Native Innovation Inc.

24-Point IT Health Checklist

Safeguarding Technology • Strengthening Security • Supporting Innovation

1. Verify regular system backups are occurring and tested for recovery.
2. Confirm antivirus and antimalware software is installed and updated.
3. Ensure operating systems are patched with the latest security updates.
4. Review firewall configurations and access control lists.
5. Test disaster recovery plan and ensure documentation is up to date.
6. Check password policies meet best practices (length, complexity, expiration).
7. Enable multi-factor authentication (MFA) for all critical systems.
8. Audit user accounts for inactivity and unnecessary privileges.
9. Verify secure remote access (VPN, encryption, MFA).
10. Review physical security controls (locks, access cards, cameras).
11. Confirm email filtering and spam protection are effective.
12. Test data encryption at rest and in transit.
13. Ensure compliance with relevant regulations (HIPAA, PCI-DSS, etc.).
14. Check patch management for third-party applications.
15. Test network vulnerability scans and penetration testing results.
16. Confirm logging and monitoring are enabled and reviewed.
17. Review incident response plan and conduct tabletop exercises.
18. Verify secure configurations of servers, routers, and switches.
19. Confirm endpoint detection and response (EDR) solutions are deployed.
20. Check cloud service security settings and shared responsibility compliance.
21. Audit software licenses and remove unauthorized applications.
22. Review wireless network security (WPA3, guest network isolation).
23. Assess employee cybersecurity awareness training completion.
24. Document and remediate any identified risks or vulnerabilities.