CS331 Code of Ethics

Before taking this course, you must agree to adhere to a code of ethics. This code says, in essence, that you will not use the knowledge you gain to harm other people or property. Many of the activities you will engage in this semester have been authorized by campus stakeholders only because I personally assured them that you will adhere to the highest standards of personal and professional responsibility.

Any student who does not sign this form will be dropped from this course. Any student who signs this form and who does class assignments in good faith can count on me to be a strong advocate in the event of misunderstandings. Conversely, any student who signs this form and knowingly violates these principles during the semester will be forwarded to the Honor and Discipline Committee. The skills you obtain this semester can cause in serious harm if abused, so before I teach you, I must have your assurance that you will use your knowledge responsibly.

Some of the rules in this code may strike you as especially stringent. As a potential cybersecurity worker, you need to understand that your actions can adversely affect the profession. The study of computer security is a critically important area of computer science, but because of its pervasiveness and impact, its activities are always in danger of being outlawed. Therefore, we must hold ourselves to a higher standard of conduct than our peers.

The Code*

You agree to:

- Keep private and confidential information gained in your work. You will not collect, give, sell, or transfer any personal information to a third party without the consent of affected parties.
- Disclose to the appropriate persons or authorities potential dangers to e-commerce, the Internet community, and the public.
- Be honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.
- Never knowingly use software or process that is obtained or retained either illegally or unethically.
- Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use the property of a third party only in ways properly authorized, and with the owner's knowledge and consent.
- Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- Ensure good management for any project you lead, including full disclosure of risk.
- Add to the knowledge of the cybersecurity community by your study, share the lessons of your experience with your cybersecurity peers, and promote public awareness of benefits of good security practice.
- Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.

*Adapted from the EC-Council's Code of Ethics.

- Ensure ethical conduct and professional care at all times on all assignments without prejudice.
- Not associate with malicious hackers nor engage in any malicious activities.
- Not purposefully compromise or allow a third party's systems to be compromised in the course of your activities.
- Ensure all penetration testing activities are authorized and within legal limits.
- Not take part in any "black hat" activity or be associated with any community that serves to endanger people or infrastructrure.
- Not be a part of any underground hacking community for purposes of preaching and expanding black hat activities.
- Not make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
- Not be convicted of any felony, or violate any law.

I, the undersigned, agree to the above code of conduct and I understand that failure to adhere to this code constitutes an Honor Code violation, or worse.

Signature: _____

Name: _____