

White Hat Code of Conduct

Just because you *can* do something, doesn't mean you *should*.

I understand that, as a student in the Information Security Program¹, I must abide by WMU's information technology and computing policies. For purposes of this Code, those Policies include, but are not limited to, the Computing Resources Acceptable Use Policy, which applies directly to my courses in this Program. I know that I can find this and other Office of Information Technology Policies at <http://wmich.edu/it/policies>. In addition to these policies, I agree to adhere to the terms, conditions, and the spirit of this White Hat Code of Conduct.

I understand that, while at WMU, I will learn tools, techniques, and approaches for evaluating data security, security procedures, networks, and systems. These tools and approaches are critical for information security professionals to secure and protect assets. However, if used incorrectly, they can also result in security breaches, network degradation, and other forms of damage. In performing work within the program or using knowledge that I learned in program classes, I will strive not to adversely impact organizational computing resources or overall security architecture of WMU or other entities.

I further agree to:

- Examine and use the tools and approaches I learn through the program's classes only as directed and confined to the course labs;
- Report any security vulnerabilities discovered to the course instructor immediately, and not disclose them to anyone other than the appropriate authorities;
- Maintain the confidentiality of any private information learned through course labs;
- Hold harmless and indemnify the course instructor, department, college, and University if I incorrectly use, intentionally or unintentionally, any of the tools or information I learn in this Program to cause damage to University or private systems; and
- Abide by all laws governing use of computer resources.

I agree to NOT:

- Attempt to gain unauthorized administrator access to any server, network hardware or other network device to increase privileges on any university workstation;
- Disclose any private information that I discover as a direct or indirect result of this course;
- Take actions that will modify or deny access to any data or service that I do not own;
- Attempt to perform any unauthorized actions or use utilities outside the confines and structure of the labs; and
- Utilize any security vulnerabilities other than those for which I am specifically authorized during my enrollment in this program and/or course.

I have been given the opportunity to ask questions about this Code of Conduct and I understand its terms. I understand that I may suffer academic and/or disciplinary consequences for failing to follow this Code or any of WMU's information technology or computing policies.

Signature: _____

Printed Name: _____

Date: _____

Sites Referenced

- <https://cert.eccouncil.org/code-of-ethics.html>
- <https://www.eccouncil.org/code-of-ethics/>
- <http://www.wmich.edu/it/policies/computingrules>

¹ This includes students in the Information Security M.S. or Graduate Certificate, as well as any other students taking a course offered primarily as a part of this program.