IOT Identity & Access Management Team - 2022

Who We Are:

An 8-member team that supports and maintains identity and access service technology infrastructure for all supported State agencies as well as their business partners and constituents.

Our Mission:

The IOT Enterprise Identity Services team works to provide enterprise grade authentication and access control needs to all State of Indiana supported Agencies and where applicable business partners and customers. Nearly every service or modern business process integrates with our Active Directory based infrastructure offerings. Therefore, we strive to increase productivity across platforms through modern SSO opportunities yet keep data and identities secure and highly available.

Located:

IGCN – 5th Floor. Department: 493006

Manager:

Patrick Evans

What We Do:

Manage Active Directory (AD) domain services for the organization, which is the backbone for authentication and name resolution (DNS). The AD team is responsible for design, implementation, security hardening, disaster planning, recovery, management and troubleshooting of Active Directory infrastructure issues. In addition to Active Directory, we also maintain Azure Active Directory for use with Azure AD integrated applications including Office 365 as well as ADFS, MFA, Azure AD B2B and B2C services.

Our Products:

Microsoft Active Directory, Microsoft Active Directory Federation Services, Microsoft Azure Active Directory, Microsoft Azure Active Directory B2B, Microsoft Azure Active Directory B2C, Microsoft AD Connect, Microsoft MFA Server, Microsoft Identity Management Server

Our Tools:

ASM Ticket Management and SLA Measurement

Our Metrics:

Resolve customer issues within 2 IOT business days 90%+ G; 87%+ Y; <87% R

Mon-Fri 6am-6pm excluding state holidays

Our Customers:

39,000+ state employees and contractors, 5000+ Service and resource accounts, 6000 Guest business partner accounts and 500000 constituent B2C accounts.

Our Budget:

Please see Seat

Major Accomplishments:

- With CTO team, and in accordance with the Gartner Maturity Assessment, developed Enterprise Identity Strategic plan to mature IOT, outlining our current state and desired future state. The goal in developing an IAM Strategy

document is that all agencies can consume, and respective IOT/agency teams can build technical roadmaps for the future.

- Increased Identity team in size from four staff members to eight, including two new intermediate positions to balance the structure of the team.
- As required by Microsoft, provided remediation from Two-way SMS, and migrated users to remaining authentication methods, including Microsoft Authenticator app and Phone call.

Current Projects:

- Replacement of our current Azure AD Connect infrastructure. This is to remediate issues faced within the current AD Connect environment and provide for more flexibility as our footprint continues to expand.
- Migration of end users/applications/infrastructure from current on-premises MFA environment (Azure MFA Server) to one hosted in the cloud (Azure AD MFA). This will modernize the state's MFA and provide for a more secure environment.