*Cybersecurity Code of Ethics*

Nathan Ketterlinus

*Fisher College of Science and Mathematics*

*Towson University*

Towson, United States

[nketter1@students.towson.edu](mailto:nketter1@students.towson.edu)

***Abstract*—This paper is designed to outline basic guiding principles for ethical and professional behavior in the field of cybersecurity. These principles, while not an exhaustive list, serve more as a minimum for ethical behavior and should be treated as such.**

***Keywords—Ethics, Cybersecurity, Behavior***

# Preamble

As the world becomes increasingly digitized, the role that computer scientists and cybersecurity experts play becomes more and more relevant to all groups of people. As such, the power they hold as system designers and data protectors must be used in a way that promotes the greater good of the public above all else. This document is meant to serve as a guideline for responsible and ethical behavior in the computing field but should not be considered a complete list. It is divided into three areas in which a computer professional should be focused: their duty to self, duty to peers, and duty to employers.

# Duty to Self

Computer professionals have certain responsibilities that they must uphold in order to be effective in their field. Among these, computer professionals should:

1. Keep the greater good at the forefront of all computer related activity. As everyone is a stakeholder in computing, efforts should be made to minimize the potential damage of any project, and to respect all groups equally [1] (section 1.1).
2. Strive to continually learn. Computing is one of the most dynamic fields the world has ever seen. As such, computer professionals should adapt to changes to remain relevant and productive. They should not only continue to develop skills in disciplines they already have expertise in, but also not be afraid to build expertise in separate areas as well [2] (section 8.01-8.02).
3. Be collaboration oriented. Just as computer professionals have a duty to continuously increase their own knowledge, they also have a duty to share their knowledge with others. This can be done in a variety of ways, but the most relevant is an effort to be as transparent in documentation as possible and to make work open-source when able.

# Duty to Peers

Computer professionals have a responsibility to behave ethically towards both their colleagues and the people that use their product. As such, they have an obligation to:

1. Respect copyright and intellectual property of their fellow creators. The research, work, and passion that goes into any project should be honored. Ultimately it is the right of the creator to share or withhold any of their creations, and as such their wishes should be respected when using their projects [1][3] (section 1.4)(points 4, 6-8).
2. Respect the privacy of everyone. This includes behaviors such as: collecting as little data as necessary, being transparent about what data is collected and how it will be used, only using data in authorized ways, and only accessing systems with explicit permission from their owners unless under the extreme circumstance that doing otherwise impedes the objective of contributing to the greater good [1] (sections 1.6-1.7).
3. Be conscientious of the impact of products. The possibility of any product being used for any purpose other than the intended one is large, and developers should take precaution to anticipate these alternate uses and limit those that abuse others, break governmental laws, or otherwise cause harm to the best of their ability [1] (section 3.7).

# Duty to Employers

Computer professionals often find themselves dealing with very confidential parts of their employer’s business. As such, precautions should be taken such that:

1. Confidential information, no matter how it is learned, stays confidential, unless it is to the detriment of the greater good. If information is acquired that should not have been, relevant authorities should be informed.
2. Ethical practices, such as the ones outlined here, are being enforced in the workplace.
3. Products are accurately advertised. This includes the skills of a computer professional to employers, as well as commercial products to consumers [4] (*Personal Integrity*).
4. Conflicts of interests are avoided as much as possible. Any conflict of interest is communicated to all relevant parties, and said parties have the authority to determine how to proceed [4] (*Personal Integrity*).

As a future computer professional, I hereby agree to uphold this code of ethics to the best of my ability.

##### References

1. D. Gotterbarn et al., “The code affirms an obligation of computing professionals to use their skills for the benefit of society.,” Code of Ethics, https://www.acm.org/code-of-ethics (accessed Sep. 3, 2023).
2. D. Gotterbarn, K. Miller, and S. Rogerson, “Software engineering code - ACM ethics,” ACM Ethics - The Official Site of the Association for Computing Machinery’s Committee on Professional Ethics, https://ethics.acm.org/code-of-ethics/software-engineering-code/ (accessed Sep. 3, 2023).
3. Cjohnson, “The Ten Commandments of Computer Ethics,” CPSR, http://cpsr.org/issues/ethics/cei/ (accessed Sep. 3, 2023).
4. USENIX, “System administrators’ code of ethics,” USENIX, https://www.usenix.org/system-administrators-code-ethics (accessed Sep. 3, 2023).