ETHICAL CODE OF CONDUCT

Cyber Security Club
Department of Computer Science & Engineering
University of Texas at Arlington
500 UTA Blvd, ERB 316
Arlington, TX 76010

While attending and participating in activities with the Cyber Security Club, you will be learning about security information systems. In doing so, you will also be learning how one can break such systems with *hacking tools*, including but not limited to buffer overflows, injection attacks, cross-site scripting, viruses, network scanners, and reverse engineering.

This information is shared solely for the purposes of cyber defense. In participating in these activities, you hereby submit that you will not use any of the *hacking tools* we discuss or any other *hacking tools* or other means to improperly access any systems that you do not own or have express written authorization to do so, deny service to legitimate users, or otherwise act in an illegal or improper manner.

If at any time you think that your actions could possibly violate this code, you will discuss the matter with any of the club officers or faculty advisors before proceeding.

Any violation of this ethical code of conduct may result in legal penalties, University sanction, and you will be permanently banned from the Cyber Security Club organization and not be allowed to participate in any future activities.

Club Officers, John Podolanko, Zehra Jafri, Mitchell Shelton, Cam Nguyen and Andrew Collyer, Faculty Advisors Jiang Ming and Dave Levine, the Cyber Security Club, the Department of Computer Science and Engineering, the University of Texas at Arlington, and the State of Texas take no responsibility for your conduct with regards to what you learn within. You take full responsibility for your own actions.

I, _____, hereby acknowledge that I have read and agree to follow the terms of this ethical code of conduct statement.

Signature: _____ Date: _____

CSEC Officer's Signature: _____ Date: _____