Customer Portal Application - Microsoft Graph Integration

Project Overview

This document outlines the integration plan for our Customer Portal application with Microsoft Graph API to enable seamless access to customer data, calendar management, and email communications.

Application Information

Source Application: CustomerPortal v2.1
Target Application: Microsoft Graph API
Connection Type: REST API Integration via OAuth 2.0
Classification: Business Critical

Required Microsoft Graph Permissions

Critical Risk Permissions:
• User.ReadWrite.All - Full access to user profiles for customer management
• Directory.ReadWrite.All - Modify organizational directory for customer onboarding
• Application.ReadWrite.All - Manage application configurations and settings

High Risk Permissions:
• Mail.ReadWrite - Access customer email communications
• Calendars.ReadWrite - Manage customer meeting schedules
• Contacts.ReadWrite - Synchronize customer contact information
• Files.ReadWrite.All - Access customer documents and files

Medium Risk Permissions:
• User.Read.All - Read customer profile information
• Directory.Read.All - Access organizational structure
• Mail.Read - Monitor customer email interactions

Low Risk Permissions:
• User.Read - Basic user profile access
• profile - Standard OpenID Connect profile
• openid - OpenID Connect authentication
• email - Email address for identification

Data Flow Description

The Customer Portal application will establish bidirectional data flows with Microsoft 365 services:
• **Customer Data Synchronization:** Real-time sync of customer profiles, preferences, and interaction history
• **Communication Management:** Integration with Outlook for email tracking and calendar management
• **Document Access:** SharePoint integration for customer document storage and retrieval

Security and Compliance

This integration implements enterprise-grade security measures:
• **Encryption:** TLS 1.3 for all data in transit

- **Authentication:** OAuth 2.0 with PKCE for secure authorization
- **Compliance:** GDPR and SOX compliance requirements
- **Access Control:** Role-based permissions and conditional access policies
- **Audit Logging:** Comprehensive logging of all data access and modifications

Risk Assessment Requirements

Due to the extensive permissions required for this integration, a comprehensive risk assessment is mandatory. The application will access sensitive customer data, organizational directory information, and communication channels. Regular security reviews and permission audits are required to maintain compliance.