■■ Core Four Cybersecurity Framework

A distilled, high-integrity model for securing digital infrastructure

1. Windows 11 Active Update Enforcement

Principle: Let the operating system defend itself.

Action: Ensure Windows Update is enabled and configured for automatic patching.

Scope: Includes OS kernel, drivers, Microsoft Defender, and core applications.

Rationale: Eliminates manual patching delays and ensures rapid mitigation of zero-day threats.

Verification: Use Group Policy or Intune to enforce update compliance and audit patch status.

2. Advanced Antivirus & Malware Defense

Principle: Detect, block, and respond in real time.

Action: Deploy next-gen antivirus with behavioral analysis, cloud intelligence, and EDR (Endpoint Detection & Response).

Scope: All endpoints, including workstations, laptops, and mobile devices.

Rationale: Signature-based AV is obsolete; modern threats require adaptive, AI-driven defense.

Verification: Monitor threat logs, validate update frequency, and test detection with simulated payloads.

3. Isolated & Segmented Network Architecture

Principle: Contain risk by design.

Action: Segment networks based on criticality and harden backbone services.

Scope:

- Air-gapped systems for high-risk zones (e.g., SCADA, R&D;)
- DMZs for public-facing services
- No direct routing between sensitive and public networks
- Harden Windows Servers (Domain Controllers, DNS, File Servers):
- Disable SMBv1 and enforce SMB signing
- Enable Credential Guard and LSASS protection
- Enforce GPO lockdowns for PowerShell, registry, and RDP
- Secure DNS with audit logging and role isolation

- Deploy Sysmon and integrate with SIEM

- Apply Microsoft Security Baselines (Security Compliance Toolkit)

Rationale: Prevent lateral movement, data leakage, and remote exploitation. Hardened infrastructure blocks escalation within segments.

Verification: Conduct network mapping, firewall rule audits, penetration testing, and server baseline scans.

4. Strict Employee Access Control

Principle: Trust no one by default.

Action: Enforce least privilege, role-based access, and session monitoring.

Scope:

- No shared accounts

- No local admin rights unless justified

- Disable USB and external media where unnecessary

Rationale: Human error and insider threats are primary breach vectors.

Verification: Audit access logs, review privilege escalations, and rotate credentials regularly.

This framework is lean, enforceable, and grounded in operational reality — not compliance theater.