## **Purpose**

The purpose of this assessment is to identity risks and security gaps associated with the Snipe-IT asset management application (*application)* in use by the Zen Strategics (*company*).

### **Scope**

This ROE applies to the Snipe-IT application, and the host(s) it is running on, and excludes all other workloads, hosts, networks, and data the in use by the company. The underlying cloud infrastructure is also in scope for review and recommendations for improvement. The ROE also applies to the personnel engaged in, or having access to the data obtained, and activities generated because of this assessment.

## **Key assumptions**

There’s inherent risk of data loss due to this assessment, however no activities will result in “intentional” data loss. This assessment will not replicate adversarial action as such activity(s) fall outside the scope of the assessment. The application will be deployed on the hardened systems per company policy, which may necessarily limit the assessment activities to the application itself.

## **Background statement**

The company has authorized the activity as described in the scope, and the company officers will take full responsibility and absolve the assessors of any liability the assessment may result in. The assessment will be conducted remotely over the company-supplied connections to the assessor virtual machine residing in the company owned AWS account.

## **Preparation**

The company will furnish a Kali Linux official AMI (*attack machine)*, provide access to the necessary bastion servers or other secured access to the attack machine, and ensure the machine had adequate compute and storage to conduct the assessment.

The company will provide access to the application source code for offline static code review.

## **Assessment**

The assessment team will conduct their activities only from the furnished attack machine.

The assessment team will limit their tool choice based on available software on the attack machine, to include but not limit to Nmap, Nikto, Metasploit and Burp Suite.

The assessment team will notify the company and its officers of any significant event that may occur during the assessment.

## **Post Assessment**

The assessment team will provide a final penetration test report within an agreed upon time frame after the conclusion of the test (TBD).

The report will contain the scope of the assessment also found in this document, the list of activities performed, the results of the assessment and recommendations on remediation of the findings. The final report is provided as-is and for information purposes only. The assessment team does not provide any warranties that further findings are not present in the system(s) and application(s) in scope.