CodeBlue technology

MANAGED IT CHECKLIST

Best Practices for Business

Managed IT Security Best Practices Checklist

1. **Conduct Regular Security Audits**

☐Assess current security measures and identify vulnerabilities.

2. **Implement Strong Password Policies**

☐ Require complex passwords and regular changes.

3. **Enable Multi-Factor Authentication (MFA)**

☐ Add an extra layer of security beyond passwords.

4. **Regularly Update and Patch Systems**

☐ Ensure all software and systems are up-to-date with the latest patches.

5. **Develop and Maintain a Disaster Recovery Plan**
☐ Outline procedures for data recovery in case of a security breach or disaster.

6. **Conduct Regular Backup of Data**
☐ Schedule automatic backups and test restore procedures regularly.

7. **Secure Cloud Services**
☐ Implement encryption and access controls for cloud-stored data.

8. **Train Employees on Cyber Security**
☐ Conduct regular training sessions on identifying phishing attempts and best security practices.

9. **Implement Network Security Measures**
☐ Use firewalls, intrusion detection/prevention systems, and secure Wi-Fi.

10. **Monitor and Manage User Access**
☐ Regularly review and adjust user permissions based on roles and responsibilities.

11. **Install and Maintain Anti-Malware Software**
☐ Ensure all systems have updated anti-malware protection.

12. **Develop an Incident Response Plan**
☐ Establish clear protocols for responding to security incidents.

13. **Secure Mobile Devices**
☐ Implement mobile device management (MDM) and ensure all devices are encrypted.

14. **Regularly Test Security Systems**
☐ Conduct penetration testing and vulnerability assessments.

15. **Implement Data Encryption**
☐ Encrypt sensitive data both in transit and at rest.

16. **Monitor IT Infrastructure**
☐ Use security information and event management (SIEM) tools to monitor for suspicious activity.

17. **Secure Remote Access**
☐ Use VPNs and ensure remote connections are secure.

18. **Establish a Clear BYOD Policy**
☐ Define security requirements for employee-owned devices used for work.

19. **Manage Third-Party Risks**
☐ Assess and monitor the security practices of vendors and partners.

20. **Document and Review Policies Regularly**
☐ Keep security policies and procedures up-to-date and review them periodically.

21. **Implement Role-Based Access Control (RBAC)**
☐ Assign access permissions based on user roles to minimize the risk of unauthorized access.

22. **Perform Regular Network Penetration Tests**
☐ Simulate cyber attacks to identify and fix vulnerabilities.

23. **Monitor Dark Web for Compromised Credentials**
☐ Keep track of potential breaches involving company data on the dark web.

24. **Create a Culture of Security Awareness**
☐ Promote a culture where security is a shared responsibility among all employees.

25. **Utilize Endpoint Detection and Response (EDR) Solutions**
☐ Deploy EDR tools to detect and respond to threats on endpoints in real-time.

IT Services Data Center Premise Security Cabling Voice Services

CodeBlue Technology supports businesses in all industries, sizes and locations around the United States. Our mission is to delivery positively memorable technical service while improving your businesses health in the data landscape.

Our team of solutions engineers, networking technicians and business professionals are here to guide, coach and implement a strategy that best suits your needs. If you or any member of your team would like a free consultation, please consider CodeBlue Technology for all of your IT needs.

You can visit us around the web **@CodeBlueTech**
Or **(804) 521-7660**

Contact Sales today at **Sales@codebluetechnology.com**