WindSim Accelerator – Security

Date: 3. May 2022

Introduction

WindSim Accelerator is a SaaS (software as a service) application running on the Microsoft Azure Cloud platform.

Microsoft Azure maintains the largest compliance portfolio in the industry including CSA Star, SOC 3, and several ISO standards. For the full list see https://docs.microsoft.com/en-us/azure/compliance/offerings/ .

WindSim follows industry standards and best practices to protect the interests and privacy of our client's organization by securely managing customer data. This document describes the security measures implemented in WindSim Accelerator, divided into the following categories: Security, Availability, Processing integrity, Confidentiality and Data Privacy.

Security

This principle refers to protection of the system against unauthorized access. Access controls help prevent potential misuse of the system or data.

We ensure to safeguard our application from the following vulnerabilities through the following measures and deployment infrastructure on Azure:

- SQL Injection
- Cross Site Scripting (XSS)
- URL/HTTP Manipulation Attacks (Parameter Tempering)
- Cross Site Request Forgery (CSRF)
- Brute Force Attacks (DDoS)
- Insufficient Access Control
- Too Much Information in Errors/Public Configuration

Secure Access Control

We have implemented authentication and authorization to ensure that the user can only access appropriate services, views, and data. WindSim Accelerator uses a basic authentication method where the user provides a username and password to log in. Furthermore, we manage authorization through roles and claims and logging, so that the users, application, and data are isolated from each other to ensure security.

Availability

The availability principle refers to the accessibility of the system.

We monitor the system through health checks and heartbeat to ensure continuous up-time for our users. WindSim Accelerator uses multiple redunadant servers to secure up-time and scales the system automatically according to the load.

We have different logging and monitoring systems in place and have configured alerts against certain thresholds to take timely actions.

Processing integrity

We ensure the quality and integrity of the system by testing it in several ways: Automated tests of the software to ensure that the system is producing the expected output and manual periodic reviews of the system output.

Confidentiality

The data in our system is only accessible to the intended users of an organization. We encrypt the data for protecting confidentiality.

We secure the data at rest and in transit by the following methods:

- Protecting data during transmission through SSL
- Microsoft SQL and Azure SQL provide Transparent Data Encryption (TDE)
- SQL Azure encrypts the database by default
- Azure Blobs, Files, Table, and Queue Storage are encrypted by default

Data Privacy

We follow the privacy guidelines mentioned in the GDPR standard, which describes the collection and use of personal identifiable information.

- We collect the following personal information to use our application
    - First name, last name, email, phone number and organization name, address, and phone number
- The personal information is kept to perform necessary operations in the application and according to the contract / agreement.
- User can delete data (personal, organization, project level).
- Your data will not be used or shared for any other purpose than stated in the contract.
- Additional use of data is described in detail in the contract.