

**ALLEGATO III – Misure di sicurezza tecniche ed organizzative
(DA COMPILARE A CURA dell'aggiudicatario)**

relativa alla Procedura aperta, ai sensi degli artt. 14 e 71 del d.lgs. 36/2023, per la fornitura quinquennale di reagenti e strumento per analisi molecolare di mutazioni e polimorfismi genetici suddivisa in 3 lotti.

Il fornitore deve garantire le seguenti misure tecniche e organizzative al fine di garantire adeguati standard di protezione dei dati personali e di sicurezza informatica.

Il fornitore è tenuto ad integrare con ulteriori misure tecniche/organizzative ovvero, in caso di impossibilità di fornire qualche misura fra quelle indicate, individuarne altre, per garantire un livello di sicurezza adeguato al rischio.

CATEGORIA	MISURA RICHIESTA
Misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento	<p>Backup con applicazione della regola 3-2-1 (n. 3 copie dei dati, su n. 2 differenti storage, di cui n. 1 off-site)</p> <p>Verifica periodica delle operazioni di ripristino</p> <p>Crittografia asimmetrica in storage con lunghezza della chiave per un minimo di 2048 bit (o crittografia di pari resistenza ad attacchi a forza bruta)</p> <p>Installazione software antivirus fornito da ASST Lariana (F-Secure)</p> <p>Installazione agenti per il monitoraggio delle performance e della disponibilità del servizio, forniti da ASST Lariana o invio di log ai server predisposti da ASST Lariana</p> <p>Installazione agenti per monitoraggio intrusioni forniti da ASST Lariana o invio di log di accesso e relativi ad eventi di sicurezza ai server predisposti da ASST Lariana</p>
Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	<p>Consegna del manuale/procedura per la gestione delle chiavi di crittografia</p> <p>Consegna del manuale/procedura per la gestione dei backup</p> <p>Consegna del manuale/procedura per la gestione del ripristino</p>
Misure di identificazione e autorizzazione dell'utente (comprese le utenze tecniche ed amministrative)	<p>Gestione di profili utenti improntati al paradigma "need to know" e al paradigma "least privileges", quindi in grado di rendere accessibili all'operatore le sole funzioni di cui ha bisogno, inibendo l'accesso alle funzioni non strettamente necessarie all'attività a cui l'operatore è preposto; gestione delle relative attività di verifica periodica dei profili esistenti.</p> <p>Blocco del profilo dopo 5 tentativi di accesso falliti</p> <p>Uso di password di lunghezza minima pari a 12 caratteri di cui almeno un numero, almeno una minuscola, almeno una maiuscola ed almeno un carattere speciale</p> <p>Cambio password obbligatorio entro 60 giorni</p> <p>Nessun utilizzo di Accounting tramite social network</p>

Misure di protezione dei dati durante la trasmissione	<p>Crittografia asimmetrica in storage con lunghezza della chiave per un minimo di 2048 bit (o crittografia di pari resistenza ad attacchi a forza bruta)</p> <p>Utilizzo del protocollo TLS</p>
Misure per garantire la registrazione degli eventi	<p>Presenza di log delle attività di amministrazione</p> <p>Presenza di log delle attività operative</p>
Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita	<p>Test di compatibilità con il sistema informativo dell'ASST Lariana: richiede, fra l'altro, la valutazione ad opera del personale della UOC SIA delle specifiche tecniche del sistema fornito e del documento progettuale.</p> <p>Consegna del kit di configurazione iniziale dei sistemi (file di setup ed istruzioni di installazione e configurazione)</p> <p>Uso di Sistema Operativo Linux o Microsoft Windows, ad esclusione di tutte le versioni per le quali non è previsto il supporto da parte del produttore e applicazione periodica degli aggiornamenti di sicurezza del Sistema Operativo rilasciati dal fornitore, per tutta la durata del contratto. In caso di versione software per le quali il produttore ha programmato la fine del supporto, il fornitore è tenuto ad aggiornare con la nuova versione del software (supportata dal produttore).</p> <p>Uso di DBMS (Database management system) completi di licenza d'uso e per i quali è garantito il supporto da parte del produttore tramite applicazione periodica degli aggiornamenti di sicurezza, per tutta la durata del contratto.</p> <p>Utilizzo di un browser adeguato in base allo stato dell'arte, supportato in aggiornamenti correttivi ed evolutivi durante tutta la durata del contratto.</p> <p>Integrazione delle utenze (utenze applicative, utenze tecniche, utenze M2M e utenze A2A) e dei dispositivi nel dominio aziendale Microsoft oppure con credenziali personali e non cedibili</p>
Misure di informatica interna e di gestione e governance della sicurezza informatica	Network Penetration Test, effettuati dal fornitore ovvero da ASST Lariana
Misure di certificazione/garanzia di processi e prodotti	<p>Web Application Penetration Test, effettuati dal fornitore ovvero da ASST Lariana</p> <p>Mobile Application Penetration Test, effettuati dal fornitore ovvero da ASST Lariana</p> <p>Certificazione Standard ISO/IEC 27001</p>
Misure per garantire la minimizzazione dei dati	<p>Trattamento dei soli dati necessari e sufficienti per il raggiungimento della finalità</p> <p>Trasmissione dei soli dati necessari al raggiungimento della finalità</p> <p>Divieto di trattare dati personali per future funzionalità, non previste dalle finalità</p>

<p>Misure per collegamento da remoto per monitoraggio allarmi</p>	<p>La comunicazione del monitor dovrà avvenire in HTTPS in outbound, quindi dall'ospedale verso l'esterno. Il sistema di monitoraggio dovrà gestire solo dati tecnici e dovrà essere configurato solo in outbound verso i server del fornitore comunicati ai Sistemi Informativi Aziendali per predisporre la configurazione sui firewall aziendali.</p> <p>Eventuali richieste di accesso VPN dovranno essere formalizzate ai Sistemi Informativi Aziendali e il fornitore dovrà utilizzare il sistema VPN 2FA in uso ad ASST Lariana sottoscrivendo apposita modulistica. Gli accessi VPN possono essere solo nominali.</p>
<p>Misure per garantire la conservazione limitata dei dati</p>	<p>Reportistica sulla durata del trattamento dei dati</p> <p>Funzionalità di cancellazione massiva rispetto alla durata del trattamento</p> <p>Garanzia della conservazione dei dati per tutta la durata del contratto, coerentemente con le finalità del trattamento</p> <p>A conclusione del contratto, consegna dell'archivio completo e del software necessario alla ricerca e visualizzazione dei dati gestiti.</p>
<p>Misure per garantire la responsabilizzazione (accountability)</p>	<p>Nomina DPO del fornitore</p> <p>Formalizzazione registri art. 30 GDPR del fornitore</p> <p>Formalizzazione soggetti autorizzativi del fornitore</p> <p>Formazione soggetti autorizzati del fornitori</p> <p>Formalizzazione della designazione dei sub-responsabili (fornitori e professionisti) ex art. 28 del GDPR</p> <p>Formalizzazione della procedura per la gestione dei diritti degli interessati</p> <p>Formalizzazione della procedura per la gestione delle violazioni di dati personali</p>