Wilmington University Code of Conduct for Computer Network Security (CNS) and Information Assurance (IA) Students

Undergraduate-level Computer and Network Security (CNS) and graduate-level Information Assurance (IA) students are entrusted with access to the practices, procedures and technologies used to attack and protect valuable information assets and systems. This trust requires an uncompromising commitment to satisfying the highest moral and ethical standards. Adherence to all laws, rules and regulations applicable to the field and practice of Computer and Network Security/Information Assurance is critical.

Maintaining Wilmington University's unique position in the field of Computer and Network Security/Information Assurance education, however, requires more than simple obedience to the law. Our faculty – as well as those who employ our graduates – expects that professionals trained by Wilmington University will demonstrate sound ethics, honesty and fairness in providing security products and services.

Wilmington University understands that this code must be flexible enough to deal with hundreds of different daily activities in addition to future academic, technology and business issues. Toward that end, Wilmington University expects each student to use sound judgment in the performance of his/her studies. Sound judgment means, among other things, that the student should consider whether his/her conduct would be viewed with approval by family, friends, colleagues, professors and the community at large were the activity to be disclosed. When in doubt, students should seek out their Program Chair for guidance and direction.

Students should read this code carefully, <u>and then execute the attached form</u> to certify that they have done so and to acknowledge a commitment to follow its terms.

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.

General Responsibilities

All students enrolled in the Computer and Network Security/Information Assurance programs are expected to conduct their activities in a manner that satisfies the highest of ethical standards. Each student must:

✓ Conduct activities in accordance with high ethical and moral standards.

✓ Conduct all activities in accordance with the academic integrity standards posted on the Wilmington University web site.

✓ 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.

✓ Do not condone, ignore or passively participate in any illegal or unethical act for any reason.

✓ Safeguard Wilmington University's security systems, confidential information and technology.

✓ Understand that this is a zero tolerance policy.

Confidentiality of Information

Students enrolled in the Computer and Network Security/Information Assurance programs are frequently required to deal with sensitive, proprietary and/or confidential information ("Confidential Information"). Every student must exercise care in handling Confidential Information concerning Wilmington University and its students, faculty, staff, employees, programs, sponsoring firms, or other organizations with which he or she comes into contact in the course of academic activities. Handling Confidential Information in a highly professional and discreet manner promotes Wilmington University's reputation for integrity, thereby enhancing relationships with Wilmington University, sponsors and other organizations.

Students should exercise the utmost care with Confidential Information in order to avoid violations of legal or ethical constraints. When in doubt, students should assume that information is Confidential Information and therefore subject to this high standard of care.

Students shall refrain from disclosing any Confidential Information, directly or indirectly, or using it for any purpose except as required in the course of their studies.

✓ Students will not be assigned to engagements or other tasks where they might be required to use or disclose trade secrets belonging to their employers.

✓ Students should not bring to class or group activities any information from their place of employment that might be considered proprietary or any proprietary items that may have been purchased or produced in the performance of the student's employment.

For students graduating or otherwise leaving the Program, the obligation to preserve the confidentiality of Confidential Information acquired in the course of their studies does not end upon termination of their studies at Wilmington University. The obligation continues indefinitely until Wilmington University or the individual or organization that owns the Confidential Information authorizes disclosure, or until the Confidential Information legally enters a public domain.

Copyrighted or Licensed Materials

It is both illegal and unethical to engage in practices that violate copyright laws or licensing arrangements. All Wilmington University CNS and IA students must respect the rights conferred

by such laws and arrangements, such as, refraining from making unauthorized copies of protected materials, including articles, documents and computer software and using software only in accordance with the applicable license agreement.

Access and Use of Computer Systems and Networks

Wilmington University supplies its students with access to Wilmington University-owned computer systems and networks for their use in accomplishing the studies and projects to which they have been assigned. Students should not assume any message transmitted by the student is private or confidential.

- ✓ The Wilmington University computers, software, telecommunications networks, and electronic mail systems are to be used only for official Wilmington University studies.

- ✓ Non-Wilmington University-owned electronics, software, equipment or computers are not to be introduced into, placed upon or connected to Wilmington University computers, systems or networks without the prior written permission of Wilmington University.

- ✓ Electronic mail accounts provided to students by Wilmington University are intended for exchanges related to their academic endeavors, not for personal communication or other inappropriate, illegal or unethical activities.

- ✓ Access to the Internet and the World Wide Web provided to students by Wilmington University is intended for academic research only, not for personal access, downloading, uploading, or other inappropriate, illegal or unethical activities.

- ✓ Wilmington University reserves the right to audit, intercept and monitor the use of computers, systems, networks, electronic mail accounts, and access to the Internet or the World Wide Web without notice to ensure proper usage. Further, Wilmington University reserves the right to save, use, print and disclose, including to authorities, without notice for any legal purpose any information related to a student's use of such technology.

- ✓ Students must have proper authorization and follow specified procedures in accessing and utilizing computers and computing networks whether the computers or networks are owned by Wilmington University or by a third party. Students must respect and strictly adhere to all security measures implemented by Wilmington University or on behalf of Wilmington University when accessing and utilizing any Wilmington University computers, software, telecommunications networks and electronic mail systems.

Summary

It is imperative that Wilmington University and its students conduct Wilmington University's academic activities in accordance with the highest possible ethical and legal standards. Every student is responsible for ensuring that his or her personal conduct is above reproach. Any student, faculty member or staff member who is involved or becomes aware of a violation or suspected violation of the standards described in this Code of Conduct should immediately notify the appropriate faculty member(s), the Program Chair, or the Dean of the College of Technology.

New students will read this Code of Conduct and sign the attached Student Certification and Agreement. The Student Certification and Agreement will be retained by Wilmington University for a period of not less than five (5) years following the student's graduation or otherwise leaving the Program.

Acceptable Behavior
The afore-listed constitutes the basis for establishing an "acceptable behavior" policy for the Computer and Network Security Program at Wilmington University (WU). This document is drawn from the policy statement (S/N 052001-2) by Dr Julie and Dan Ryan of George Washington University as revised by Adjunct Faculty member Mr. Russell Vitale. Subsequent drafts will be posted. Rev 4, 5/29/12

Wilmington University Code of Conduct
for Computer Network Security (CNS)
and Information Assurance (IA) Students

STUDENT ACKNOWLEDGEMENT

I acknowledge that I have received, read and fully understand Wilmington University's CNS / IA Code of Conduct policy. I understand my responsibility for adhering to this zero tolerance policy. I further understand that if I have any questions or am confused by any portion of the policy, it is my responsibility to get the matter resolved by asking your Program Chair.

_____
Student Signature

Print Name: _____

Date: _____