

System Hardening Checklist

Prepared By: Muneer Shaukath

Department: IT

Review Date:

Version: 1.0

Reference

Reference: ISO/IEC 27001:2022 Clause 8 Operational Planning and Control, Control A.8.9 – Configuration Management

#	Item/Control Point	Windows Servers / Endpoints	Linux Servers	Network Devices	Status (Y/N)	Remarks / Evidence
1	Baseline configurations defined and documented	☐	☐	☐		
2	Remove/disable unnecessary services & applications	☐	☐	☐		
3	Default accounts removed/disabled/renamed	☐	☐	☐		
4	Default passwords changed	☐	☐	☐		
5	Security patches applied and up to date	☐	☐	☐		
6	Unnecessary ports closed	☐	☐	☐		
7	Strong authentication configured (e.g., MFA)	☐	☐	☐		
8	Admin/root access restricted and monitored	☐	☐	☐		
9	Remote access securely configured (VPN, SSH, RDP)	☐	☐	☐		
10	Firewall rules reviewed and implemented	☐	☐	☐		
11	Antivirus/antimalware installed and active	☐	☐	☐		
12	Audit and logging enabled and retained	☐	☐	☐		
13	File and folder permissions reviewed	☐	☐	☐		
14	Backups tested and protected	☐	☐	☐		



15	Configuration changes tracked/version controlled	☐	☐	☐		
16	System hardening standards reviewed annually	☐	☐	☐		

For Office Use Only:

Approved By: Sherry George	
Designation: Technical Director	
Reviewed By: Rixon Thomas	
Designation: Sr. Infrastructure Engineer	
Signature Of Approver:	Date:

--End of Document--