1. Použití standardů a kompatibility
* Veškeré dodávané zařízení, které ke své činnosti využívá bezdrátový přenos dat (ať už mezi vlastními komponentami, nebo mezi dodaným zařízením a systémy Krajské zdravotní), musí podporovat standard IEEE 802.11ad nebo novější.
* Všechny bezdrátové moduly, které nejsou nezbytné pro běžný provoz zařízení, musí být deaktivovány; případná opětovná aktivace je možná pouze prostřednictvím privilegovaného účtu (administrátorského přístupu). Aktivace a deaktivace musí být logovány a auditovány.
1. Řízení výkonu a frekvence
* Výkon používaných bezdrátových prvků (routery, vysílače, antény apod.) nesmí být vyšší, než je nezbytně nutné. Zařízení musí umožňovat regulaci výkonu a jeho nastavení dle provozních potřeb. Nastavený výkon podléhá schválení KZ při akceptaci.
* Preferováno je použití směrových antén (při zachování požadovaného pokrytí a funkčnosti) před všesměrovými, aby se omezilo rušení a kolize signálu.
* Upřednostňuje se pásmo 6 GHz nebo vyšší z důvodu snížení vzájemných kolizí a rušení v rámci bezdrátových kanálů.
1. Minimalizace rušení a bezpečnost ostatních aktiv
* Bezdrátová technologie se smí použít pouze tehdy, pokud není použití kabelového (drátového) připojení možné nebo provozně efektivní.
* Navržené bezdrátové řešení nesmí v žádném případě negativně ovlivňovat funkčnost a bezpečnost jiných zařízení, zejména zdravotnické techniky nebo určených ICT systémů v nemocnici.
1. Řízení přístupu a šifrování
* K bezdrátové části sítě je nutné zavést řízení přístupu v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcími vyhláškami a metodikami. Identity a nakládání s nimi musí být logovatelné.
* Veškerý provoz bezdrátových sítí musí být šifrován metodami odpovídajícími platným bezpečnostním standardům (podle aktuálního doporučení NÚKIB).
* Bezdrátová síť, s výjimkou technicky omezeného a zcela odděleného propojení PtP, musí podporovat segmentaci.
1. Soulad s požadavky kybernetické a informační bezpečnosti
* Bezdrátové sítě musí být navrženy, nasazeny a provozovány v souladu s požadavky na zajištění kybernetické a informační bezpečnosti v rozsahu důvěrnosti, integrity a dostupnosti dat (v intencích zákona o kybernetické bezpečnosti a jeho prováděcích předpisů).
* Veškeré změny či rozšiřování bezdrátových sítí je nutné podrobit interním bezpečnostním procesům organizace (např. řízení rizik a řízení změn), aby bylo zaručeno, že nově dodané komponenty neohrozí probíhající zdravotnické činnosti.
* Na bezdrátové síti musí být detekovány a logovány bezpečnostní události a incidenty.