Threat Model – [tm-project-name]

# Preamble

*Important to note: The curators of this document cannot certify/attest to security of an architecture nor code – the below is intended to help identify and track design decisions and outstanding work related to discussed attack vectors identified during the engagement and intended to provide guidance to CSE dev crews.*

*This document should remain internal-only and is intended to help produce backlog items specific to the customer engagement, in conjunction with those suggested via https://aka.ms/BRIE. Please direct your customer to work with their account team or preferred security vendor to seek an audit or pen-test from a security vendor if required/desired.*

# Overview

Please find the Threat Model for the [tm-project-name] below. This document shows the threat model and data flow diagram of the application. These artifacts were constructed based on documentation and source code from the project itself and are subject to change as the architecture and codebase evolves. Each of the labeled entities in the figures below are accompanied by meta-information which describes the threats, describes the data in scope, and recommendations for security controls.

# Diagrams

## Architecture Diagram

< Insert Arch Diagram here>

## Data Flow Diagram

< Insert DFD/s here>

## Threat Map

< Insert Threat Map here>

## Data Flow Attributes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Transport Protocol** | **Data Classification** | **Authentication** | **Notes** |

## Threat Properties

# Appendix

## Security Principles

* **Confidentiality** refers to the objective of keeping data private or secret. In practice, it’s about controlling access to data to prevent unauthorized disclosure.
* **Integrity** is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable.
* **Availability** means that networks, systems, and applications are up and running. It ensures that authorized users have timely, reliable access to resources when they are needed.
* **Privacy** relates to the activities that focus on individual users’ rights.

## Microsoft [Zero Trust](https://www.microsoft.com/en-us/security/business/zero-trust/?ef_id=67d61e29cde6157ddb0b7f7559e92f81:G:s&OCID=AID2200938_SEM_67d61e29cde6157ddb0b7f7559e92f81:G:s&msclkid=67d61e29cde6157ddb0b7f7559e92f81) Principles

* **Verify explicitly**. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
* **Use least privileged access**. Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.
* **Assume breach**. Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defense

## Microsoft Data Classification Guidelines

|  |  |
| --- | --- |
| **Classification** | **Description** |
| **Sensitive** | Data that is to have the most limited access and requires a high degree of integrity. This is typically data that will do the most damage to the organization should it be disclosed.  Personal data (including PII) falls into this category and includes any identifier, such as name, an identification number, location data, online identifier. This also includes data related to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of an individual. |
| **Confidential** | Data that might be less restrictive within the company but might cause damage if disclosed. |
| **Private** | Private data is usually compartmental data that might not do the company damage but must be kept private for other reasons. Human resources data is one example of data that can be classified as private. |
| **Proprietary** | Proprietary data is data that is disclosed outside the company on a limited basis or contains information that could reduce the company's competitive advantage, such as the technical specifications of a new product. |
| **Public** | Public data is the least sensitive data used by the company and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in the company. |