Highline
COMMUNITY COLLEGE

Code of Conduct for CIS/CSci students

In the course of their study and during project work, CIS/CSci students are trusted with access to the practices, procedures and technologies used to attack and protect valuable information assets, systems, and data. This trust requires an uncompromising commitment to the highest moral and ethical standards. Adherence to all laws, rules and regulations applicable to the field and practice of information security is critical. This requires more than simple obedience to the law. We expect that professionals trained by HCC will demonstrate sound ethics, honesty and fairness in providing secure products and services.

HCC expects each student to assume a sense of personal responsibility for assuring the compliance of his or her own behavior and those of their fellow students. The Code of Conduct represents a “zero tolerance” policy. All students enrolled in CIS and CSci courses are expected to:

Conduct all activities in accordance with the academic integrity standards posted on the HCC web site (see below)

- Be aware of, and abide by, the laws of the United States, the individual states, foreign countries and other jurisdictions in which the student may conduct studies, projects, research or other activities
- Adhere to the spirit of the law as well as its substance
- Always act with personal integrity based on principles of sound judgment
- Neither condone nor ignore any illegal or unethical acts for any reason

Students should be aware that they may be held personally liable for any improper or illegal acts committed during the course of their education, and that "ignorance of the law" is not a defense. Students may be subject to civil penalties, such as fines, or regulatory sanctions, including suspension or expulsion. Potential penalties for illegal acts under federal sentencing guidelines are severe and may include imprisonment and substantial monetary fines. Existing federal and state laws, as well as the laws of foreign jurisdictions, may impose civil money penalties, permit the issuance of cease and desist orders, or have other consequences.

All students are required to abide by the Student Rights and Responsibilities in Instruction Computing Facilities (http://flightline.highline.edu/ic/policies/responsible.php) as well as the Highline Computing Resources Appropriate Use Policy (http://policies.highline.edu/docs/aup.php). Key excerpts are listed below, but students are expected to abide by the full policies.

It is the obligation of College students to be aware of their responsibilities as outlined in the Student Rights and Responsibilities policy (http://studentservices.highline.edu/srr.php). ⍰ Users shall respect the rights and property of others and not improperly access or attempt to access, misuse, misappropriate or violate security of computing resources. ⍰ Sharing of passwords constitutes a violation to network security, which may lead to unauthorized use or misuse of campus resources. All computer account passwords are confidential and should not be shared with anyone. Individuals will be held accountable for any activity occurring through the use of their respective passwords. ⍰ Using someone else's password, regardless of how it was obtained, is also a violation of this policy. ⍰ Running or installing a program intended to damage or create excessive load on any computer system or network is forbidden

Using the campus network to gain unauthorized access to any computer system is forbidden.

Every student is responsible for ensuring that his or her personal conduct is above reproach. Violations of the standards described in this Code of Conduct should be reported immediately to your instructor. HCC takes these ethical obligations very seriously. Violations will not be tolerated and will result in disciplinary action appropriate to the violation.

Statement for Network Specialist and Data Recovery & Forensics students:

Due to the special nature of the lab exercises for network intrusion detection, certain additions to the above policies will be in effect, as follows:

- Students understand that the removeable hard drives in the Building 29 labs are not to leave the building. Lockers are available if you want to use your drive during open lab hours and the storage room in locked.
- Every experiment run in conjunction with this course will have certain rules and regulations regarding its conduct. These will be explained when the assignments are given and students are expected to comply with any additional restrictions.
- To the extent that lab computers are used to stage attacks under controlled circumstances, they will be physically disconnected from all external networks. All student users of this lab must maintain this lack of connection and must verify this lack of connection (with instructor help) before running any malicious code or exploit.
- Students understand that the exercises are being taught to gain knowledge about security flaws and how to prevent them. Use of same against an outside entity or the institution is a felony and prosecutable offense.
- Security flaws and other problems in this lab should be pointed out immediately to the lab instructor who will report it to the helpdesk.
- Students may only affect approved computers in 29-203. All other computers are off limits.
- Students are responsible for the consequences of any actions they take without the knowledge of the lab instructor.

Statement for Web/Database Developer students:

Due to the confidential nature of some data accessed during development projects, certain additions to the above policies will be in effect, as follows:

- You will be required to take the FERPA (Family Educational Rights and Privacy Act) online tutorial (http://registration.highline.edu/ferpa/intro.php). Any student information accessed during development projects should be considered confidential and kept protected at all times.
- Under Washington state law, all student records are considered privileged communication and information may not be disclosed to others without the students' written consent. Do not access or share any student information unless your instructor directs you to do so.

NOTE:

Anyone violating appropriate use policies as outlined in this agreement will be held accountable for their actions. Your instructors will not provide excuses for unethical or questionable behavior of students who do not discuss their intentions with the instructor, in person, and prior to taking any actions. Students are encouraged to think about and report computer or data security vulnerabilities, but should seek guidance and approval from an instructor before testing any theories they have.

I hereby certify that I have read and understand the college policies and Code of Conduct outlined on these pages and agree to abide by them.

______________________________________ ______________________________________

Print Name Student ID Number

______________________________________ ______________________________________

Sign Date