Hospital Security Assessment Checklist

I. Physical Security Measures

☐ Are access controls (e.g., card readers, locks, security zones) in place and functioning?

☐ Is visitor management policy enforced and monitored?

☐ Are high-risk areas (ED, pharmacy, behavioral health, OB, pediatrics) appropriately secured?

☐ Are surveillance cameras strategically placed, functional, and monitored?

☐ Are security cameras on emergency power?

☐ Is exterior lighting sufficient around entrances, parking lots, and walkways?

☐ Are windows unobstructed by plants (plants no higher than 3 feet tall, tree canopy no lower than 6 feet from the ground)

☐ Are emergency exits secure and alarmed without obstructing egress?

☐ Are infant/pediatric abduction prevention systems tested regularly?

☐ Is access to hazardous materials and biomedical waste areas restricted?

II. Security Personnel & Operations

☐ Is there a primary point person responsible for security?

☐ Is there a designated committee responsible for oversight of the security program?

☐ Are patrols conducted routinely in vulnerable areas?

☐ Is there a process for staff to quickly summon security?

☐ Are incident reports reviewed and analyzed for trends?

☐ Is there a process for staff to report security incidents or incidents of violence?

III. Policies, Procedures & Training

☐ Are security-related policies (e.g., access control, visitor policy, weapons prohibition) current and enforced?

☐ Are workplace violence prevention policies in place?

☐ Is there a clear process for staff to report violence or threatening behavior?

☐ Are staff trained in workplace violence awareness and response upon hire and annually?

☐ Is there a code system (e.g., Code Gray, Code Silver) known to all staff?

☐ Are contractors, students, and vendors briefed on security procedures?

☐ Are security officers and appropriate staff adequately trained (e.g., de-escalation, restraints, trauma-informed care)?

IV. Risk Identification & Mitigation

☐ Has a formal security risk assessment been conducted within the past 1–3 years?

☐ Were findings from previous assessments addressed with corrective actions?

☐ Are security concerns included in Environment of Care (EC) risk rounds?

☐ Are behavioral threat assessments conducted for concerning individuals?

☐ Are local crime statistics incorporated in risk identification?

V. Emergency Preparedness & Response

☐ Are security roles integrated into the hospital's emergency operations plan (EOP)?

☐ Is security involved in drills for active shooter, evacuation, lockdown, etc.?

☐ Are communication protocols (e.g., overhead alerts, mass notification) tested regularly?

☐ Does security have access to and training on emergency equipment (e.g., panic buttons, radios)?

☐ Is there coordination with local law enforcement for crisis response?

VI. Staff and Patient Safety

☐ Are staff in high-risk units protected by panic alarms or other security measures?

☐ Are behavioral restraint protocols in place and reviewed?

☐ Are elopement prevention measures in place and tested?

☐ Are assaults, threats, and violent incidents tracked and reported?

☐ Are trends in workplace violence reviewed by leadership and shared with staff?

VII. Documentation & Continuous Improvement

☐ Is the security risk assessment documented and retained?

☐ Are results reported to leadership and Environment of Care Committee?

☐ Is there a plan to review and update the assessment annually or after major incidents?

☐ Are KPIs tracked (e.g., response times, incident rates, training completion)?

☐ Are lessons learned from incidents incorporated into policy and training?