ACE Networks

Cybersecurity Audit Preparation Checklist

30-Point Checklist for Cyprus SMEs

1. Document your Information Security Policy
2. Define roles and responsibilities for cybersecurity
3. Maintain an Acceptable Use Policy for employees
4. Implement a Password Management Policy
5. Set up Multi-Factor Authentication for critical systems
6. Create a Data Retention and Destruction Policy
7. Establish a Remote Work/BYOD Policy
8. Ensure your Firewall is properly configured and updated
9. Deploy endpoint protection on all workstations and laptops
10. Encrypt sensitive data at rest and in transit
11. Run regular vulnerability scans on your network
12. Apply all security patches within 30 days of release
13. Maintain an asset inventory with current device statuses
14. Backup critical data daily and test restore procedures monthly
15. Store backups securely off-site or in the cloud
16. Set up email filtering to block phishing attempts
17. Conduct quarterly phishing simulation exercises
18. Train staff on basic cybersecurity hygiene annually
19. Implement access controls based on job roles
20. Log and monitor user activity across critical systems
21. Review and audit privileged user accounts regularly
22. Test your incident response plan at least once per year
23. Document incident handling procedures and contacts
24. Log security events and monitor for anomalies
25. Update antivirus and anti-malware signatures daily

26. Restrict admin access to only necessary users

27. Maintain security awareness posters or reminders in the workplace

28. Restrict USB and external device access

29. Evaluate your vendors' cybersecurity posture

30. Schedule an internal pre-audit or third-party assessment