REGIONE DEL VENETO
ULSS3 SERENISSIMA

UOC Provveditorato, Economato e Logistica

INDICAZIONI DI SICUREZZA INFORMATICA PER I SISTEMI ELETTROMEDICALI

REV00 valida dal 10/06/2024

Tutti i sistemi da connettere alla rete aziendale della Azienda ULSS 3 Serenissima (AULSS3) dovranno essere messi, ove possibile, a dominio (Microsoft Windows) e tenuti aggiornati costantemente all'ultima release disponibile relativamente alle patch di sicurezza.

I sistemi dovranno essere dotati dell'antivirus (*) attualmente in uso nella AULSS3 e andranno installati e configurati su VLAN dedicata (piano di indirizzamento da concordare in fase di installazione con i Sistemi Informativi della AULSS3).

Il Sistema Operativo degli eventuali server (fisici o virtuali) dovrà essere almeno Windows Server 2019 aggiornato.

Il Sistema operativo degli eventuali PC dovrà essere almeno Windows 11 Professional aggiornato.

È necessario, inoltre, che siano eseguite da parte del fornitore le seguenti azioni relative alla sicurezza informatica:

- implementare misure di cifratura per i dati in transito e a riposo (anche su eventuali DB), specialmente per i dati sensibili o personali trattate dalle apparecchiature elettromedicali;
- utilizzare di protocolli di comunicazione sicura/cifrata (es. HTTPS, TLS, FTPS) per la trasmissione dei dati tra le apparecchiature elettromedicali e la rete della AULSS3;
- implementare, in collaborazione con i Sistemi Informativi della AULSS3, politiche di:
  - restrizione connettività (VLAN, VPN, regole firewall...)
  - gestione profilature utenti che limitino l'accesso ai dati e ai sistemi solo al personale autorizzato e ai soli dati minimi essenziali per lo svolgimento delle attività assegnate
  - backup (e verifica periodica di ripristino) dei dati applicativi/sistemistici e di eventuali DB, in linea con gli strumenti e procedure della AULSS3
  - definizione finestre manutentive da utilizzarsi per installazione di eventuali patch, aggiornamenti e/o manutenzione programmata;
- adeguare costantemente e tempestivamente i sistemi installati alla normativa vigente in ambito privacy e cybersecurity, durante tutto il periodo di garanzia;
- definire SLA di intervento, contatti e procedure per la gestione di richieste/problematiche di carattere informatico durante il periodo di garanzia.

Relativamente all'eventuale gestione amministrativa degli apparati installati, il fornitore dovrà prevedere, in collaborazione e concordando le attività con i Sistemi Informativi della AULSS3:

- *l'attivazione di account amministrativi nominali con accesso tramite strumento di amministrazione dedicato (PAM aziendale) o, in alternativa qualora non possibile, tramite sistemi di accesso da remoto controllati con autenticazione MFA;*
- *qualora necessario/previsto e/o se ritenuto opportuno da parte dell'AULSS3, l'abilitazione del monitoraggio continuo e della registrazione dei LOG di accesso ai sistemi e ai dati e/o dei LOG relativi alla gestione amministrativa dei sistemi.*

(*) Antivirus aziendale: Cynet Cybersecurity Platform (https://www.cynet.com/)