## Introduction:

This document highlights the ROE (Rules of Engagement). This is an overview of what we consider to be permitted and off limits while we perform the web application security assessment.

### Rules of Engagement:

#### We will not perform the following tasks in our assessment:

* Scanning or testing assets outside of the target list.
* Gaining access to any data that is not wholly our own.
* Performing any kind of denial of service testing.
* Performing automated testing of services that generates significant amounts of traffic.
* Deliberately accessing any data owned by but not limited to other third party vendors, or customer(s).
* Moving beyond “proof of concept” reproducible steps for infrastructure execution issues (i.e. proving that you have sysadmin access with SQLi is acceptable, running xp\_cmdshell is not).
* Using your services in a way that violates your Acceptable Use Policy or End User License Agreement.
* Attempting phishing or other social engineering attacks against your employees.

#### We will attempt to perform the following activities:

1. Create a small number of test accounts and/or trial tenants for demonstrating and proving cross-account or cross-tenant data access.
   1. We will not attempt to use one of these accounts to access the data of another customer or account.
2. Perform network fuzzing, port scan and vulnerability scan against the noted web server.
3. Perform web application fuzzing, and vulnerability scans against the noted web application.
4. Load testing your application by generating traffic which is expected to be seen during the normal course of business.
5. Testing security monitoring and detections (e.g. generating anomalous security logs, dropping [EICAR](https://en.wikipedia.org/wiki/EICAR_test_file), etc.).
6. Attempt to break out of a shared service container (e.g., Azure Websites or Azure Functions, AWS, Google Cloud Platform).
   1. Should we succeed we will immediately report our finding to you and we will stop any further testing (we will not dig any deeper).
7. Test the enforcement of any other restriction policies.