Cybersecurity Checklist for SMBs & Government Agencies

1. Risk Assessment & Governance

- [ ] Conduct a yearly cybersecurity risk assessment to identify vulnerabilities.
- [ ] Maintain an up-to-date inventory of all hardware, software, and data assets.
- [ ] Establish a formal cybersecurity policy approved by leadership.
- [ ] Designate a cybersecurity officer or team responsible for oversight.

2. Access Control

- [ ] Enforce strong password policies (e.g., 12+ characters, no defaults like "admin").
- [ ] Enable multi-factor authentication (MFA) for all user accounts.
- [ ] Implement role-based access control (RBAC) to limit privileges.
- [ ] Review and revoke access for former employees/contractors immediately.

3. Network Security

- [ ] Deploy a firewall to monitor inbound/outbound traffic.
- [ ] Segment networks to isolate sensitive data (e.g., finance, citizen records).
- [ ] Encrypt Wi-Fi networks and disable unused ports/protocols.
- [ ] Regularly update firmware on routers, switches, and IoT devices.

4. Data Protection

- [ ] Encrypt sensitive data at rest and in transit (e.g., AES-256, TLS 1.3).
- [ ] Classify data by sensitivity (e.g., public, internal, confidential).
- [ ] Establish a secure data disposal process for outdated hardware/files.
- [ ] Backup critical data daily and store copies offline or in secure cloud storage.

5. Incident Response

- [ ] Develop an incident response plan with roles, escalation paths, and communication steps.
- [ ] Test the plan with annual drills or tabletop exercises.
- [ ] Maintain a list of contacts for law enforcement, legal, and cybersecurity firms.
- [ ] Monitor systems 24/7 for anomalies using SIEM tools or managed services.

6. Employee Training

- [ ] Conduct mandatory cybersecurity training quarterly.
- [ ] Run simulated phishing campaigns to test awareness.
- [ ] Teach employees to recognize social engineering (e.g., fake invoices, urgent requests).
- [ ] Create a reporting process for suspicious activity (e.g., phishing emails).

7. Vendor & Supply Chain Security

- [ ] Assess third-party vendors for cybersecurity compliance.
- [ ] Include cybersecurity requirements in vendor contracts (e.g., SOC 2, ISO 27001).
- [ ] Restrict vendor access to only necessary systems/data.

8. Physical Security

- [ ] Secure server rooms and offices with keycards/biometrics.
- [ ] Install surveillance cameras and alarm systems.
- [ ] Require employees to lock devices when unattended.
- [ ] Destroy physical documents containing sensitive data.

9. Compliance & Audits

- [ ] Align with regulations (e.g., NIST CSF, GDPR, HIPAA, CMMC, FISMA).
- [ ] Perform penetration testing annually.
- [ ] Document all cybersecurity measures for audit trails.

10. Continuous Improvement

- [ ] Patch software and OS within 30 days of updates.
- [ ] Review and update policies biannually.
- [ ] Subscribe to threat intelligence feeds (e.g., CISA alerts).

Quick Start for Immediate Actions

1. Enable MFA on all accounts.
2. Update all software and operating systems.
3. Backup critical data and test restoration.
4. Train employees on phishing risks.

Disclaimer: This checklist is a foundational guide. Tailor it to your organization's needs and consult cybersecurity professionals for advanced threats.