Windows Security Hardening Checklist

Summary
This checklist is designed for enterprise IT teams.

Baseline
* Apply CIS or Microsoft Security Baseline
* Enable BitLocker with recovery escrow
* Enforce MFA for admin accounts

Endpoint Protection
* Enable Defender AV and cloud protection
* Configure ASR rules
* Enable controlled folder access

Identity & Access
* Disable local admin accounts
* Enforce strong password policies
* Review privileged group memberships

Network
* Enable firewall profiles
* Disable legacy protocols (SMBv1)
* Ensure VPN and DNS security settings

Logging
* Enable audit policies for logon and privilege use
* Forward logs to SIEM