AI Readiness Checklist

Microsoft Copilot Implementation Guide

Company: _____ Date: _____

Completed by: _____

Phase 1: Pre-Implementation Planning

- [ ] Identify executive sponsor and project stakeholders
- [ ] Define business objectives and success metrics for AI implementation
- [ ] Review Microsoft 365 licensing and Copilot subscription requirements
- [ ] Allocate budget for licensing, training, and security measures
- [ ] Identify specific use cases where Copilot will enhance productivity
- [ ] Establish project timeline with key milestones

Phase 2: Technical Prerequisites & Environment Assessment

- [ ] Verify Microsoft 365 environment meets Copilot technical requirements
- [ ] Review current data classification and sensitivity labels
- [ ] Audit existing SharePoint, OneDrive, and Exchange permissions
- [ ] Document current information architecture and data repositories
- [ ] Assess integration with existing security tools (SIEM, DLP, EDR)
- [ ] Verify backup and recovery procedures for AI-accessible data

Phase 3: Data Security & Access Controls

- [ ] Conduct comprehensive data security assessment with STACK Cybersecurity
- [ ] Implement or verify data classification scheme (public, internal, confidential, restricted)
- [ ] Review and update information protection policies
- [ ] Configure role-based access controls for Copilot users
- [ ] Establish privileged user protocols for administrators
- [ ] Define and enforce least-privilege access principles
- [ ] Review third-party and guest access policies
- [ ] Enable multi-factor authentication for all Copilot users

Phase 4: Compliance & Regulatory Requirements

Note: Compliance requirements vary by industry. Review applicable regulations with legal counsel and compliance officers.

- [ ] Document compliance requirements (CMMC, HIPAA, FTC Safeguards, GDPR, etc.)
- [ ] Verify AI usage aligns with data privacy regulations
- [ ] Review data retention and deletion requirements
- [ ] Assess cross-border data transfer implications
- [ ] Establish procedures for data subject access requests

For Defense Contractors (CMMC):

- [ ] Verify Copilot configuration meets CUI protection requirements
- [ ] Document AI tool usage in System Security Plan (SSP)

For Healthcare Entities (HIPAA):

- [ ] Execute Business Associate Agreement with Microsoft
- [ ] Restrict Copilot access to Protected Health Information (PHI)

For Financial Services (FTC Safeguards):

- [ ] Document AI usage in Information Security Program
- [ ] Ensure encryption requirements for customer information

Phase 5: Policy Development & Governance

- [ ] Develop AI Acceptable Use Policy
- [ ] Create data governance framework for AI tools
- [ ] Establish AI ethics guidelines and responsible use principles
- [ ] Define prohibited use cases and sensitive data handling procedures
- [ ] Document data quality standards for AI-accessible information
- [ ] Establish change management process for AI policy updates

Phase 6: User Training & Awareness

- [ ] Develop targeted training program for Copilot functionality
- [ ] Create security awareness training specific to AI tools
- [ ] Provide data privacy and responsible AI usage training
- [ ] Educate users on prompt engineering and effective AI interaction
- [ ] Train users to recognize AI-generated errors or hallucinations
- [ ] Conduct role-specific training for different user groups
- [ ] Establish ongoing training schedule and refresher courses
- [ ] Create quick reference guides and support resources

Phase 7: Monitoring & Auditing

- [ ] Implement monitoring solution with STACK Cybersecurity
- [ ] Enable Microsoft Purview audit logging for Copilot activities
- [ ] Configure alerts for suspicious or anomalous AI usage patterns
- [ ] Establish baseline metrics for normal Copilot usage
- [ ] Create regular reporting schedule for AI usage and performance
- [ ] Review audit trails for data access and sharing patterns
- [ ] Monitor for potential data leakage or compliance violations

Phase 8: Incident Response & Risk Management

- [ ] Update incident response plan to include AI-specific scenarios
- [ ] Define procedures for AI-related data breaches or exposure
- [ ] Establish breach notification protocols for AI incidents
- [ ] Document escalation procedures for AI security concerns
- [ ] Conduct tabletop exercises for AI-related security scenarios
- [ ] Maintain contact list for incident response team members

Phase 9: Ongoing Maintenance & Review

- [ ] Schedule quarterly security assessments of AI implementation
- [ ] Review and update AI policies annually or when regulations change
- [ ] Conduct annual user access reviews for Copilot permissions
- [ ] Monitor Microsoft updates and new Copilot features for security implications
- [ ] Gather user feedback and assess productivity improvements
- [ ] Review and optimize Copilot license allocation based on usage patterns
- [ ] Stay informed on emerging AI threats and best practices

Need Expert Assistance?

STACK Cybersecurity provides comprehensive support for AI readiness assessments, security implementation, compliance guidance, and ongoing monitoring.

Contact Us Today

Email: digital@stackcyber.com | Phone: (734) 744-5300

33131 Schoolcraft Rd, Livonia, MI 48150

STACK Cybersecurity - Your Premier Partner in Digital Defense

SOC 2 Type II Certified | CMMC Registered Provider Organization