Zero Trust Implementation Checklist for Small Businesses

Foundation Phase

- [ ] Complete security assessment to identify critical assets and vulnerabilities
- [ ] Inventory all devices accessing your network (company-owned and personal)
- [ ] Document all user accounts and their current access levels
- [ ] Map data flows to understand how information moves through your organization
- [ ] Review current security tools and capabilities

Identity & Access Management

- [ ] Implement Multi-Factor Authentication (MFA) for all accounts
- [ ] Enforce strong password policies (length, complexity, no reuse)
- [ ] Deploy password management solution for your team
- [ ] Remove shared/generic accounts where possible
- [ ] Implement Just-In-Time (JIT) access for administrative accounts
- [ ] Create role-based access control (RBAC) framework
- [ ] Document procedures for access requests and approvals

Network Security

- [ ] Segment network based on function (admin, user, guest)
- [ ] Implement separate Wi-Fi networks for business and guests
- [ ] Configure firewalls to default-deny unauthorized traffic
- [ ] Enable logging for network devices
- [ ] Review and update firewall rules quarterly

[ ] Implement secure remote access solutions (VPN, etc.)

[ ] Deploy network monitoring solution

Device Security

[ ] Install and configure endpoint protection on all devices

[ ] Implement device encryption for laptops and mobile devices

[ ] Create standard configuration templates for company devices

[ ] Establish patch management procedures

[ ] Implement device health verification before network access

[ ] Create procedures for lost/stolen device handling

[ ] Develop and enforce BYOD policies if applicable

Data Protection

[ ] Classify data based on sensitivity (public, internal, confidential)

[ ] Implement appropriate controls for each data classification

[ ] Deploy backup solutions with appropriate retention policies

[ ] Test data recovery procedures regularly

[ ] Implement encryption for data in transit and at rest

[ ] Review and limit data access permissions

[ ] Document data retention and destruction policies

Cloud Security

[ ] Enable security features in cloud services (Microsoft 365, Google Workspace, etc.)

[ ] Configure conditional access policies based on user, location, device

[ ] Review default permissions in cloud storage

[ ] Enable logging and monitoring for cloud services

[ ] Implement cloud backup solution

[ ] Regularly review third-party app integrations and permissions

Security Monitoring

- [ ] Configure alerts for suspicious activities
- [ ] Establish regular review schedule for security logs
- [ ] Document incident response procedures
- [ ] Define escalation paths for security incidents
- [ ] Set up automated reporting of security metrics
- [ ] Test incident response plan quarterly
- [ ] Review and update security monitoring as needed

Policies & Training

- [ ] Develop and document security policies
- [ ] Conduct regular security awareness training for all employees
- [ ] Implement phishing simulation and testing
- [ ] Create specific security training for IT staff
- [ ] Document acceptable use policies
- [ ] Establish vendor security assessment procedures
- [ ] Implement security policies for third-party access

Ongoing Management

- [ ] Schedule regular security assessments (quarterly)
- [ ] Review and update access permissions when staff roles change
- [ ] Conduct periodic compliance reviews
- [ ] Evaluate and update security tools annually
- [ ] Test disaster recovery procedures regularly
- [ ] Maintain documentation of security architecture
- [ ] Budget for security improvements in annual IT planning

Advanced Implementations (As Resources Allow)

[ ] Deploy Security Information and Event Management (SIEM) solution

[ ] Implement micro-segmentation of network

[ ] Deploy advanced threat protection tools

[ ] Consider managed detection and response services

[ ] Implement comprehensive data loss prevention

[ ] Develop advanced automation for security responses

[ ] Conduct regular penetration testing

Implementation Notes:

- Prioritize actions based on your risk assessment results
- Focus first on protecting your most critical assets and data
- Document progress and maintain evidence of implementation
- Review and update this checklist as your security program matures

This checklist was developed by RZR Solutions to help small businesses implement Zero Trust security principles in a practical, budget-conscious manner. Contact us at 972-904-1559 or visit rzrsolutions.com for personalized guidance.