in materia e a quelle che dovessero essere emanate in corso di esecuzione del contratto. Tra le normative di riferimento si citano: GDPR, Direttiva NIS (Dlgs 65/2018), framework nazionale per la Cybersecurity e la data protection, linee guida o disposizioni ACN e AgID.

E’ a carico del fornitore la messa in atto delle misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche che possano

derivare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati nei sistemi oggetto di fornitura

In particolare il fornitore si impegna a :

- Censire le piattaforme e le applicazioni software in uso
- Garantire l'aggiornamento dei sistemi, dei database e degli applicativi
- Disporre di sistemi antivirus aggiornati e idonee misure di sicurezza
- Garantire una capacità elaborativa conforme agli standard del settore
- Individuare ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per le eventuali terze parti rilevanti (fornitori, clienti, partner)
- Effettuare peridiche attività di Risk Assestement relative agli asset e agli individui coinvolti
- Verificare che l'accesso agli asset logici e fisici, alle risorse dell'infrastruttura tecnologica e ai dati in generale è limitato al personale, ai processi e ai dispositivi autorizzati;
- Garantire che le modalità di autenticazione all'applicativo e/o ai sistemi sono commisurate al rischio della transizione;
- Garantire canali di comunicazione sicuri e criptati durante la trasmissione dei dati;
- Garantire la separazione tra gli ambienti di test e di sviluppo;
- Garantire che i backup delle informazioni siano eseguiti, amministrati e verificati con cadenza periodica.
  Il fornitore deve impegnarsi ad effettuare come minimo un backup giornaliero di tipo incrementale e uno settimanale di tipo completo;
- Garantire la manutenzione a caldo dei sistemi conformemente agli standard di mercato;
- Disporre di piani di risposta (Incident response e business Continuity) e recupero (Incident recovery e Disaster Recovery) in caso di incidente /disastro
- Effettuare periodiche attività di vulnerability assestement
- Disporre di un sistema di registrazione dei logs dei sistemi
- Disporre di un sistema di monitoraggio degli eventi che attraverso la correlazione dei dati consenta di rilevare tempestivamente incidenti o anomalie che possono avere di impatto sull'infrastruttura, sui sistemi e sui dati oggetto di fornitura
- Comunicare tempestivamente all'Azienda Sanitaria USL Umbria 1 eventuali anomalie o rischi rilevati

- Comunicare repentinamente e comunque non oltre le 24 ore il verificarsi di un data breach
- Collaborare con l'Azienda Sanitaria USL Umbria 1 in caso di Data Breach
- Garantire l'interoperabilità e la portabilità dei dati
- Garantire metriche di uptime pari al 99,00 %
- Consentire, se richiesta da parte dell'Azienda USL Umbria 1, verifiche di conformità da parte di proprio personale o di soggetti terzi (preventivamente individuati)

Il fornitore dovrà disporre di adeguata documentazione attestante le misure intraprese.

Dovrà inoltre produrre periodiche informazioni attestanti le attività di aggiornamento e monitoraggio dei sistemi, dei database e del software.

Al termine del contratto il fornitore deve impegnarsi restituire i dati oggetto del trattamento e a provvedere successivamente alla cancellazione definitiva dai propri sistemi

RIFERIMENTI

- Regolamento UE 2016/679 (GDPR) – Regolamento generale sulla protezione dei dati
- Decreto Legislativo 30 giugno 2003, n° 196: "Codice in materia di protezione dei dati personali" e ss.mm.ii
- CAD Decreto Legislativo 82/2005 e ss.mm.ii
- Circolare Agid 18 Aprile 2017 n° 2: "Misure minime di sicurezza ICT per la PA"
- Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi)
- Regolamento recante "livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione" adottato dall'AgID con Determinazione n. 628/2021 del 15 dicembre 2021
- "Aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa, e affidabilità delle infrastrutture digitali per la pubblica amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi cloud per la pubblica amministrazione, nonché requisiti di qualificazione dei servizi cloud per la pubblica

amministrazione": aggiornamento del regolamento adottata con determinazione ACN n. 307/2023 Determina ACN 307/2023

- Ulteriori norme in materia che dovessero essere emanate in corso di esecuzione del contratto