 <p><b>AS FO</b> Azienda sanitaria Friuli Occidentale</p> <p>REGIONE AUTONOMA FRIULI VENEZIA GIULIA</p>	<p><b>Azienda sanitaria Friuli Occidentale</b></p> <p><b>Allegato specifiche IT Medicali e Analitici AsFO</b></p>
--	---

## **Allegato specifiche IT Medicali e Analitici AsFO**

### **Introduzione**

Il presente documento ha come scopo regolamentare, tramite informazione e categorizzazione in casi d'uso, l'ingresso dei nuovi sistemi forniti in qualsivoglia modalità (acquisto, noleggio, service, donazione, ...).

La parte informativa del documento rappresenta le specifiche che i sistemi/beni forniti dovranno rispettare relativamente all'area IT. Nel documento verrà fornita una panoramica che riporterà concetti fondamentali sulla tipologia di rete presente in AsFO e le metodologie legate all'integrazione dei sistemi offerti con quelli esistenti.

La categorizzazione dei casi d'uso viene definita in coerenza con la legislazione vigente, normativa generale e specifica di settore, linee guida e best practice, sempre e comunque a tutela di AsFO, nell'interesse dell'Azienda e dei fruitori dei servizi erogati. Casi d'uso non riconducibili alla categorizzazione presentata dovranno essere analizzati e validati prima dell'affidamento del contratto.

In nessun modo elementi indicati nell'offerta tecnica da parte del fornitore, in contrasto con quanto riportato nel presente documento, avranno valenza contrattuale.

Resta inteso che dovrà essere fornito tutto il supporto necessario dal fornitore e tutta la documentazione utile riguardante i sistemi forniti per consentire ad AsFO di rispondere a tutte le indicazioni rappresentate nella governance nazionale vigente per l'area di riferimento.

### **Normativa e tecnica di riferimento**

**Privacy:** corrispondenza dei sistemi e beni a quanto indicato - dal Regolamento Europeo sulla Protezione dei Dati – GDPR del 14.04.2016 (<https://eur-lex.europa.eu/>) e al D. Lgs. 196/2003 s.m.i., cosiddetto Codice Privacy, così come novellato dal d.lgs. 101/2018; l'aggiudicatario verrà designato responsabile ex art.28 del GDPR e dovrà produrre ed attuare tutto quanto richiesto, per quanto pertinente prima del collaudo e per tutta la durata del contratto.

**Cybersecurity-cloud:** corrispondenza di quanto fornito alla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", con livello ALTO; inoltre l'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'AsFO è chiamata a redigere in ottemperanza alla suddetta circolare AGID.

In riferimento allo sviluppo e all'acquisizione di software dovranno essere rispettate le indicazioni di AgID secondo quanto riportato nelle "linee guida di sicurezza nello sviluppo delle applicazioni". Dovrà essere garantita la conformità alle regole sull'interoperabilità prescritte dalle linee guida emanate in attuazione dell'art. 73 del CAD.

Dovrà essere possibile per AsFO esportare l'intera base di dati (inclusi di ogni tipo di indice o metadato utilizzato per implementare le funzionalità del software stesso) in formato standard e

aperto, per scongiurare la possibilità di lock-in, come meglio specificato nelle linee guida n.8 di ANAC.

Il fornitore si renderà disponibile a produrre il dettaglio del oggetto di fornitura per permettere ad AsFO di ottemperare a quanto indicato nella Direttiva NIS 2016/1148 e d.lgs 65/2018, Decreto NIS e , se necessario, nel decreto legge n.105/2019 “Perimetro Nazionale di Sicurezza Cibernetico” e decreti attuativi.

Nello specifico è richiesta la disponibilità del fornitore per supportare AsFO o suoi delegati nei precorsi di analisi e miglioramento previsti dal Framework Nazionale per la Cybersecurity e Data Protection, ovvero dalla normativa nazionale vigente in materia di cybersecurity.

Disponibilità totale del fornitore a fornire le informazioni necessarie e intraprendere i percorsi per permette ad AsFO di ottemperare a quanto indicato e definito dall'Agenzia per la Cybersicurezza Nazionale (ACN) e dal Dipartimento per la Trasformazione Digitale (DTD) in relazione alla cybersecurity e al cloud.

### **Requisiti/riferimenti particolari**

La rete aziendale di AsFO, in quanto integrante dispositivi e applicazioni individuati come dispositivo medico secondo MDR (e IVDR), e quanto definito all'art.120 del regolamento per il periodo transitorio, si intende come rete IT medica ai sensi di quanto indicato dalla norma ISO IEC 80001-1.

In conseguenza di ciò si precisa che il collaudo di sistemi (inclusivi di DM e non) sarà condizionato alla redazione e sottoscrizione di un accordo di responsabilità, dove si evidenziano i profili di responsabilità della gestione della fornitura (DRW). Ad esempio la gestione di server virtualizzati, patch OS, dominio, integrazioni e visibilità.

Se l'oggetto di fornitura include dispositivi medici, il fornitore dovrà compilare, sottoscrivere e allegare all'offerta tecnica il modulo Manufacturer Disclosure Statement for Medical Device Security (MDS2) versione 2019 per ciascuno di essi, in maniera da permettere ad AsFO una più agevole valutazione delle eventuali criticità della messa in uso dei sistemi offerti anche secondo EC/TR 80001-2-2. È comunque onere del fornitore verificare la versione più recente del modulo dal sito NEMA e compilare e fornire tale versione.

Inoltre, sempre nel caso in cui l'oggetto di fornitura includa dispositivi medici, il sistema fornito dovrà rispondere a quanto richiesto:

- dal IHE Patient Care Device (PCD) White Paper, “Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide”;
- dalla linea guida “MDCG 2019-16 Guidance on Cybersecurity for medical devices”.

In generale l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e del trattamento dei dati affidato nell'ambito di quanto richiesto dalla presente procedura d'acquisto/noleggio/service/donazione, in particolare in merito all'integrità, disponibilità e riservatezza dei dati e dei sistemi. Pertanto, anche nei casi in cui la sicurezza dei dati gestiti dai sistemi oggetto di fornitura possa essere legata agli effetti di altro hardware e software in gestione ad un soggetto terzo, l'aggiudicatario rimane responsabile di monitorare tali elementi e segnalare in via formale qualora ritenga vi siano aspetti di inadeguatezza. In tale responsabilità ricade anche l'onere di richiedere gli strumenti per fare gli audit ed il monitoraggio, per eseguire le ricerche di anomalie, oltre alla comunicazione formale delle proposte percorribili per raggiungere gli obiettivi.

In coerenza con quanto stabilito dal Piano Triennale AGID che suggerisce un approccio “cloud first”, i servizi oggetto di fornitura potranno essere erogati in modalità SaaS, aderente nell'erogazione

(tipologia e qualificazione del soggetto erogatore) a quanto indicato dalla Strategia Cloud Italia, fermo restando tutte le prescrizioni riportate nel presente documento. I servizi erogati in modalità SaaS dovranno essere pubblicati sul Cloud Marketplace di ACN, la piattaforma che espone i servizi e le infrastrutture qualificate da ACN secondo quanto disposto nel Decreto direttoriale prot. N. 29 del 02/01/2023.

La soluzione messa a disposizione attraverso l'infrastruttura in cloud dovrà rispettare i requisiti previsti da ACN (QC2 e QI2), in conseguenza del fatto che verrà utilizzata per l'erogazione di un servizio trattante dati di livello critico secondo la classificazione definita all'interno della Strategia Cloud Italia pubblicata a settembre 2021 dall'Agenzia per la Cybersicurezza Nazionale e il Dipartimento per la Trasformazione digitale.

L'infrastruttura cloud dovrà essere tra quelle qualificate per la gestione dei servizi e dati classificati come critici (Cloud qualificato di tipo pubblico criptato, privato/ibrido e privato) e pertanto coerente con quanto indicato nella determina ACN n. 307 del 2022, tenendo in considerazione quanto indicato all'art.2 decreto direttoriale di ACN n. 29 del 2 gennaio 2023, che discrimina la fase transitoria nel passaggio di gestione da AgID a ACN.

Sarà prevista una fase di test di funzionamento - con la simulazione di interruzioni/guasti- per validare l'affidabilità, la resilienza e la conformità del sistema ai livelli di servizio attesi.

Nel caso la connettività verso il servizio in cloud venga fornita attraverso la rete RUPAR, ritenuta conforme ai requisiti prestazionali richiesti dalla soluzione applicativa - in ottemperanza alla strategia Cloud Italia contenente le indicazioni strategiche per la migrazione dei dati e servizi digitali classificati come critici - il fornitore dovrà garantire la distribuzione dei servizi in cloud (SaaS) in alta affidabilità con peering VPC.

I servizi SaaS offerti dovranno essere fruibili tramite collegamento internet invocabile con i web browser in uso presso AsFO e senza alcun componente aggiuntivo sul browser stesso o sul client in generale; la sicurezza delle connessioni tra browser e servizi SaaS remoti dovrà essere adeguata alla tipologia di dati scambiati, in ogni caso dovrà essere adottato il protocollo HTTPS (TLS 1.2 o superiore - in ogni caso non deprecato - con certificato pubblico in gestione e a carico dell'aggiudicatario; tale certificato dovrà essere riconosciuto come valido dai browser di cui sopra, senza specifiche configurazioni, ovvero non dovranno essere usati certificati di tipo self-signed) e in alcun caso verranno realizzate connessioni VPN o di altro tipo ad hoc, per sopperire ad eventuali carenze architetture in termini di sicurezza o funzionalità, quindi resta inteso che i servizi dovranno sempre essere fruibili in maniera efficace e sicura tramite internet. I server che contengono i dati trattati di titolarità AsFO dovranno risiedere all'interno della UE e per nessuna ragione dovranno essere effettuate copie di tali dati al di fuori del perimetro della UE, neppure per motivi di continuità di servizio e disaster recovery.

Sarà ammessa, e fortemente consigliata, la predisposizione di apparati edge (preferibilmente virtuali, eventualmente su infrastruttura messa a disposizione da AsFO), ovvero server applicativi che possano garantire la piena continuità di servizio in caso di irraggiungibilità del cloud, in un'ottica di applicazione delle best practice di Business Continuity come suggerito dalla norma ISO/IEC 22313:2020. Il server edge dovrà avere ridottissima profondità temporale. Gli apparati di edge dovranno essere adeguatamente dimensionati (inteso come prestazioni) per l'erogazione di tutti i servizi con la massima efficienza, compresi eventuali servizi di server side rendering necessari all'erogazione dei tool avanzati.

AsFO è responsabile per la sola parte di corretta esecuzione dell'ambiente virtualizzato su cui insistono le macchine virtuali, alimentazione e raffrescamento dei locali tecnici e del collegamento verso la LAN Aziendale, eventualmente verso internet se la connettività verso il sistema in cloud non

è provvisto di doppia connessione dedicata fornita dall'aggiudicatario.

Restano in capo all'aggiudicatario la gestione del S.O. della macchina (aggiornamenti e patch di sicurezza), politiche di backup e replica in cloud coerenti con la tipologia di servizio e tutto quanto il necessario alla corretta erogazione del servizio applicativo ad esclusione della connettività alla LAN.

Nel caso in cui l'oggetto di fornitura sia o contenga un software DM è necessario fornire adeguata documentazione da parte del fornitore relativa all'impossibilità di procedere con gli aggiornamenti, di qualsiasi tipo.

Le attività di aggiornamento dovranno essere comunque concordate e documentate nel report DAPS relativo al contratto che verrà stipulato e che lo seguirà lungo tutto il suo periodo di validità.

Qualsiasi malfunzionamento o interruzione del servizio, dovuta al non corretto dimensionamento della infrastruttura è da considerarsi a carico del fornitore.

L'accesso ad Internet (anche cloud del fornitore) delle soluzioni oggetto di fornitura va documentato, validato e attivato solo a seguito della nomina a Responsabile al trattamento del fornitore, su proposta di AsFO.

L'accesso dovrà essere regolamentato come segue:

- autorizzato;
- indicato nel "documento riepilogativo attori e transazioni"
- seguire il principio di minimizzazione dei dati (GDPR);
- solo verso indirizzi specifici;
- solo tramite canali cifrati;
- mantenuto aggiornato.

L'accesso da internet, solamente per scopi manutentivi, alle soluzioni oggetto di fornitura va documentato, validato e attivato solo a seguito della nomina a Responsabile al trattamento del fornitore, su proposta di AsFO.

L'accesso dovrà essere regolamentato come segue:

- autorizzato;
- indicato nel "documento riepilogativo attori e transazioni"
- seguire il principio di minimizzazione dei dati (GDPR);
- solo sulle apparecchiature oggetto di fornitura;
- solo tramite VPN aziendale;
- solo con account nominale;
- possibilmente con MFA.

Con cadenza trimestrale l'aggiudicatario dovrà fornire report degli accessi fatti in VPN per la validazione, indicando: utente, motivazione, attività svolta durata dell'intervento. AsFO potrà in qualsiasi momento richiedere un report anticipato rispetto a quelli programmati per confrontarli con i log del servizio VPN.

### **Autenticazione applicativa**

Relativamente al sistema di autenticazione da utilizzare, dovrà essere possibile attivare nel corso di tutta la durata contrattuale, a discrezione di AsFO e senza oneri aggiuntivi per AsFO stessa, il SSO così come di seguito descritto: AsFO è dotata di un sistema IdP basato su tecnologia Microsoft ADFS v3.0, accessibile dalla rete privata regionale RUPAR, ed i sistemi oggetto di fornitura dovranno interfacciarsi con tale IdP tramite il protocollo SAML v2.0. In tal senso dovrà essere possibile l'autenticazione ai sistemi forniti tramite le credenziali di dominio Microsoft Active Directory di AsFO,

se i servizi sono fruiti dall'interno delle reti private RUPAR, oppure dal sistema di autenticazione fornito da Insiel S.p.A. SIALI, di cui andranno poi comunicate le specifiche d'integrazione.

### **Ulteriori requisiti e best practices**

Inoltre, sempre in coerenza con quanto stabilito da AGID, i sistemi forniti dovranno essere progettati, realizzati ed installati in modo da minimizzare fenomeni di lock-in e in ogni caso, durante gli ultimi due trimestri di durata del contratto ed eventualmente per i tre mesi successivi, e comunque fino al raggiungimento dell'obiettivo, l'aggiudicatario dovrà favorire in ogni modo il travaso e la fruizione dei dati verso sistemi di terze parti, il che sarà vincolante al pagamento delle ultime due fatture in caso di servizio, applicazione di penale in caso di singola fornitura. Tali attività ed i servizi professionali e tecnici associati sono perciò da intendersi oggetto di fornitura del presente contratto. Dovrà essere indicato chiaramente in offerta tecnica in quale contesto tecnologico (client DM/IVD, client SaaS ibrido, client SaaS con edge così come descritti nel presente documento) ricade l'offerta presentata e dovrà essere dettagliato come - tecnicamente e organizzativamente - l'aggiudicatario intende rispondere alle prescrizioni del presente documento.

In caso di soluzioni rientranti nei contesti 2 e 3 con utilizzo del sistema di virtualizzazione di AsFO come primario o come edge dovrà inoltre essere indicato in offerta tecnica il numero di risorse computazionali richieste (almeno: numero di macchine virtuali, sistema operativo, funzione, RAM, core, spazio disco, necessità in termini di backup e disaster recovery). Se tali richieste dovessero risultare non congrue rispetto alle finalità del contratto o non sostenibili per la stazione appaltante ad insindacabile giudizio di AsFO, AsFO stessa si riserva di richiedere il passaggio alla soluzione SaaS definita nel contesto 3 senza oneri aggiuntivi.

In generale per l'analisi preliminare e l'avviamento all'uso dei sistemi oggetto di fornitura AsFO metterà a disposizione 5 giornate uomo di tecnico sistemista senior e 5 giornate uomo di project manager. La mancanza di autonomia operativa da parte dell'aggiudicatario o particolari necessità di assistenza svolta da personale AsFO, che vadano oltre i limiti sopra riportati, verranno computati da AsFO che si riserva la facoltà di quantificare le relative spese in base al listino allegato alla Convenzione Consip attiva con a listino il servizio necessario o più aderente, e di dedurle dal piano di fatturazione previsto. Con la partecipazione alla gara si intende accettato tale meccanismo compensativo.

Nel caso in cui il sistema fornito, indipendentemente dal contesto di mesa in servizio in cui si trovi, debba integrarsi con il SIO per esportare dati con lo scopo di:

- alimentare maschere di refertazione;
- richiamare altri applicativi (Insiel) con chiamate di contesto;
- aggiungere dati strumentali alla documentazione di referto;
- produrre un referto autonomamente e inviarlo al SIO per la conservazione;

dovrà ottemperare a quanto indicato nelle regole tecniche Fascicolo 2.0 e nella documentazione di HL7 Italia ([http://www.hl7italia.it/hl7italia\\_D7/node/2359](http://www.hl7italia.it/hl7italia_D7/node/2359)). Questo per rispettare nello specifico le modalità e le metodiche di creazione controllo e validazione dei referti, inclusa la tipologia di firma digitale applicata al documento.

Per le apparecchiature radiologiche è obbligatoria la possibilità di ottenere tramite report DICOM SR i dati di dose per la categorizzazione della procedura clinica in una delle classi di esposizione come definito dalla Direttiva EURATOM 2013/59, recepita con d.lgs. 101/2020 e modificato dal d.lgs. 203/2022.

### **L'infrastruttura di ASFO ed integrazione**

I sistemi oggetto di fornitura dovranno essere integrati ed interfacciati con l'infrastruttura informatica di rete e sistemistica di AsFO, secondo quanto riportato nel seguito.

I dispositivi dotati di connettività di rete (host) che necessitano di collegamento alla rete dati per svolgere le funzioni richieste, potranno essere inseriti nella LAN dell'azienda di destinazione seguendo uno degli scenari descritti nel seguito.

I firewall aziendali, utilizzati come ISFW a protezione di ciascuno dei contesti di rete descritti nel presente documento (reti e VLAN), sono tecnologicamente dei NGFW (Next Generation Firewall) dotati di funzionalità di statefull inspection e con application control attivo, conseguentemente tutti i sistemi e le applicazioni oggetto di fornitura, nonché i servizi di assistenza remota e manutenzione, anche erogati tramite VPN, dovranno essere compatibili con tali tecnologie. AsFO si riserva di bloccare qualunque tipologia di traffico ritenuto malevolo, in particolare a fronte di specifiche vulnerabilità che dovessero emergere nel corso della durata contrattuale.

Non sarà in generale consentita la fornitura di sistemi di cablaggio dati dedicati, a meno di casi particolari tecnicamente motivati, che dovranno essere esplicitati in offerta tecnica, motivati dettagliatamente ed approvati in ultima istanza da AsFO. Riguardo al cablaggio strutturato, dovranno essere utilizzati sempre e comunque i sistemi aziendali e gli eventuali ampliamenti necessari saranno eseguiti da AsFO. Dovranno essere indicati in offerta tecnica il numero e la dislocazione spaziale dei punti rete necessari al funzionamento dei sistemi oggetto di fornitura, indicando per ciascun punto l'eventuale necessità di installazione di dispositivi di separazione (Separation Device) conformi alle norme IEC 60601-1, la cui installazione sarà a carico di AsFO. Nel caso in cui l'aggiudicatario volesse comunque offrire servizi di posa in opera di cablaggio strutturato, dovrà sottostare alle indicazioni e validazioni progettuali di AsFO, oltre alle norme tecniche di riferimento.

AsFO potrà avvalersi di supporto specialistico per l'esecuzione di VA/PT dei sistemi collegati alla propria rete. Pertanto il fornitore potrebbe essere chiamato da AsFO per fornire supporto ed eseguire verifiche funzionali legate all'esecuzione dei VA/PT in giornate programmate e concordate. Il costo per il ripristino del funzionamento è da intendersi completamente a carico del fornitore.

## **Scenari**

### **Specifiche comuni**

In funzione del tipo di sistema/soluzione/apparecchiatura verrà valutata la possibilità di applicare politiche di segmentazione della rete in coerenza con i fabbisogni aziendali, criticità e necessità per le apparecchiature. In quel caso i dispositivi oggetto di fornitura saranno integrati nella sole infrastrutture di rete di AsFO e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico verrà effettuata assegnando agli host stessi una specifica classe di indirizzi IP statici o tramite il servizio DHCP aziendale operando specifiche reservation in modo coerente con il piano di indirizzamenti di AsFO e verranno inseriti in una VLAN dedicata, assegnata da AsFO stessa, dalla quale potranno effettuare solo l'eventuale traffico necessario per svolgere le funzioni richieste in capitolato e l'eventuale traffico relativo all'assistenza remota da parte del fornitore come definito nel documento DRW. La segregazione del traffico verrà garantita tramite configurazioni sui firewall aziendali (ISFW – Internal Segregation Firewall), stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico, evidenziate anche dal DRW per svolgere le funzioni richieste in capitolato. Il fornitore dovrà garantire piena collaborazione nella redazione di tali regole sui firewall aziendali (ISFW – Internal Segregation Firewall), per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia, in particolare

la rete IP/VLAN assegnata avrà visibilità di rete sulle reti IP/VLAN dei PC di AsFO solo in caso di necessità. AsFO si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.

Nel caso in cui i dispositivi forniti siano di tipo trasportabile, palmari o mobile (tablet, smartphone, ecc) la connettività verrà garantita unicamente per mezzo di connessione cablata o Wi-Fi e solo per l'attività clinica, secondo quanto riportato precedentemente. Non sarà consentito in alcun caso il collegamento di tali dispositivi tramite le postazioni di lavoro (PC) – per esempio con collegamenti USB –. I collegamenti cablati dovranno essere realizzati con un adeguato grado di resistenza meccanica, nel caso per esempio dei dispositivi palmari o mobile, dovrà essere fornita una docking station.

### **Accessi VPN**

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dagli amministratori di sistema e o dai tecnici formalmente nominati dall'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN validati da AsFO. L'accesso verrà consentito solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario – compilando il modulo standard allegato "Modulo B" – ed inviato via PEC alla casella PEC di AsFO, con allegati i documenti di identità e CF in corso di validità dei soggetti da abilitare. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali con bassi privilegi (livello user), ed in alcun caso saranno consentite connessioni di tipo site-to-site. A valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza dovrà avvenire esclusivamente con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi da parte di AsFO. Il servizio di connessione remota VPN non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio VPN in altro modo (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio VPN.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo da internet dei sistemi oggetto di assistenza gli scenari possibili sono due:

1. firewall di navigazione gestito dalla società in house della Regione Autonoma Friuli Venezia Giulia denominata Insiel SpA;
2. Firewall di navigazione gestito da AsFO;

In ogni caso i sistemi forniti potranno raggiungere solo un numero limitato di destinazioni internet, su specifiche porte; il traffico consentito sarà quello minimo necessario per il funzionamento dei sistemi e non sarà consentita la navigazione internet nonché l'esfiltrazione di dati tramite questo canale. Verranno perciò effettuate specifiche abilitazioni basate su IP sorgente, IP destinazione e porta solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario ed inviata via PEC alla casella PEC di AsFO o in risposta alla RdO/ODA effettuata, consegnando il "Modulo A" dettagliatamente compilato. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso per la definizione delle suddette abilitazioni. Analogamente al servizio VPN individuato da AsFO, anche il servizio di connettività in uscita non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio in altro modo (per esempio con intervento sul posto

o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio.

## **CONTESTI**

Di seguito si riportano i vari contesti a cui devono essere ricondotte tutte le soluzioni presentate in sede di offerta. Eventuali offerte non riconducibili a nessuna delle tre situazioni dovranno essere valutate di volta in volta e dovranno comunque rispettare le caratteristiche indicate nel documento con il più alto grado di attinenza al possibile contesto di affinità.

### **Contesto 1 Client o singolo DM/IVD**

Singolo dispositivo o PC, collegabile alla rete aziendale, che riceve, invia o salva localmente informazioni di tipo diagnostico.

### **Contesto 2 Client Saas ibrido**

Sistema client server, dove la parte server risiede all'interno dell'infrastruttura virtualizzata di proprietà di AsFO, la quale assicura alimentazione elettrica, raffreddamento e ripristino della macchina secondo le specifiche di backup concordate con il fornitore in fase di configurazione. Sarà cura dell'aggiudicatario tutto quanto il necessario al mantenimento della soluzione al top delle performance, e dovrà provvedere agli aggiornamenti lato applicativo e OS dandone preventiva comunicazione ad AsFO. Nel caso siano disponibili aggiornamenti dovrà essere cura dell'aggiudicatario avvisare tempestivamente AsFO per valutare e programmare le attività necessarie. Per l'esecuzione dei servizi verrà realizzato un utente di servizio con cui dovranno essere eseguiti i tasks propri dell'applicativo per garantirne il funzionamento. AsFO si riserva comunque la possibilità, a proprio insindacabile giudizio, di operare con la dismissione e spegnimento del sistema nel caso in cui si venisse rilevata una criticità che possa compromettere l'erogazione del servizio e di conseguenza possa generare un danno alla salute dei pazienti e operatori. In ogni momento AsFO potrà richiedere il passaggio al contesto 3 della soluzione durante tutto l'arco contrattuale senza alcun onere aggiuntivo.

RPO e RTO verranno stabiliti in base alla criticità del servizio.

### **Contesto 3 Client - Saas con edge**

Vale tutto quanto come sopra, in aggiunta il sistema dovrà lavorare con replica sincrona nell'infrastruttura cloud messa a disposizione dall'aggiudicatario (di livello QC2 o QS2) e/o nello spazio Cloud messo a disposizione da AsFO (PSN oppure Cloud qualificato privato disponibile in convenzione e rispondente alla normativa vigente in relazione alla tipologia di servizio fornito). Sarà a carico dell'aggiudicatario verificare le performance della soluzione e che le stesse rispondano ai bisogni relativi all'erogazione del servizio.

La parte EDGE verrà gestita come da contesto 2, la parte in cloud dovrà essere fornita interamente in Saas. Il sito di erogazione primaria verrà definito sulla base della criticità del servizio e delle performance di connettività.

## **Requisiti ulteriori comuni ai contesti**

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare, sia nel caso di non collegamento in rete, sia di realizzazione aderente ai vari contesti, relativamente ad aspetti generali della sfera dell'IT (Information Technology) con particolare riferimento alla sicurezza informatica (security).

Vale in ogni caso il principio generale per cui la sicurezza informatica è un fattore intrinseco dell'architettura dei sistemi oggetto della presente fornitura e delle caratteristiche tecniche degli



elementi che li compongono; perciò l'aggiudicatario dovrà garantire che, sia l'architettura che gli elementi, siano progettati, implementati e mantenuti nel tempo in modo da minimizzare il rischio informatico residuo (sia di "attacchi ai sistemi" che di "attacchi dai sistemi") e comunque in osservanza delle normative e best practice già citate dal primo paragrafo del presente documento e sempre in coerenza con il paradigma "Zero Trust".

Potrebbero eseguite periodicamente da AsFO o da personale a tal scopo incaricato procedure di Vulnerability Assessment e Penetration Test e l'aggiudicatario si impegna pertanto a risolvere criticità o vulnerabilità che dovessero in tal modo emergere. Analogamente l'aggiudicatario si impegna a collaborare con il SOC (Security Operation Center) di AsFO per il miglioramento continuo dei sistemi forniti.

Inoltre i sistemi forniti dovranno rispettare le seguenti prescrizioni.

In generale, tutti gli elementi forniti non dovranno essere in alcun caso fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato per tutta la durata contrattuale.

In generale, tutti i software forniti dovranno essere:

- coerenti con la necessità di richiedere applicazioni, servizi e procedure privacy by design e privacy by default per ogni percorso di trattamento. Tutti i sistemi devono essere costruiti per proteggere i dati trattati e farlo come impostazione predefinita. L'aggiudicatario è tenuto a fornire documentazione delle misure implementate anche allo scopo di permettere le necessarie valutazioni al Titolare;
- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
- dotati di impostazioni internazionali di Microsoft Windows (se presente) IT standard, comprese le tastiere, allo scopo di non incorrere in nessun caso in errori nelle date, nei dati numerici e nei dati personali locali;
- stabili, in particolare che siano in grado di gestire le eccezioni;
- sicuri, sia dal punto di vista della sicurezza informatica che della qualità delle funzioni svolte;
- ottimizzati, in termini di rapporto tra uso delle risorse e prestazioni;
- sviluppati tenendo conto dei principi del "ciclo di vita del software" e dell'"analisi del rischio", secondo le norme tecniche (o principi e metodologie almeno equivalenti) e le best practice internazionali; in ogni caso non dovranno utilizzare librerie deprecate e/o obsolete, né dovranno essere scritti e sviluppati con versioni del linguaggio di programmazione fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato per tutta la durata contrattuale;
- pensati, progettati e realizzati nel rispetto del quadro legislativo vigente, nonché in modo da non mettere in alcun caso gli operatori in condizione di violare il quadro legislativo stesso nell'espletamento del normale utilizzo dei sistemi;
- installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità, così come descritto nel presente documento;
- mantenuti e gestiti in modo da conservare e mantenere stabili nel tempo tutte le caratteristiche possedute al momento del collaudo definitivo.

In particolare, tutti i software forniti che verranno installati su dispositivi collegati alle LAN aziendali e inseriti nei rispettivi domini dovranno essere eseguiti sempre:

- in un contesto user space per i client,
- come servizio per tutti i server,
- come servizio per i client se non è richiesta interazione con l'operatore,

ed in ogni caso non dovranno essere modificati in alcun modo i permessi di default del file system e del registro di sistema Microsoft (ove presente).

In particolare, per quanto concerne le configurazioni:

- quelle degli applicativi server dovranno risiedere in database e comunque mai sui dischi locali dei PC client;
- quelle globali degli applicativi client (ovvero non riferite alle personalizzazioni dei singoli account) dovranno risiedere in un file nella cartella di installazione dell'applicativo (a cui quindi avranno accesso solo gli utenti con ruolo Amministratore) oppure nella cartella %HOMEDRIVE%\ProgramData, oppure nel registro di sistema (ove presente) nella sottochiave appositamente creata in fase di installazione in HKEY\_LOCAL\_MACHINE\SOFTWARE, ed in ogni caso informazioni critiche in termini di sicurezza e funzionalità (a titolo di esempio non esaustivo: le stringhe di connessione ai database, le credenziali necessarie per instaurare eventuali altre connessioni client/server, ecc.) dovranno essere cifrate almeno con algoritmo AES256;
- quelle personali degli applicativi client (ovvero riferite alle personalizzazioni dei singoli account) dovranno risiedere nel profilo dell'account a cui si riferiscono (ove presente).

Ovvero, in ogni caso non dovranno risiedere configurazioni globali degli applicativi client nei profili degli account, né altresì configurazioni personali degli applicativi client fuori dai profili degli account.

In particolare, a titolo esemplificativo e non esaustivo, si ricorda che, anche nel perimetro delle prescrizioni previste dalla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", i sistemi forniti:

- non devono prevedere nessun account locale;
- non devono prevedere nessun account impersonale per gli operatori e account di servizio solo se del tipo gMSA, group Managed Service Account;
- devono consentire azioni di software inventory;
- devono poter essere distribuiti in "package" fruibili dal sistema di distribuzione software;
- devono utilizzare solo sistemi di comunicazione sicuri (crittati);
- devono rispettare le tecnologie di protezione delle banche dati di dati personali e sensibili;
- devono consentire le valutazioni di vulnerabilità e il fornitore deve adoperarsi per la risoluzione in tempi certi ed accettabili delle anomalie rilevate da AsFO o dalle aziende da AsFO deputate.

In ogni caso i software oggetto di fornitura non dovranno fare uso di Applet Java e ActiveX.

Come indicato in premessa, l'aggiudicatario verrà designato responsabile ex art.28 del GDPR, ed in quest'ambito dovrà, tra l'altro, inviare, nel rispetto delle procedure di AsFO, le richieste di abilitazione degli incaricati e degli amministratori afferenti all'aggiudicatario (anche quelle necessarie per lo svolgimento delle attività di assistenza remota). I relativi account e le relative autorizzazioni verranno sempre erogate a livello personale, secondo le varie procedure aziendali ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

Per quanto concerne gli "account amministrativi" (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), questi:

- potranno, nel caso di account amministrativi locali di default (a titolo di esempio non esaustivo: "admin", "administrator", "root", ecc.), essere impersonali e dovranno essere tutti comunicati ad AsFO ove richiesto, AsFO potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi locali ulteriori rispetto a quelli di default; ove non richiesto da AsFO la gestione e responsabilità si intende completamente a carico dell'aggiudicatario;
- dovranno, nel caso di account amministrativi non locali che consentano l'accesso interattivo a macchine/sistemi/applicativi collegati alla LAN di AsFO, essere sempre personali e rispettare quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
- non dovranno, nel caso di account amministrativi impersonali, essere in alcun caso presenti, se non del tipo gMSA;
- dovranno, nel caso di tutti gli account di sistemi non in LAN, essere gestiti a cura e responsabilità dell'aggiudicatario;
- potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN di AsFO, essere impersonali e dovranno essere tutti comunicati ove richiesto, AsFO potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi in numero maggiore dello stretto necessario; ove non richiesti la gestione e responsabilità si intende a carico dell'aggiudicatario;

in tal caso, ovvero per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel punto precedente, questi non dovranno in alcun caso permettere:

- di modificare le configurazioni, impostazioni e settaggi di macchine/sistemi/applicativi;
- di visualizzare, modificare o cancellare dati personali diversi da quelli eventualmente trattati contestualmente all'uso dell'account stesso.

Eventuali dati personali salvati in ulteriori archivi, diversi da quelli descritti nel presente documento, saranno ammessi solo con funzioni di "archivi provvisori", ovvero di passaggio intermedio dei dati prima dell'invio agli archivi definitivi. I dati personali devono permanere negli archivi provvisori il minor tempo possibile, ovvero per un tempo massimo che sia configurabile e che in ogni caso non superi le 24 ore naturali, con l'implementazione di opportune procedure di cancellazione automatica che non consentano il recupero locale dei dati.

Ogni attività di aggiornamento, dovrà essere prima comunicata e validata da AsFO, testata e rilasciata nelle modalità concordate anche in coerenza con il possibile impatto sulla capacità di erogazione delle prestazioni sanitarie di AsFO. Tutte le attività di aggiornamento dovranno necessariamente essere indicate nel "Modulo C DAPS" che rappresenta parte integrante della documentazione relativa alla fornitura e potrà essere utilizzata per il rilascio della regolare esecuzione del servizio/fornitura affidato/a.

In ogni caso l'accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo da parte degli account personali e degli account gMSA autorizzati, sulla base di opportuni permessi settati in

modo che il livello dei privilegi di accesso sia il più basso possibile e che l'accesso ai dati avvenga sempre per tramite dell'applicativo e non direttamente da parte dell'account.

Non è consentita l'archiviazione, anche temporanea ed anche in forma anonima, dei dati su macchine situate esternamente rispetto alla rete di AsFO, salvo esplicita autorizzazione.

Non sarà in alcun caso consentita la fornitura ed installazione di apparati attivi di rete standard (switch, router, firewall, access point Wi-Fi, VPN concentrator, Mi-Fi etc.) a meno di eccezioni concordate e validate a seguito di presentazione di adeguata documentazione tecnica che ne giustifichi la necessità. In particolare: nel caso di apparati di sicurezza, l'aggiudicatario si impegna, come precedentemente riportato, a trasferire le logiche di sicurezza sui firewall Aziendali (ISFW – Internal Segregation Firewall); nel caso di apparati per la connettività remota, l'aggiudicatario si impegna a far uso degli strumenti aziendali messi a disposizione da AsFO, come precedentemente riportato.

## **PACS**

Il sistema PACS di AsFO è Suitestensa di Esaote S.p.A., configurato su livelli, che confluiscono nel PACS centrale di ASFO (P.O. di Pordenone) e per la parte di conservazione legale in Regione.

La connettività tra i vari livelli del PACS è garantita all'interno della rete Regionale FVG RUPAR, gestita da Insiel S.p.A.

Il Sistema RIS attualmente in uso, che fornisce anche il servizio di modality worklist è G2 Clinico, di Insiel S.p.A. Il servizio RIS è erogato all'interno della rete Regionale FVG RUPAR, gestita da Insiel S.p.A.

Le apparecchiature dovranno essere fornite complete delle licenze per la messa in rete e rispettare il seguente standard: DICOM 3.0 completo delle classi worklist, store, print, q/r, mpps, sc.

Per i dispositivi offerti dovrà essere data evidenza della corrispondenza ai profili di integrazione IHE. Tutte le licenze d'uso del software non devono avere scadenza o limiti temporali che possano determinare blocchi funzionali e/o che richiedano oneri per ASFO.

Per ogni apparecchiatura messa a disposizione dall'OE dovranno essere forniti:

- copia dell'"INTEGRATION STATEMENTS IHE" o in subordine, copia del Conformance Statement Standard DICOM 3.

## **LIS**

Specifiche di integrazione con il LIS

I sistemi oggetto di fornitura dovranno essere marcati CE IVD ai sensi della direttiva 98/79/CE relativa ai dispositivi medico diagnostici in vitro recepita con D.Lgs. 332/2000, ove applicabile.

Tutti i software di interpretazione dei dati oggetto di fornitura dovranno colloquiare bidirezionalmente con il LIS (Laboratory Information System) Aziendale. Il LIS attualmente in uso (non oggetto di fornitura) è DNLab di NoemaLife S.p.A. fornito da Insiel S.p.A., gestito e mantenuto da Insiel S.p.A. in tutta la Regione Friuli Venezia Giulia. Attualmente, è previsto che il DNLab si interfacci con la strumentazione analitica per mezzo del middleware HALIA di NoemaLife gestito da Insiel S.p.A. Pertanto, l'aggiudicatario dovrà interfacciare i software di interpretazione forniti con il sistema in uso al momento della consegna e, qualora questo sia DNA, si intende compreso nel prezzo di fornitura la successiva migrazione (secondo i tempi che saranno indicati) ad HALIA.

L'interfacciamento tra strumento/WAM (Work Area Manager)/Middleware e Halia dovrà avvenire tramite socket TCP e solo in caso di vincolo tecnico potrà essere realizzato tramite interfacciamento seriale. Tali casistiche andranno giustificate e motivate tecnicamente in offerta ed in ogni caso tali soluzioni dovranno essere insindacabilmente validate da AsFO; in tal caso dovranno essere oggetto

di fornitura i convertitori seriale/ethernet che si intendono perciò garantiti e certificati dal fabbricante per la specifica destinazione d'uso.

Versione	Data
0.2	17/04/2023

### **Documenti eventuali da allegare**

#### **Modulo A**

##### **Documento Riepilogativo Workflow "DRW"**

Nel caso di sistemi complessi, non dispositivi stand alone (anche stand alone ma che dovranno essere integrati con l'infrastruttura LAN di AsFO) si richiede di completare quanto previsto per contestualizzare le specifiche di funzionamento ed integrazione con AsFO.

Si richiede di fornire in offerta tecnica un "documento riepilogativo workflow" (esempio DRW Documento A), firmato digitalmente dove dev'essere evidenziato quanto segue:

- tipologia di architettura (anche a livello grafico);
- tipologie di trasmissioni indicando eventualmente il protocollo, la porta e la tipologia di dati trasmessi;
- elementi coinvolti (server, client, applicativo) e responsabilità di gestione, indicando eventualmente fornitori terzi e tipologia di accordo contrattuale tra fornitore e partner.

Prima parte grafica.

Seconda parte descrittiva: indicare attori coinvolti, tipologia di comunicazione (protocollo, porte, ...), figura responsabile

#### **Modulo B**

##### **Modulo richiesta VPN**

#### **Modulo C**

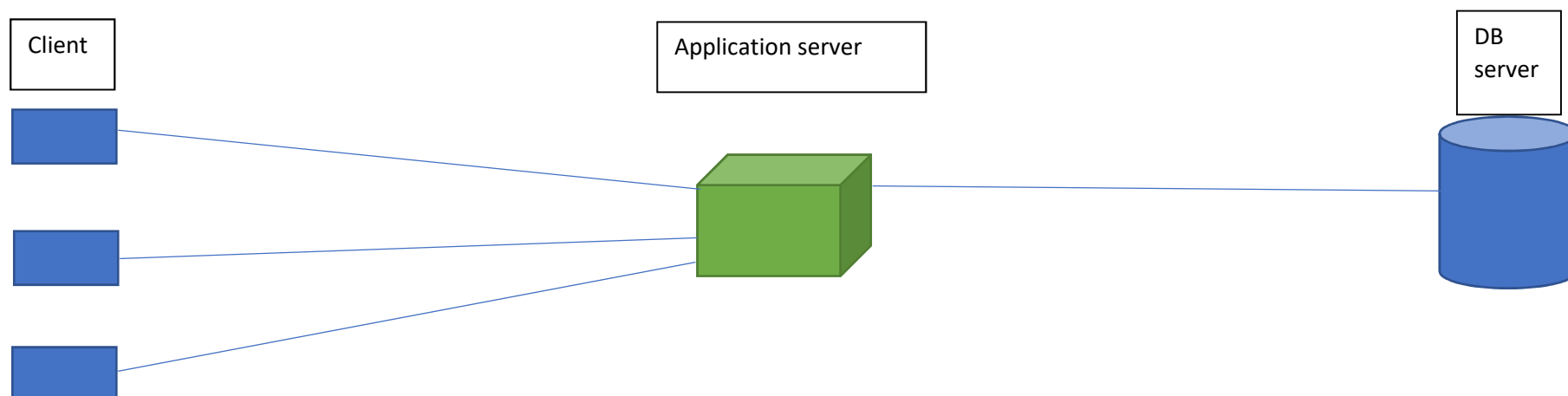
##### **Documento Aggiornamenti e Patch Sicurezza "DAPS"**

Documento che verrà mantenuto aggiornato dall'OE per tutta la durata del contratto e reso disponibile ad AsFO in qualsiasi momento per verificare lo stato di messa in produzione di aggiornamenti di sicurezza/nuove funzionalità/test.

## Documento Riepilogativo Workflow "DRW"


Parte grafica

esempio non esaustivo



Seconda parte descrittiva (esempio)

Elemento	descrizione	Ubicazione	Destinatario trasmissione	Tipologia di comunicazione	Responsabile/gestore	Note
1	Software installato su PC fornito da ASFO/OE	In Azienda sanitaria	Application server	https porta 443	OE	Requisiti minimi: versione windows, versione .NET
2	Application server	In cloud oggetto di fornitura	DB server	TCP porta 1433	OE	
3	...	...	...	...	...	...

 <p><b>AS FO</b> Azienda sanitaria Friuli Occidentale</p> <p><small>REGIONE AUTONOMA FRIULI VENEZIA GIULIA</small></p>	<p><b>Azienda sanitaria Friuli Occidentale</b></p> <p><b>Modulo B</b> <b>Modulo richiesta VPN</b></p>
---	---

### Modulo richiesta VPN

Il presente documento fa riferimento alla richiesta di collegamento tra una sede da Voi definita e AsFO per l'esecuzione di attività di:

- configurazione;
- manutenzione;

da eseguire da remoto su apparati localizzati all'interno della LAN di AsFO.

La S.C. Gestione e Innovazione Tecnologie, richiede alla Vostra Ditta di inviare il presente modulo completo in ogni sua parte al seguente indirizzo mail: **asfo.protgen@certsanita.fvg.it**

#### Dati richiedente

Il sottoscritto, .....

nato a ....., il.....

in nome dell'Azienda .....

con sede legale .....

in qualità di .....

**RICHIEDO**

una coppia di credenziali personali per poter instaurare una connessione tramite VPN con AsFO per l'esecuzione di attività di:

- configurazione;
- manutenzione;

da eseguire da remoto su apparati localizzati all'interno della infrastruttura di AsFO per il seguente personale dipendente dell'azienda sopra indicata:

Nome	Cognome	Qualifica	Numero di cellulare

Dichiaro inoltre, relativamente a obblighi di riservatezza, segretezza e sicurezza nei collegamenti da remoto

di accettare quanto segue:

1. mantenere la più assoluta riservatezza e segretezza sulle informazioni acquisite durante lo svolgimento dell'attività. Per informazioni si intendono sia le informazioni necessarie per



aprire/chiudere il collegamento remoto, sia i dati che vengono trattati durante la sessione di collegamento remoto. Accedere ai dati strettamente necessari all'espletamento dell'attività di cui è stata richiesta l'esecuzione. Ovvero a espletare l'attività nel pieno rispetto del D.lgs. 196/2003 ("Testo Unico della Privacy - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") e del Regolamento Europeo 679/2016 "GDPR" sulla protezione dei dati personali recepito con D.lgs. 101/2018 e successive modificazioni e integrazioni;

2. non divulgare in nessun modo le informazioni di cui al punto 1;
3. utilizzare il collegamento per i soli scopi ed alle condizioni definiti dal contratto di assistenza e dalla scheda di collegamento remoto e modalità di connessione relativa al collegamento (che sarà redatta congiuntamente durante l'attivazione del collegamento);
4. salvo il caso di collegamenti tramite VPN o altre soluzioni concordate con S.C. Gestione Innovazione Tecnologie, **non** utilizzare applicativi che facciano uso di protocolli di comunicazione SSL (https, ssh, ecc.) ed in generale meccanismi di crittografia che impediscano l'interpretazione dei pacchetti in transito da parte di personale incaricato AsFO;
5. nominare il proprio responsabile dei trattamenti effettuati con il collegamento remoto;
6. inviare un elenco del personale che utilizzerà la connessione messa a disposizione, precisando se dipendente interno o consulente;
7. garantire che i propri incaricati - che effettuano trattamenti con il collegamento remoto - operino nel pieno rispetto dei punti 1, 2 e 3.

#### INOLTRE PRENDO ATTO CHE:

1. tutto il traffico prodotto tramite il collegamento remoto può essere monitorato, i pacchetti di dati vengono salvati in file di log e mantenuti per tutto il tempo che la S.C. Gestione e Innovazione Tecnologie riterrà opportuno, e potrebbero in qualsiasi momento essere utilizzati per scopi statistici o di verifica delle operazioni effettuate;
2. AsFO potrà decidere in qualsiasi momento di disabilitare temporaneamente o definitivamente l'accesso, qualora ne ravvisi necessità per qualsiasi ragione.

*Il/La sottoscritto/a dichiara, ai sensi Regolamento UE 2016/679, di autorizzare il trattamento dei propri dati personali contenuti nel presente modulo, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presente dichiarazione viene resa.*

Data

...../...../.....

COGNOME e NOME

\_\_\_\_\_

FIRMA

\_\_\_\_\_

**Documento Aggiornamenti e Patch Sicurezza "DAPS"**

Data messa in produzione	Descrizione rilascio/aggiornamento	Reparto coinvolto	Date prove pre produzione (inizio e fine)	Reparto coinvolto	Referente per l'aggiornamento
-----------------------------	---------------------------------------	-------------------	---	-------------------	----------------------------------