ISE Security Checklist Items

**Please remove this page before sharing security plan information with your customers**

Complete these tasks and share your progress throughout the engagement at [ISE SecDev Calculator](https://aka.ms/isesecdevcalc). If guidance is needed on completing the SecureDev checklist items, please see [ISE SecDev Guidance](https://github.com/commercial-software-engineering/ISE-Security-Plan/blob/main/ISE%20Security%20Checklist%20Instructions.md).

* Regularly review security recommendations from Defender for Cloud throughout your engagement as you deploy your code. Remediate findings or create backlog items as appropriate.
* Identify and meet with the customer’s security stakeholder during the start, middle, and end of the engagement. Identify and prioritize security requirements, share progress, and hand off unfinished backlog items.
* Meet with an ISE security champion or a member of the Security Tech Domain to review the design for your solution.
* With the help of a champion or the Security TD, review and identify the elements in this security plan template that will be completed during the engagement. Deliver the completed components of this plan to the customer, ideally by committing it in markdown format to the customer's repo, so that they can integrate it into their threat model(s).

Security Plan – Project Name

# Preamble

*Important to note: ISE cannot certify/attest to the security of an architecture nor code. This document is intended to help produce backlog items specific to the customer engagement and to document the relevant security design decisions made by the team during build. 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 Security Plan for the Project Name below. This document shows the architecture 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 image here>

## Data Flow Diagram

<insert image here>

For help getting started, please see our [Security Plan Guidelines](https://www.cwcwiki.com/wiki/Security_Plan_Guidelines) and [Microsoft Threat Modeling Security Fundamentals](https://learn.microsoft.com/en-us/training/paths/tm-threat-modeling-fundamentals/).

## Data Flow Attributes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Transport Protocol** | **Data Classification** | **Authentication** | **Authorization** | **Notes** |
| 1 | Name of the protocol for the service | Data classification guidance can be found in the [Appendix](https://www.cwcwiki.com/wiki/Security_Plan_Guidelines#Microsoft_Data_Classification_Guidelines) | Method of authenticating the caller | Method of authorizing the caller | Additional notes |
| … | … | … | … | … | … |

# 4. Threats and Mitigations

<insert notable threats and mitigations here however you like>

For inspiration, see our [Example Threats and Mitigations](https://www.cwcwiki.com/wiki/Security_Plan_Guidelines#Example_Threats_and_Mitigations)

# 5. Secrets Inventory

An ideal architecture would contain **zero secrets**. Credential-less options like managed identities should be used wherever possible. Where secrets are required, it’s important to track them for operational purposes. Please see our [Example Secrets Inventory](https://www.cwcwiki.com/wiki/Security_Plan_Guidelines#Example_Secrets_Inventory) to help you get started.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **What is its purpose?** | **Where does it live?** | **How was it generated?** | **What's the rotation strategy? Does it cause downtime?** | **How does the secret get distributed to consumers?** | **What’s the secret’s lifespan?** |
| … | … | … | … | ... | … | … |