**Terms and Conditions**

The participant of the bug bounty program, by registering to participate agrees to the terms and conditions that are laid out in this document. Only students, faculty, and staff are allowed to participate in the bug bounty program at **{Insert College/University Name}**. Faculty and staff participants must not participate in this program during working hours. Any faculty and/or staff participation must not create a conflict of interest.

1. **Definitions**
2. **Participant-** An individual is registered as a participant in the bug bounty program and is allowed to look for vulnerabilities.
3. **Automated Scanners-** A tool/software that can be used to auto-run scans on the university’s systems.
4. **Non-Substantial Vulnerability-** A vulnerability that is deemed to be a low severity or less and does not pose a significant risk.
5. **In-Scope-** A vulnerability that participants are allowed to test/look for as a participant of the bug bounty program.
6. **Out-of-Scope-** Vulnerabilities that participants are not allowed to test for as a participant in the bug bounty program. If the participant accidently discovers one, they will be provided safe harbor if it is reported using the same method as an in-scope vulnerability.
7. **Bounty and Point Eligibility**

A participant is eligible for points and a bounty if they are a registered participant in the bug bounty program and has reported a vulnerability that is deemed to be in-scope. The amount of the bounty and the number of points awarded is dependent upon the severity of the vulnerability that is reported. A duplicate vulnerability is not eligible for bounty or points. All points will be reset at the beginning of each academic year on **{Insert Date Here}**. This is to ensure that as new participants join, they are not behind in points and have a chance to win the reward for most points.

All reported vulnerabilities will be verified by the university’s IT department to verify severity at which point the points and bounty will be awarded. The university has final say in the final severity determination of a reported vulnerability. All bounties will be awarded no later than a month after the vulnerability was reported. All points will be awarded within **{Insert time frame here}** of vulnerability confirmation by the IT department

At the end of the point cycle, which is just before the beginning of a new academic year, the participant with the most points will receive an award for being in first place in the bug bounty.

**Points**

* Critical: 150 points
* High: 100 points
* Medium: 50 points

**Bounty:**

* Critical: $200
* High: $125
* Medium: $50

1. **Registration Requirements**

Any individual who would like to participate in the bug bounty program for **{Insert College/University Name Here}**. Any member not registered for participation is not eligible for points or for bounty and is not granted guaranteed safe harbor for a reported vulnerability. No participation in the bug bounty program is authorized until the participant receives the welcome/confirmation email from the university confirming their registration and providing the details to participation in the program.

1. **Tax Requirements**

Any total bounty awarded to a participant will be reported to the IRS for tax purposes. Therefore, all earned bounty must be reported as income on the participant’s personal tax return.

1. **Violations of the Terms and Conditions**

Any individual that violates the terms and conditions of this bug bounty program are subject to disciplinary/legal actions under the student honor code and any applicable state and federal laws that regulate this type of activity.