CYICU Rapid Hardening Checklist (v1)

2026-02-07

Purpose: a fast, sane baseline you can apply in hours, then iterate into maturity.

Notes: This is a general checklist. Adapt to your environment and compliance requirements.

1) Identity & Access

- Enforce MFA on admin + remote access accounts (VPN, email, cloud).
- Remove shared admin accounts; create named admins with least privilege.
- Rotate privileged credentials; store in a password manager with audit trails.
- Disable legacy auth protocols; require modern auth where supported.
- Review external access paths: RDP/SSH exposure, VPN posture, SSO apps.

2) Patch & Configuration Baselines

- Patch high-risk systems first: edge devices, VPN, public web, email.
- Update firmware for routers/switches/APs; confirm management planes are locked down.
- Harden OS baselines (CIS-style): disable unused services, tighten policies.
- Inventory what you own (hardware + SaaS). If it isn't inventoried, it isn't defended.

3) Network Segmentation (80/20)

- Separate: admin systems, user devices, guest Wi-Fi, and servers.
- Block lateral movement by default; allow only required ports between zones.
- Restrict management interfaces to an admin subnet + VPN only.

4) Logging, Detection, Response

- Centralize logs (auth, VPN, firewall, endpoint). Retain at least 30 days hot + 90 days cold if possible.
- Create alerts for: new admin creation, MFA changes, suspicious logins, config changes.
- Draft a one-page incident response playbook: who decides, who communicates, what gets preserved.

5) Backups & Recovery

- 3-2-1 backups. Test restore quarterly. Protect backups from admin compromise (separate credentials).
- Snapshot critical servers before major changes. Keep offline or immutable backups if possible.