# Tyler Shobe, CISSP

Cincinnati, Ohio | tylershobe24@gmail.com | 419-302-3497

## Professional Summary

Hands-on Microsoft infrastructure and security engineer with 7+ years in Azure, Microsoft 365, and identity. Started in operations for a 500-person, five-branch company, then built a federal contractor's IT department and GCC High environment from nothing. Strength is owning the full lifecycle: writing the roadmap, doing the engineering, leading the team, and standing behind the result in an audit. Results include a zero-nonconformity ISO 27001 recertification, 109 of 110 NIST SP 800-171 controls met in a C3PAO-led CMMC Level 2 mock assessment, and a Microsoft Secure Score raised from 45% to 83%.

## Core Competencies

Azure Cloud Infrastructure • Microsoft 365 GCC High • Entra ID / Active Directory • Identity and Access Management
Zero Trust Architecture • Conditional Access and PIM • Intune and Autopilot • PowerShell Automation • Power Platform
Exchange Online • Email Security • Tenant Migrations • VMware • Microsoft Sentinel • Vulnerability Management
Incident Response • Endpoint Hardening • Disaster Recovery • Change Management • Compliance • Networking

## Technical Skills

| | |
|---|---|
| **Identity and Access** | **Entra ID**, **Active Directory**, Entra Connect, ADFS, Conditional Access, PIM, SAML SSO, Cisco Duo, FIDO2, LAPS, Adaxes |
| **Azure and Infrastructure** | **Microsoft Azure** (GCC High), **VMware**, Azure VMs, Load Balancer, Bastion, Key Vault, Azure Update Manager, AWS, Windows Server, Windows 11, SQL Server, SSRS |
| **Microsoft 365** | Exchange Online, SharePoint Online, OneDrive, Teams, Purview, Defender for Office 365, AvePoint Backup, GoDaddy Microsoft 365 |
| **Endpoint Management** | **Intune**, Autopilot, BitLocker, App Control for Business (WDAC), Windows Firewall, WSUS, Microsoft Deployment Toolkit, PDQ Deploy, PDQ Inventory, Meraki MDM, patch management |
| **Automation** | **PowerShell**, Microsoft Graph, Power Automate, Power Apps, Azure Logic Apps, Power BI |
| **Security and Monitoring** | Microsoft Sentinel, Log Analytics, Graylog, Defender for Endpoint, DISA STIGs |
| **Networking** | FortiGate, FortiClient ZTNA, Ubiquiti UniFi, VLAN segmentation, VPN, WPA3, DMARC/DKIM/SPF |
| **Service Management** | Jira, Confluence, Zendesk, Spiceworks, Salesforce, custom Power Platform ticketing, ITIL 4 |
| **Frameworks** | NIST SP 800-171, NIST SP 800-61, NIST SP 800-63B, CMMC, DFARS, ISO 27001, ISO 27017 |

## Experience

### Total Systems Technology Corporation | Arlington, Virginia (Remote) — 2022 – Present

*Microsoft 365 Technical Lead*

#### Identity and Access Management

- Architected a zero-trust authentication model with Microsoft Conditional Access, Duo MFA, and ADFS.
- Automated identity lifecycle with PowerShell and Microsoft Graph: provisioning, licensing, and offboarding.
- Implemented a PIM program that reduced privileged accounts and limited admin rights to least privilege.
- Designed break-glass accounts with FIDO2 keys, split-knowledge storage, and documented rotation testing.
- Aligned password policy to NIST SP 800-63B, increasing minimum length and eliminating password expirations.

#### Cloud and Infrastructure

- Executed two tenant migrations, O365 to GCC and then GCC to GCC High, covering 50+ mailboxes and 2TB+ data.
- Engineered Azure infrastructure including domain controllers, Entra Connect, web app proxies, Bastion, and Key Vaults.
- Provisioned and managed 5+ Azure VMs with load balancers, Key Vault, and Azure Update Manager patching.
- Hardened email with Defender for Office 365 Safe Links, anti-phishing, DMARC, DKIM, SPF, and mail flow rules.
- Improved sensitivity labeling by consolidating 13+ sensitivity labels into a streamlined sensitivity labeling taxonomy.
- Segmented the office network into staff, guest, camera, and management VLANs with WPA3 authentication.

### Endpoint Management

- Managed 75+ endpoints with Intune, Defender for Endpoint, FIPS-validated BitLocker, and Autopilot.
- Rolled out DISA STIGs to 100% of Windows 11 endpoints in pilot, test, and production rings, holding 90%+ compliance.
- Deployed App Control for Business (WDAC) via Intune with publisher-based allowlisting for ~270 cataloged applications.
- Directed a full reimaging of the Windows 11 fleet, enforcing baseline compliance and removing unapproved software.

### Operations and Security Response

- Built the IT department from scratch in 2022, leading a three-person service desk resolving 400+ tickets annually.
- Project-managed, architected, and engineered the org-wide service desk on SharePoint, Power Automate, and Power BI.
- Established change management with CAB review and security impact analysis, handling 74 requests in FY2025–2026.
- Deployed Microsoft Sentinel SIEM integrating Cisco Duo, Intune, Entra ID, and Log Analytics workspaces.
- Raised Microsoft Secure Score ~45% to 83% by building and leading a vulnerability management program.
- Eliminated WMI persistence vectors, deprecated Python and Git installs, and expired SSL certificates across the fleet.
- Authored the NIST SP 800-61 incident response program, ran tabletop exercises, and led response to multiple incidents.
- Instituted a monthly review calendar covering access log reviews, data ingestion checks, and backup recovery tests.

### Compliance and Client Delivery

- Led the technical portion of ISO 27001 recertification: zero nonconformities, change management cited as best practice.
- Led the company through a C3PAO mock assessment for CMMC Level 2, meeting 109 of 110 NIST SP 800-171 controls.
- Completed a CMMC pre-assessment with an outside expert, remediating findings through structured change requests.
- Authored all 110 NIST SP 800-171 SSP implementation statements plus the CUI data flow and system boundary diagrams.
- Produced Azure, M365, hardware, and third-party configuration baselines backed by 1,000+ screenshots of evidence.
- Built Power Apps, Power Automate, and SharePoint solutions for TSA and USCG, including a ~$500K JWICS cost tracker.

## **Silco Fire and Security** | Cincinnati, Ohio **2019 – 2022**

*System Administrator*

- Rose through multiple roles to lead on-premises infrastructure for a 5-branch regional organization of ~500 employees.
- Ran 3 VMware hosts and 50+ Windows servers supporting ~300 laptops and ~400 iPads across 5 branches.
- Implemented a full-mesh FortiGate VPN connecting all 5 branches and wrote every firewall rule behind it.
- Researched, built, and deployed FortiClient ZTNA company-wide, enforcing device compliance before connectivity.
- Automated identity lifecycle in Adaxes, shifting onboarding and offboarding to HR through a self-service web portal.
- Configured SAML single sign-on for 5+ business applications with Azure AD as the identity provider.
- Designed an attribute-based access control model governing content on the SharePoint intranet.
- Deployed LAPS across the Windows fleet, giving every machine a unique, rotating local administrator password.
- Stood up Cisco Meraki MDM for ~400 iPads, enrolling the devices and building their configuration profiles.
- Imaged laptops with MDT, then pushed group-specific software and updates through PDQ Deploy and PDQ Inventory.
- Restored company operations in two days after a major ransomware attack as part of the IT recovery team.
- Administered Microsoft 365 and Azure AD identity, including Exchange Online, SharePoint Online, OneDrive, and Teams.
- Migrated on-premises file shares to SharePoint Online and deployed OneDrive with automated backup and sync policies.
- Automated nearly 30 business processes using Power Automate and Azure Logic Apps to simplify repetitive office tasks.

# Education and Certifications

### Certifications

CISSP, CompTIA Security+, ITIL 4 MSF, ITIL 4 Foundation, AZ-900, PL-900, DP-900

### Master of Business Administration (MBA)

*Northern Kentucky University* | Expected graduation in 2028

### BS, Business Management, IT Concentration

*Cincinnati Christian University* | 3.96 Cumulative Grade Point Average | Valedictorian