Enterprise Customer Portal

Azure Application Registration Project Plan

Project Name	Enterprise Customer Portal
Version	2.1.0
Date	August 10, 2025
Author	IT Security Team
Classification	Internal Use
Review Status	Pending Security Assessment

Executive Summary

The Enterprise Customer Portal is a comprehensive web application designed to provide secure access to customer data, financial records, and administrative functions. This application requires extensive Azure Active Directory permissions to integrate with Microsoft Graph API and provide seamless user experience across the organization.

Project Objectives

• Provide secure customer data access with role-based permissions

• Implement comprehensive audit logging for compliance requirements

• Enable administrative functions for user and group management

• Integrate with existing directory services and applications

• Ensure GDPR and SOX compliance for financial data handling

• Support multi-factor authentication and conditional access policies

Technical Architecture

The application is built using Microsoft .NET Core 6.0 with Azure AD integration. It leverages Microsoft Graph API for user management, SharePoint for document access,

and Exchange Online for email communications. The application implements OAuth 2.0 authentication flow with PKCE for enhanced security.

Security Requirements

• Multi-factor authentication mandatory for all users

• Conditional access policies based on location and device compliance

• Privileged Identity Management (PIM) for administrative roles

• Regular access reviews and automated de-provisioning

• Encryption in transit and at rest for sensitive data

• Comprehensive audit logging with 7-year retention

Required Azure Application Permissions

The following Microsoft Graph API permissions are required for the application to function properly. Each permission has been evaluated for necessity and follows the principle of least privilege.

Critical Risk Permissions

Directory.ReadWrite.All

Justification: Required for managing organizational units and administrative settings

RoleManagement.ReadWrite.All

Justification: Needed for automated role assignment and access provisioning

High Risk Permissions

Application.ReadWrite.All

Justification: Required for managing application registrations and service principals

User.ReadWrite.All

Justification: Needed for user provisioning and profile management

Group.ReadWrite.All

Justification: Required for dynamic group management and security group operations

Policy.ReadWrite.All

Justification: Needed for conditional access policy automation

Files.ReadWrite.All

Justification: Required for SharePoint document management and file operations

Medium Risk Permissions

Directory.Read.All

Justification: Required for reading organizational structure and user relationships

Application.Read.All

Justification: Needed for application discovery and configuration validation

User.Read.All

Justification: Required for user profile access and directory browsing

AuditLog.Read.All

Justification: Needed for security monitoring and compliance reporting

SecurityEvents.Read.All

Justification: Required for threat detection and incident response

Low Risk Permissions

Mail.Read

Justification: Required for reading user emails in customer service scenarios

Group.Read.All

Justification: Needed for group membership validation and access control

User.Read

Justification: Basic profile access for authentication and user identification

profile

Justification: Standard OpenID Connect profile claims

openid

Justification: Standard OpenID Connect authentication

email

Justification: Email address access for user identification

Compliance and Risk Management

GDPR Compliance

The application implements data protection by design and by default. Personal data processing is limited to legitimate business purposes with appropriate technical and organizational measures. Users have full rights to access, rectify, and erase their personal data as required by GDPR Articles 15-17.

SOX Compliance

Financial data access is restricted to authorized personnel with appropriate segregation of duties. All financial transactions are logged with immutable audit trails. Access controls are reviewed quarterly and any changes require management approval.

NIST Cybersecurity Framework Alignment

- IDENTIFY (ID): Asset management and risk assessment procedures implemented
- PROTECT (PR): Access control and data security measures in place
- DETECT (DE): Continuous monitoring and anomaly detection configured
- RESPOND (RS): Incident response procedures and communication plans established
- RECOVER (RC): Recovery planning and backup procedures documented

Implementation Timeline

Phase	Timeline	Deliverables	Risk Level
Planning & Design	Weeks 1-2	Architecture review, permission justification	Low
Development	Weeks 3-8	Core application, API integration	Medium
Security Testing	Weeks 9-10	Penetration testing, vulnerability assessment	High
UAT & Deployment	Weeks 11-12	User acceptance testing, production deployment	Medium
Monitoring & Review	Ongoing	Continuous monitoring, quarterly access reviews	Low

Contact Information

Role	Name	Email	Phone
Project Manager	Sarah Johnson	sarah.johnson@company.com	+1 (555) 123-4567
Lead Developer	Michael Chen	michael.chen@company.com	+1 (555) 123-4568
Security Architect	David Rodriguez	david.rodriguez@company.com	+1 (555) 123-4569

Compliance Officer	Emily Davis	emily.davis@company.com	+1 (555) 123-4570

This document is intended for testing the Azure Application Registration Risk Analysis tool. The permissions and scenarios described represent realistic enterprise requirements that should trigger appropriate risk assessments and NIST CSF 2.0 mappings.