To: The Knowledge House
From: The Group Members of the Secure Program Capstone
Date: April 19, 2023

Statement of Scope for the Threat and Vulnerability Assessment of The Knowledge House

1. Purposes and Objectives

The objective of this threat and vulnerability assessment is to identify potential risks and vulnerabilities in the information technology infrastructure of the non-profit educational organization The Knowledge House, whose headquarters is located 363 Rider Avenue, Bronx, NY 10451. The assessment will help the organization to strengthen its security posture and reduce the risk of cyber attacks and physical security breaches.

2. Focus of the Assessment

The assessment will focus on identifying potential security weaknesses in the following areas:

- Network and system architecture, including firewalls, routers, switches, and servers
- Web applications and databases
- Mobile devices, laptops, and desktops
- Data storage and transmission, including cloud services
- Third-party vendors and service providers

The focus of the assessment will include the following:

- *Information systems*: This includes all hardware, software, and network infrastructure used by the non-profit, including servers, workstations, laptops, mobile devices, and cloud-based systems.
- *Applications*: This includes all web-based and mobile applications used by the non-profit, including those used for financial transactions, data management, and communication.
- *Physical infrastructure*: This includes all buildings, entrances, exits, and security controls used by the non-profit to protect its physical assets.
- *Employees*: This includes all employees of the non-profit who have access to sensitive information.

3. Assessment Techniques & Methodologies

The assessment will be conducted in accordance with industry best practices, including the Open Web Application Security Project (OWASP) and the National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO) Cybersecurity Frameworks.

The assessment will be conducted by performing a combination of automated and manual techniques, including network and system scanning, vulnerability scanning, penetration testing, social engineering, and phishing simulations.
The threat and vulnerability assessment will use a combination of techniques, including:

- *Physical security assessment*: This will involve an on-site inspection of the non-profit's physical infrastructure, including buildings, entrances, exits, and security controls.

- *Network scanning and penetration testing*: This will involve scanning the non-profit's network for vulnerabilities and attempting to exploit those vulnerabilities to gain access to sensitive information.
- *Social engineering*: This will involve attempting to gain access to sensitive information by tricking employees into revealing passwords or other confidential information.
- *Application security testing*: This will involve testing the security of the non-profit's applications, including web-based applications and mobile applications.

4. Limitations

The threat and vulnerability assessment will not disrupt the day-to-day operations of the non-profit. The assessment will be conducted during normal business hours, and all testing activities will be coordinated with the non-profit's IT department to ensure that no disruption occurs.

5. Reporting

Upon completion of the assessment, a comprehensive final report will be prepared that summarizes the findings of the threat and vulnerability assessment. The report will include a list of all identified vulnerabilities, an assessment of the overall security posture of the non-profit, and recommendations for improving security. The report will also include a summary of all testing activities, including methodologies, tools used, and testing results. The report will be designed to help the organization improve its overall security posture and reduce the risk of cyberattacks.

Acknowledgement of Consent

(To be reviewed and signed by a representative of The Knowledge House.)

This statement of scope outlines the objectives, scope, and boundaries of the threat and vulnerability assessment for The Knowledge House. We understand and agree to the project's objectives, scope, and limitations as outlined in this document.

We acknowledge that the project team has the authority to define and implement the project scope and methodology, with adherence to Section 4 of the Statement of Scope and we commit to providing the necessary resources and support to ensure the project's success.

Representative Printed Name: _____

Representative Job Title: _____

Representative Signature: _____

Date: _____