User Story 3 – Secure Identity & External Access Strategy

As a Security Architect, the goal is to design a secure access model that allows both internal employees and external partners to use the system without exposing Dynamics 365 directly.

Internal users such as support agents and managers authenticate using Azure Active Directory. This ensures centralized identity management and consistent access control across the organization. External users, including partners or customers accessing portals, are authenticated using Azure AD B2C, which is designed for secure external access scenarios.

Authentication and authorization are handled as separate concerns. Authentication confirms who the user is, while authorization controls what the user is allowed to do once access is granted. Role-based access control is used to assign permissions based on user responsibilities.

User roles are mapped using Azure AD groups. For example, support agents can create and update service cases, managers can view reports and handle escalations, and external partners are limited to viewing only the data relevant to them.

Access to services is managed using secure, token-based authentication through OAuth 2.0. Short-lived access tokens are used to reduce the risk of misuse and to avoid direct access to backend systems.

Potential security risks include token exposure and excessive permissions. These risks are addressed by applying least-privilege access, using conditional access policies, limiting token lifetimes, and performing regular access reviews.