



CLAUSOLE PER LA SICUREZZA INFORMATICA

1 Campo di applicazione

Il presente contenuto si applica ogni qual volta deve essere definito il Capitolato d'Oneri relativo alla fornitura di un sistema/apparecchiatura/servizio che deve essere interfacciato con il Sistema Informativo Aziendale dell'ASST. Si applica ad ogni fornitore e relativo subfornitore.

2 Sicurezza e Privacy

In tema di sicurezza delle informazioni l'aggiudicatario deve adeguare la propria fornitura ed il proprio comportamento a quelle che sono tutte le vigenti normative e disposizioni in materia di privacy e protezione dei dati.

L'aggiudicatario deve assicurare il pieno rispetto di tutte le normative in vigore sul trattamento dei dati personali ed in particolar modo di quelli sensibili, dimostrando che sono resi operativi tutti gli strumenti atti a tale scopo e dichiarando la propria disponibilità a provvedere ai futuri adeguamenti che la normativa, il Garante per la Protezione dei Dati Personali e/o l'ASST richiederanno. Occorre che la fornitura sia allineata alle policy aziendali in termini di sicurezza riguardanti a titolo non esaustivo la gestione dei sistemi, gestione delle modalità di accesso alla rete aziendale, le procedure di installazione, manutenzione ed aggiornamento degli antivirus, il controllo degli accessi. L'ASST utilizza a tale scopo un Dominio Microsoft Active Directory sul quale devono necessariamente essere censiti tutti gli utenti della rete; non sono ammesse utenze non nominative e dovrà essere fornita la lista degli utenti che accedono ai sistemi.

Il sistema deve garantire la tracciatura completa di tutti gli eventi atti a ricostruire le operazioni intercorse quali, a titolo di esempio non esaustivo, accessi, operazioni, errori, ecc....

Eventuali VPN dovranno essere adeguatamente controllate e monitorate al fine di consentire un utilizzo conforme alle disposizioni aziendali. Nel caso di collegamento tramite rete virtuale, la postazione potrà esclusivamente accedere alla subnet predisposta: eventuali connessioni ad altre postazioni della rete aziendale o ad Internet, dovranno essere esplicitamente richieste motivate essendo la VLAN predisposta protetta da firewall: le connessioni verso altre postazioni della rete dell'ASST, non potranno in alcun modo prevedere l'utilizzo di software di controllo remoto del tipo RDP.

L'aggiudicatario si impegna a fornire un accesso amministrativo al sistema, riservato ai Sistemi Informativi Aziendali e di loro uso esclusivo, accesso che per nessuna ragione potrà essere disabilitato se non su disposizione scritta del Dirigente dei SIA.

I cablaggi di rete ed i dispositivi che abilitano collegamenti verso l'esterno utilizzati per assistenza remota, monitoraggio o aggiornamenti automatici dei sistemi dovranno essere esclusivamente quelli forniti dal SIA dell'Azienda Ospedaliera. Non sono ammesse installazioni di cablaggi e dispositivi di rete o comunicazione di terze parti e/o non approvati esplicitamente dal SIA ed in nessun caso potranno essere interconnessi alla rete aziendale. Anche le modalità di accesso alle LAN, sia via cavo che wireless/WiFi, sono esclusivamente quelle previste dall'ASST e non ne potranno essere accettate di differenti se non dopo valutazione ed accettazione esplicita dei Sistemi Informativi Aziendali. L'installazione di PdL (Postazioni di Lavoro) fornite dall'azienda appaltatrice dovrà essere preventivamente concordata con il SIA: le modalità di collegamento saranno concordate in base alla dotazione tecnologica di cui dispone il presidio ospedaliero interessato ed in base agli scopi funzionali dell'apparecchiatura. Nello specifico: 1. Le caratteristiche delle postazioni in termini di dotazioni Hardware e Software dovranno essere concordate con il SIA e sottoposte alla sua preventiva approvazione, in assenza della quale il collegamento in rete non sarà consentito. 2. In caso di collegamento diretto alla rete aziendale le postazioni saranno gestite dal dominio aziendale (Active Directory Microsoft),



compresi quindi gli accessi, protezione antivirus e aggiornamenti del sistema operativo. In nessun caso sarà possibile pilotare o accedere da remoto a tali postazioni. 3.

In generale per qualsiasi apparato informatico e/o periferica associata che verrà installato presso l'ASST, le sue caratteristiche e le modalità di collegamento ed operativo dovranno essere concordate con il SIA e sottoposte alla sua preventiva approvazione, in assenza della quale il collegamento in rete non sarà consentito: eventuali apparati installati senza autorizzazione potranno essere sconnessi, disattivati e presi in custodia dal personale SIA al fine di tutelare il corretto funzionamento dei sistemi ospedalieri.

Infine non è ammesso l'utilizzo di Basi di Dati il cui accesso non preveda il rispetto di protocolli di sicurezza con la verifica ed il log degli accessi tramite utente e password e rispettino le indicazioni e le norme in materia di Privacy in vigore.

3 Reportistica ed estrazione dati

Al fine di garantire la piena disponibilità dei dati prodotti, il sistema dovrà garantire le seguenti funzioni:

1. Piano per la piena disponibilità ed estrazione (anche in background/automatico) di tutti i dati memorizzati sotto forma di DB relazionale pienamente documentato o di tabelle estese.
2. Reportistica completa e modificabile in almeno due formati (PDF excel/doc) con pieno accesso a tutti i dati ed operazioni di aggregazione.
3. Modulo di estrazione capace di funzionare in background/automatico con tracciatura degli esiti
4. Interfaccia di accesso al DB dall'esterno
5. Interfaccia per la definizione di query di estrazione.

4 Affidabilità delle applicazioni e backup dei dati

Tutte le applicazioni oggetto di forniture dovranno essere progettate e realizzate per garantirne la massima disponibilità ed affidabilità. Dovranno essere previste le procedure per l'implementazione di un sistema di Disaster Recovery ed essere disponibili tutte le funzioni atte a garantire la Business Continuity. Per ognuna delle applicazioni software rese disponibili dovranno essere rese disponibili procedure di Backup complete ed esaustive dei dati e le modalità di re-installazione comprensive dei pacchetti di installazione completi.

5 Integrazioni

Il sistema/apparecchiatura oggetto della fornitura dovrà essere pienamente integrato all'interno dei sistemi informativi in uso presso l'ASST secondo le specifiche fornite dal SIA: i costi di integrazione sono a completo e totale carico dell'aggiudicatario. Eventuali costi aggiuntivi dovuti ad adeguamenti tecnologici dell'infrastruttura aziendale necessari per il collegamento dei sistemi oggetto di fornitura sono a totale carico dell'aggiudicatario.

6 Forniture hardware e software

I costi derivanti da forniture hardware e software (ivi comprese licenze di database) sono a carico dell'aggiudicatario.

Si richiede che la componente software supporti gli ambienti virtuali VmWare e che supporti anche le tecnologie cloud in linea dunque con la strategia per il cloud per le pubbliche amministrazioni definita dal Dipartimento per la Trasformazione digitale, in collaborazione con l'Agenzia per la Cybersicurezza Nazionale. La strategia applica il principio cloud first, favorendo l'adozione prioritaria da parte delle Pubbliche



Amministrazione di strumenti e tecnologie di tipocloud nello sviluppo di nuovi servizi e nell'acquisizione di software.

Si richiede l'impegno a conseguire la certificazione del livello 2 per l'erogazione dei servizi in cloud per la Pubblica Amministrazione secondo quanto disposto nel Decreto direttoriale prot. N. 29 del 02/01/2023 dell'ACN (Agenzia Nazionale per la Cybersicurezza). L'ottenimento di tale certificazione dovrà avvenire entro un massimo di 6 mesi dall'emanazione delle modalità e linee guida da parte dell'ACN.

Inoltre la fruizione degli applicativi in cloud dovrà avvenire esclusivamente tramite canale cifrato.

Si richiede che gli accessi ai sistemi software vengano gestiti con utenza nominale ed integrazione al sistema di autenticazione LDAP aziendale, nonché supportino meccanismi di autenticazione a doppio fattore. Non sono accettate soluzioni che prevedano l'utilizzo di utenze generiche anche solo per il funzionamento interno di servizi applicativi. Non sono accettate soluzioni che prevedano la cablatura nel codice del solo indirizzo IP, ma si richiede che esse gestiscano il nome del server.

Gli oneri di tutto quanto sopra sono a carico dell'aggiudicatario.

7 Governance

Il fornitore deve essere conforme ai requisiti di IT Governance dell'Ente, ed in particolare dovrà fornire informazioni su:

- schema aggiornato dell'infrastruttura/architettura IT
- descrizione dei dati da sottoporre a backup, utili ad un completo ripristino del sistema in caso di Disaster
- schema dell'organizzazione IT (compresi i canali di comunicazione verso di essa), che ha in carico i servizi/soluzioni IT;
- modifiche riguardanti l'architettura e le procedure di sicurezza, nonché la valutazione del rischio a esse corrispondente.

8 Gestione del rischio

Il fornitore deve adottare e seguire appropriate procedure di analisi del rischio sui servizi/soluzioni IT erogati. L'analisi del rischio dovrà essere condotta almeno annualmente ed i risultati dovranno essere condivisi con l'Ente.

9 Segregazione delle funzioni

I compiti e le aree di responsabilità devono essere segregate per ridurre le possibilità di modifiche non autorizzate, non intenzionali o l'uso improprio delle risorse dell'Ente.

10 Modifiche al servizio

Tutte le modifiche riguardanti applicazioni, architettura, procedure operative, procedure di sicurezza e la relativa valutazione del rischio, devono essere notificate con sufficiente anticipo all'Ente per permetterne la tempestiva approvazione o il rifiuto delle stesse.

11 Compatibilità con il sistema informativo socio sanitario regionale (SISS)

Tutte le applicazioni che prevedono la produzione di documenti di tipo sanitario devono prevedere l'integrazione e la piena compatibilità con il sistema SISS esistente in Lombardia.

Tale integrazione deve prevedere, previa validazione con l'Ente, almeno le seguenti funzioni minimali:

Sede: Via Papa Giovanni Paolo II – C.P. 3 - 20025 Legnano - Tel. 0331 449111 - Fax 0331 595275 -Codice Fiscale e Partita IVA 09319650967



- La gestione della Firma Digitale;
- L'utilizzo dell'anagrafica regionale NAR tramite BAC aziendale verso la quale deve essere disponibile piena e completa integrazione;
- L'invio dei documenti prodotti al Repository Aziendale previsto dalla Piattaforma Regionale;
- L'utilizzo dei nomenclatori SISS;
- L'integrazione applicativa tramite middleware in uso presso l'Ente;
- L'eventuale notifica dei referti ai Domini Centrali del SISS;

L'integrazione deve avvenire su base delle specifiche previste dalla Piattaforma Regionale di Integrazione in uso presso l'Ente e dalle Linee Guida attive in Regione Lombardia recuperabili dal sito di progetto SISS <http://www.siss.regione.lombardia.it/>

Con le stesse modalità devono essere sviluppate tutte le applicazioni che prevedono la Firma Digitale dei documenti prodotti: le modalità di firma, le regole di apposizione e di conservazioni devono essere le medesime previste al caso precedente anche quando non sia prevista la notifica al SISS del Documento Clinico Elettronico (DCE).

Le integrazioni software con i sistemi informativi dell'ente dovranno essere secondo gli standard HL7 FHIR.

12 Disponibilità dei sistemi

Deve essere prevista l'indicazione esplicita dei seguenti parametri relativi all'affidabilità e disponibilità dei sistemi:

- tempo medio fra i guasti (mean time between failures: MTBF);
- numero di cicli medio fra due guasti (mean cycles between failures: MCBF);
- tempo medio per il ripristino del funzionamento (mean time to restore/repair: MTTR).

Per ogni valore specificato devono essere indicati i parametri ed i contesti di riferimento al fine di garantire la loro corretta valutazione.

13 Gestione degli incidenti

Una procedura di escalation - che deve includere i Responsabili dell'Ente - per gestire l'operatività del servizio e il monitoraggio e la risoluzione degli incidenti di sicurezza - deve essere definita dal fornitore e approvata dall'Ente prima dell'attivazione dei servizi/soluzioni IT. La procedura prevede una modalità di comunicazione per informare il prima possibile l'Ente su eventuali problemi di sicurezza, azioni per gestirli, i rischi e criticità conseguenti.

Il fornitore è tenuto ad assicurare supporto e collaborazione relativamente ai seguenti ambiti:

- incidenti rilevati dall'Ente e riguardanti le proprie forniture all'Ente stesso;
- segnalazione all'Ente di incidenti aventi un impatto, anche potenziale, su sistemi e servizi a supporto dei processi dell'Ente, e relativa gestione, con particolare riferimento agli incidenti critici per l'Ente;
- produzione di reportistica a supporto del processo di gestione incidenti dell'Ente;
- invio alle Autorità di Controllo delle comunicazioni relative ad eventuali violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware...) verificatesi sui dati dell'Ente.

14 Security Assessment

Il fornitore deve garantire che in fase di progettazione di nuovi sistemi informativi o miglioramenti



ai sistemi informativi o dei servizi esistenti, un security assessment sia eseguito e che i controlli di sicurezza da esso scaturiti siano inclusi nei requisiti del sistema/servizio.

L'ente potrà chiedere la redazione di una DPIA propedeuticamente al rilascio in esercizio della soluzione; tale DPIA dovrà esitare con un livello di rischio accettabile per l'ente.

15 Sicurezza della rete

Il fornitore deve redigere e sottoporre, all'approvazione dell'Ente, un documento di architettura di rete che includa un diagramma completo della rete dell'Ente, illustrando i collegamenti tra ambiente dell'Ente ed eventuali altre reti coinvolte, con un diagramma di flusso dei dati completo che dettagli dove sono localizzati i dati dell'Ente, le applicazioni che utilizzano tali dati, e la loro sicurezza. Ogni variazione o aggiornamento del documento di architettura, in particolare ogni cambiamento nel modello di scambio dei dati tra il fornitore e l'Ente e ogni cambiamento significativo delle configurazioni di sicurezza devono essere comunicati e approvati da parte dell'Ente.

16 Dispositivi collegati alle reti dell'Ente

I soggetti terzi che collegano un dispositivo alla rete dell'Ente devono essere autorizzati dall'Ente. Il fornitore dovrà fornire una protezione dall'utilizzo, modifica, divulgazione o distruzione, accidentale o intenzionale, di beni dell'Ente da parte di esterni non autorizzati. Il soggetto terzo è responsabile della messa in sicurezza del dispositivo con antivirus e patch per proteggere informazioni dell'Ente. Qualsiasi dispositivo di proprietà di una terza parte che memorizza le informazioni dell'Ente, deve essere crittografato.

17 Accesso alle risorse dell'Ente e cancellazione dei dati dell'Ente

Il fornitore deve comunicare tempestivamente all'Ente quando un suo dipendente autorizzato all'accesso lascia l'azienda temporaneamente o definitivamente, o non necessita più dell'accesso, o siano cambiati ruolo e/o esigenze di privilegi per l'accesso ai beni e/o dati dell'Ente.

Quando l'accordo è risolto per qualsiasi ragione o è scaduto, tutti gli accessi vengono immediatamente revocati. Tutte le informazioni e i dati in possesso dell'Ente devono essere restituiti all'Ente e poi - salvi eventuali obblighi di legge - essere rimossi e cancellati in modo sicuro (wiping) dai dispositivi del fornitore.

Il fornitore deve rivedere almeno annualmente gli accessi del proprio personale ai beni dell'Ente, e prontamente rimediare a eventuali discrepanze. Su richiesta dell'Ente, il fornitore deve fornire i risultati dell'ultima revisione accessi e delle azioni poste in essere.

18 Collaudi e Passaggio in produzione

Eventuali modifiche che impattano l'architettura e il servizio erogato devono essere portate a conoscenza dell'Ente, informandolo circa la configurazione corrente, le modifiche proposte, le modalità e i risultati del test.

Il processo di autorizzazione alla messa in produzione è soggetto a collaudi, che dovranno essere eseguiti prima di ogni cambiamento in produzione. In particolare, sono da attuarsi i collaudi per le seguenti tipologia di fornitura:

- alla verifica e messa in funzione del sistema;
- al collaudo di tutte le apparecchiature oggetto della fornitura;



ASST Ovest Milanese

- alla piena e completa verifica funzionale in condizioni di esercizio simulando diversi cicli di funzionamento anche in condizioni di stress.
- Il collaudo verificherà:
- la corrispondenza tra le caratteristiche funzionali e tecniche dichiarate e quelle riscontrate;
- l'avvenuta esecuzione delle eventuali sessioni di formazione per le diverse tipologie di utenti dell'Ente;
- l'interconnessione di tutte le componenti del sistema con la LAN aziendale e la piena raggiungibilità da essa;

La correttezza di funzionamento di tutti i sottosistemi e del sistema nel suo complesso. Tale collaudo avverrà sulla base di un piano di lavoro redatto dai referenti del Sistema Informativo e condiviso con il Capoprogetto del fornitore e dovrà essere adeguatamente documentato in ogni sua fase.

19 Manualistica

Il fornitore si impegna a consegnare copia cartacea e/o elettronica di tutta la documentazione utente ed amministrativa del sistema oggetto di fornitura prima della messa in esercizio del sistema stesso, correttamente personalizzata per la propria installazione, comprensiva del dettaglio della configurazione adottata.

Il Fornitore deve garantire che durante lo svolgimento di tutte le attività collegate al servizio/soluzione IT erogato, la documentazione aziendale venga adeguatamente mantenuta ed aggiornata, in conformità con le best practice e la normativa vigente, e che la documentazione aziendale sia protetta contro accesso, uso, perdita, alterazione o distruzione impropria.

20 Accesso fisico ai locali aziendali

Il fornitore è tenuto a consegnare all'Ente una lista aggiornata con i nomi e i ruoli del suo personale o del personale dei subfornitori che possono avere accesso a siti dell'Ente. Il personale del fornitore oppure il personale dei subfornitori inclusi in tale elenco devono indossare un badge di riconoscimento in modo visibile e in ogni momento durante la visita presso i siti dell'Ente. Se il personale del fornitore o il personale dei subfornitori, ha bisogno di accedere alle aree riservate (come le sale server, data center, gli armadi di rete, etc.), esso deve essere accompagnato in ogni momento dal personale dell'Ente.

21 Smaltimento sicuro dei dati

Il fornitore deve essere conforme e deve garantire che anche i suoi subfornitori rispettino la normativa vigente relativa allo smaltimento sicuro dei dati dai supporti aziendali e dispositivi elettromedicali che li contengono. In particolare, come richiesto dai punti 21 e 22 dell'Allegato "B" del D.lgs. 196/03 Disciplina Tecnica in Materia di Misure Minime di Sicurezza, qualora l'erogazione dei servizi/soluzioni IT da parte del fornitore comporti il trattamento di dati personali sensibili o giudiziari, il fornitore deve definire delle istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati dell'Ente al fine di evitare accessi non autorizzati e trattamenti non consentiti. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Il fornitore deve pertanto dotarsi di procedure e strumenti adeguati ad implementare lo smaltimento sicuro di ogni potenziale dato residuo presente sull'apparecchiatura/dispositivo da dismettere o da riassegnare ad altro utilizzatore, e deve produrre una certificazione di cancellazione relativa ad ogni supporto cancellato.



Il fornitore dovrà inoltre smaltire eventuale materiale cartaceo come sancito dall'articolo 169 del Codice dei beni culturali e del paesaggio e come descritto nel paragrafo *Modalità e criteri di scarto* della documentazione del *Manuale della Documentazione Sanitaria e Sociosanitaria di Regione Lombardia*.

22 Obbligo di riservatezza

Per tutta la durata del presente accordo e successivamente alla cessazione del medesimo per qualsiasi causa intervenuta, il fornitore si obbliga a:

- mantenere riservati i fatti, documenti, progetti, dati e informazioni (intesi nella più ampia accezione dei termini) di cui verrà a conoscenza e/o disporrà in relazione al e/o in esecuzione del presente accordo (di seguito: Informazioni);
- non utilizzare le Informazioni per scopi diversi, in tutto o in parte, da quelli contemplati dal presente accordo;
- non divulgare o altrimenti rendere note a terzi le Informazioni, in mancanza di specifica autorizzazione o accordo.

Il fornitore riconosce che nel corso dell'esecuzione del contratto verrà a conoscenza di informazioni e fatti di natura strettamente riservata e confidenziale relativi all'organizzazione interna dell'Ente, al personale, ai programmi operativi, alla situazione patrimoniale, all'organizzazione finanziaria, ai progetti economici, alle tecnologie ed ai procedimenti amministrativi, ai nominativi di clienti e fornitori ed alle condizioni ad essi e con essi praticate. In relazione a ciò il fornitore si obbliga a considerare strettamente confidenziali e riservate tutte le informazioni riguardanti i dati dell'Ente, ivi comprese tutte le documentazioni di cui ha preso visione, le analisi dei computer e delle apparecchiature, i rapporti, le note, i memorandum, gli studi, e si obbliga pertanto a mantenere la totale riservatezza rispetto a tutte le informazioni suddette, a non rivelarle o divulgarle a persona alcuna in qualsiasi modo.

Il fornitore inoltre non utilizzerà tali informazioni riservate per alcun uso che non sia inerente all'attività svolta in dipendenza del contratto di fornitura, né a scopo concorrenziale o per qualsiasi fine che si possa rivelare a detrimento dell'Ente.

Alla cessazione del contratto o dell'erogazione del servizio - qualunque sia la causa che l'abbia determinata - il fornitore, su richiesta dell'Ente, sarà tenuto a fornire a quest'ultimo tutti i dati di titolarità dell'Ente ancora in suo possesso. Tali dati comprendono tutte le informazioni fornite dall'Ente al fornitore e tutte le relative elaborazioni operate in esecuzione del presente contratto. I dati dovranno essere forniti all'Ente secondo modalità tali da preservarne l'usabilità - anche sotto il profilo della semplicità nell'accesso alle informazioni e alle relative elaborazioni - ed attraverso l'impiego di formati aperti o, se proprietari, di uso comune, tali da consentirne la fruibilità, indipendentemente dall'uso delle soluzioni o dei servizi informatici resi del fornitore.

23 Misure minime di sicurezza

Il fornitore, Presa visione della tabella, dichiara di adottare le misure qui sopra riportate e si rende disponibile a fornire eventuale evidenza degli adempimenti richiesti in ragione del contratto in essere con l'Azienda Titolare del Trattamento.

MISURE DI GESTIONE CONTROLLO DELLE POLITICHE PRIVACY
<i>L'azienda ha stabilito un piano di disaster recovery e business continuity</i>
<i>L'azienda ha effettuato recentemente un'indagine sui rischi privacy</i>
<i>L'azienda dispone di un elenco degli Amministratori di Sistema e relativa mansione</i>
<i>L'azienda ha stabilito politiche che assicurano il controllo e riesame periodico delle misure stabilite a protezione dei dati personali</i>

**ASST Ovest Milanese**

<i>L'azienda ha stabilito delle misure per assicurare l'esercizio dei diritti degli interessati e pronta gestione dei reclami</i>
<i>L'azienda ha stabilito delle misure di controllo per assicurare il principio di minimizzazione dei trattamenti</i>
<i>L'azienda testa periodicamente l'efficacia del piano di disaster recovery e business continuity</i>
<i>L'azienda ha adottato un sistema di controllo che consente il trattamento SOLO sino al raggiungimento dei termini massimi di conservazione stabiliti</i>
RISCHIO RISERVATEZZA
<i>Sono stabilite misure volte a limitare l'accesso a personale non autorizzato agli spazi fisici</i>
<i>Sono stabilite misure volte a limitare l'accesso a personale non autorizzato alle banche dati digitali</i>
<i>L'azienda ha adottato sistemi di controllo automatici volti a limitare l'accesso ai locali in cui si effettua il trattamento</i>
<i>Esistono sistemi antivirus e firewall volti a bloccare tentativi di accesso non autorizzato dal web</i>
<i>Le banche dati in possesso dell'azienda sono cifrate</i>
<i>Il personale autorizzato è formalmente identificato e vi è evidenza delle istruzioni fornite</i>
<i>Sono stabilite misure per tracciare le operazioni effettuate da personale autorizzato</i>
<i>Le politiche di accesso stabilite sono verificate periodicamente</i>
RISCHIO PERDITA E CANCELLAZIONE
<i>Dove previsto l'affidamento di copia delle informazioni, esistono misure per testare l'efficacia delle procedure di backup stabilite</i>
<i>Dove previsto l'affidamento di copia delle informazioni, esistono misure per il ripristino di una copia dei dati affidati</i>
<i>Dove previsto l'affidamento di copia delle informazioni, esistono misure per assicurare la rintracciabilità delle informazioni</i>
RISCHIO DI NON COMPLETA O CORRETTA COMPILAZIONE DEI DATI
<i>Dove previsto dall'incarico, il personale adotta misure di controllo per assicurare la completa e corretta registrazione dei dati</i>
<i>Dove previsto dall'incarico, esistono delle forme di controllo indipendenti o effettuate da terze parti a garanzia della completezza e correttezza dei dati registrati</i>

24 Patching e aggiornamenti

Il fornitore si impegna a mantenere patchati ed aggiornati tutti i sw che compongono la soluzione fornita e a ritornare a sistemiinformativi@asst-ovestmi.it un report mensile di verifiche effettuate ed eventuali interventi.

Ogni onere riferibile ad aggiornamenti/rinnovi ed adeguamenti software sono a carico del fornitore.

Sui sistemi server e client della soluzione fornita i sistemi informativi provvederanno ad installare un sistema EDR (Endpoint Detection and Response) per la rilevazione delle minacce.



25 Assistenza

Il fornitore è tenuto ad eseguire la manutenzione preventiva e correttiva/adequativa dei sistemi hardware e software come di seguito specificato rispettando le tempistiche di intervento come descritto al paragrafo LIVELLI DI SERVIZIO.

26 Manutenzione Preventiva

Per *Manutenzione Preventiva* si intendono tutte quelle procedure periodiche di verifica, controllo, messa a punto, sostituzione parti di ricambio e parti soggette ad usura finalizzata a:

- prevenire l'insorgenza di guasti connessi all'utilizzo delle apparecchiature ed all'usura delle parti componenti;
- mantenere le tecnologie in condizioni di corretto funzionamento;
- prevenire il degradamento di qualità, sicurezza ed affidabilità di ciascuna apparecchiatura;
- evidenziare particolari situazioni di obsolescenza e degrado delle prestazioni.

Essa è comprensiva della manodopera e di tutte le parti di ricambio, materiali di utilizzo e consumo per i quali il produttore ne prescrive la sostituzione.

Il Concorrente dovrà dettagliare nel Progetto Offerta come intende gestire il servizio di manutenzione preventiva, in termini di organizzazione del personale, logistica nelle strutture ospedaliere, e visite preventive.

Entro 15 giorni dalla stipula dei contratti, l'Aggiudicatario dovrà comunicare al DEC, il programma di manutenzione per l'anno solare in corso. Parimenti entro il mese di gennaio di ogni anno solare, l'Aggiudicatario dovrà trasmettere al DEC il Programma di Manutenzione dell'intero anno solare.

In considerazione dell'imprevedibilità delle esigenze del servizio ospedaliero utilizzatore della soluzione fornita, l'Aggiudicatario è tenuto a verificare preventivamente la disponibilità delle apparecchiature alla data fissata per la manutenzione.

In prossimità della data di manutenzione si prenderanno accordi diretti con l'Unità Operativa interessata per confermare la data stessa dell'intervento, l'orario, la disponibilità dell'apparecchiatura e di un operatore dell'Unità Operativa che possa verificare al termine dell'intervento il funzionamento della stessa e firmare il report di intervento.

Ogni attività manutentiva preventiva dovrà essere accompagnata da un rapporto che indichi tutte le informazioni dell'intervento eseguito quali, a titolo di esempio non esaustivo, data e durata dell'intervento, evento generante e dati di chi ha segnalato l'anomalia, operatori intervenuti, operazioni effettuate, avvenuta risoluzione della segnalazione e/o eventuali operazioni successive che si rendessero necessarie. Il rapporto deve essere firmato dall'utilizzatore e dal tecnico esecutore e dovrà essere inviato a mezzo mail all'indirizzo sistemiinformativi@asst-ovestmi.it non oltre 3 giorni lavorativi dall'esecuzione.

Non sono ammessi report cumulativi riguardanti più interventi o report relativo alla stessa chiamata che perdura per più giorni di attività ovvero per ogni giorno di attività dovrà essere fatto uno specifico report anche se l'intervento non si è concluso.

Le prestazioni di manutenzione dovranno essere eseguite da tecnici specializzati e secondo le indicazioni previste dal costruttore.



27 Manutenzione Correttiva

Per manutenzione correttiva si intende quanto previsto dalle normative vigenti, ovvero una manutenzione richiesta su guasto, oppure sul malfunzionamento identificato durante la manutenzione preventiva, controlli funzionali o verifiche di sicurezza elettrica.

Le attività di manutenzione correttiva dovranno essere eseguite da tecnici specializzati e secondo le indicazioni previste dal costruttore.

La sostituzione di parti sia hardware che software, che ripristinano la funzionalità precedente dell'apparecchiatura non sono da intendersi come aggiornamenti tecnologici e sono a carico dell'aggiudicatario, ad esempio sostituzione pc, ups, reinstallazione software, compressori, etc.

I ricambi, materiali e accessori necessari alla risoluzione del guasto dovranno essere originali o certificati compatibili dall'azienda produttrice dell'apparecchiatura.

I costi per i ricambi saranno a carico della ditta aggiudicataria che si farà carico della gestione del relativo magazzino.

L'aggiudicatario dovrà prevedere la riparazione delle apparecchiature comprensiva di parti di ricambio originali o la sostituzione a titolo definitivo (nel caso di impossibilità di ripristino) delle apparecchiature (workstation, stampanti...) e relative periferiche esterne ed interne con apparecchiature che dovranno avere prestazioni e caratteristiche tecniche uguali o superiori a quelle sostituite previa autorizzazione dell'Azienda. Nulla sarà dovuto dall'Azienda, anche nel caso di chiamate per cui, in seguito all'intervento tecnico, non venga riscontrato nessun guasto.

Gli interventi di manutenzione correttiva sono da intendersi illimitati nell'ambito della durata del contratto. Tutti i costi diretti e indiretti sono a carico della ditta aggiudicataria.

Le richieste di intervento dovranno pervenire al recapito della ditta aggiudicataria via posta elettronica, tramite sistema informativo, oppure telefonicamente ed il fornitore assegnerà un numero di ticket alla segnalazione. La ditta concorrente produrrà in offerta un documento con tutti i recapiti richiesti, insieme alla descrizione dell'organizzazione del servizio di assistenza tecnica offerto.

Ogni attività manutentiva dovrà essere accompagnata da un rapporto che indichi tutte le informazioni dell'intervento eseguito quali, a titolo di esempio non esaustivo, data e durata dell'intervento, evento generante e dati di chi ha segnalato l'anomalia, operatori intervenuti, operazioni effettuate, avvenuta risoluzione della segnalazione e/o eventuali operazioni successive che si rendessero necessarie.

L'originale del verbale di intervento debitamente compilato e firmato dal tecnico esecutore e dall'utilizzatore sarà inviato all'indirizzo sistemiinformativi@asst-ovestmi.it entro e non oltre 3 giorni lavorativi dalla chiusura dell'intervento.

Non sono considerati accettabili verbali di intervento cumulativi su più ticket.

Si intendono ricomprese nelle attività di manutenzione correttiva le modifiche di configurazione di rete.

Tutte le attività correttive indicate nella gestione dei warning/avvisi di sicurezza si intendono ricomprese nel contratto di manutenzione sia per le parti HW che SW.

Sono da intendersi ricompresi nel contratto anche gli aggiornamenti di sicurezza del sistema operativo, e sono da ritenersi alla stregua delle manutenzioni correttive.

Al termine di ogni anno solare l'aggiudicatario dovrà inviare al DEC elenco con data e tipologia degli aggiornamenti fatti ivi inclusi quelli di tipo informatico hardware e software.

L'eventuale ripresentarsi del medesimo guasto o di guasto simile entro tre giorni lavorativi successivi alla data di risoluzione comporterà ai fini del livello di servizio, l'annullamento della chiusura dell'intervento precedente.

Nei conteggi rientrano anche le riparazioni effettuate da terze parti.

**ASST Ovest Milanese**

Qualora la Ditta aggiudicataria non fosse in grado di risolvere l'intervento in modo autonomo, potrà ricorrere al produttore o ad altra ditta qualificata, opportunamente subappaltata; questo non dovrà essere motivo di disagio per gli utilizzatori e varranno le stesse indicazioni riportate nei paragrafi precedenti sia per i tempi di intervento sia per i tempi di risoluzione e in caso di mancato rispetto verranno applicate le penali.

Anche in questo caso gli oneri economici conseguenti (manodopera, trasferta, ricambi, ecc.) saranno a totale carico della ditta aggiudicataria.

Nel caso in cui l'utilizzatore documenti e motivi per iscritto l'inefficacia dell'intervento correttivo sarà facoltà dell'azienda richiedere e ottenere dall'aggiudicatario l'intervento diretto della ditta produttrice a totale onere dell'aggiudicatario stesso.

28 Livelli di servizio

Si richiede l'erogazione del servizio 7x24x365 secondo i seguenti livelli di servizio:

LIVELLO DI GRAVITA'	TEMPO DI PRESA IN CARICO	TEMPO DI INTERVENTO	PENALI
ALTO – i sistemi e/o le infrastrutture hardware e software sono bloccate o presentano malfunzionamenti che impediscono la continuità operativa o hanno impatto sulla sicurezza informatica	1 ora solare	2 ore solari (comprende l'ora di presa in carico)	100 € per ogni ora solare di ritardo
MEDIO - sistemi e/o le infrastrutture hardware e software sono bloccate o presentano malfunzionamenti che non impediscono la continuità operativa, né hanno impatto sulla sicurezza informatica, ma rappresentano comunque problematiche da risolvere con urgenza	2 ore solari	3 ore solari (comprende le 2 ore di presa in carico)	50 € per ogni ora solare di ritardo
BASSO – il malfunzionamento non impatta la continuità operativa, né la sicurezza informatica	24 ore solari	48 ore solari (comprende le 24 ore di presa in carico)	50 € per ogni giorno solare di ritardo