

## MONTHLY PHYSICAL SECURITY VERIFICATION CHECKLIST

1. Visitor log/VMS entries are complete, accurate, and retained per policy.
2. Visitor badges are issued, worn visibly, and collected upon exit; unreturned badges are documented.
3. Escort requirements are enforced for all non-authorized individuals (no unescorted roaming).
4. Tailgating/challenge culture is enforced at controlled doors; incidents are reported.
5. Terminated employees/contractors are deprovisioned: badges disabled and keys recovered.
6. Mechanical keys are inventoried; issuance/return records are current; duplication is controlled.
7. Restricted areas (server rooms/labs/cages/network closets) have current authorized access rosters (reviewed).
8. After-hours access events are pre-approved, logged, and reviewed for anomalies.
9. Reception/waiting areas do not allow unsupervised access to endpoint USB ports (e.g., kiosk PCs, lobby workstations).
10. Unused/accessible network ports (RJ45 wall jacks/switch ports) in public or waiting areas are disabled, locked, or otherwise controlled.
11. Network closets and patch panels are secured; no exposed patch cords or unmanaged switches are accessible in common areas.
12. Public-facing printers/copiers and shared devices are positioned to prevent unauthorized access to USB ports, trays, or network cabling.

Reviewer Name: \_\_\_\_\_ Date: \_\_\_\_\_

Signature: \_\_\_\_\_