**Grey Hats Computer Security and Ethics Agreement**

The Grey Hats, a Registered Independent Organization at the University of Hawaii at Manoa will introduce you to a systematic approach to establishing, managing, and operating an effective information assurance program, equipping you with the latest methodologies, plans and practices. This included cyber defense and incident response strategies to system compromise, risk management decision-making, and legal and regulatory analyses.

**Members will:**

* Analyze the information assurance (IA) context
  + Demonstrate understanding of threats, vulnerabilities, strategic counter measures in a variety of contexts.
  + Describe the system services and strategies that implement IA
  + Understand the life cycle for IA in an organizational context
  + Gain an understanding of different techniques behind penetration and defense od networks and systems
  + Demonstrate an understanding of techniques, concepts, technology involved in security research, analysis, and development
* Analyze and design IA policies and plans
  + Instantiate organizational goals through IA policy and plans
  + Understand the human factors affecting the validity of IA policy and plans
  + Address legal and ethical issues related to IA
* Apply the principles of management
  + Understand the role and responsibilities of a CISO (chief information security officer)
  + Understand the role of risk management in IA decision making
  + Develop the ability and skills to maintain currency in IA
* Understand and apply the information perspective
  + Appreciate the concepts of information privacy and accountability
  + Understand the relationship between people and IA practices and technology
  + Achieve a working understanding of cryptography by studying theory and using it to communicate
  + Understand digital signatures and certificates
  + Appreciate ethical issues related to computers including privacy, freedom of speech online, IP, computer crime, influence of computers on society and trust in computers and computer professionals.

**Code of Conduct**

Schools, universities and groups such as Grey Hats that teach information security and information assurance subjects have begun to adopt codes of conduct to address the potential liability of teaching these subjects. The following was developed by George Washington University and the University of Washington, which is a leader in information assurance education, and is being adopted by this organization

**General Responsibilities for All Members**

Members are trusted 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 information security is critical. This requires more than simple obedience to the law. We expect that students trained by Gray Hats will demonstrate sound ethics, honesty and fairness in providing security products and services.

UHM and the Grey Hats RIO expect each member to assume a sense of personal responsibility for assuring the compliance of his or her own behavior and those of their fellow members. The code of conduct represents a “zero tolerance” policy. All members are expected to conduct their activities in a manner that satisfies the highest of ethical standards. Each member must:

* Conduct activities in accordance with high ethical and moral standards
* Conduct all activities in accordance with the academic integrity standards posted on the UHM website
* 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.

Members 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. Members 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 and/or monetary penalties, issue of cease and desist orders, or enforce other consequences. The Grey Hats or any affiliates take no association or responsibility for individuals or groups who act outside of the clearly stated and provided educational; lessons, training programs, and environments.

It is imperative that UHM and Grey Hats members conduct the University’s academic activities in accordance with the highest possible ethical and legal standards. Every member 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 made known immediately to Mr. Gerald K. H. Lau, Academic Advisor. UHM takes these ethical obligations very seriously. Violations will not be tolerated and will result in disciplinary action appropriate to the violation.

**Grey Hats Lab Use Policy:**

1. The following University of Hawaii at Manoa IT policy will be in effect, which can be found at:

<http://studentaffairs.manoa.hawaii.edu/policies/conduct_code/>

<http://www.hawaii.edu/policy/?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=210>

<http://studentaffairs.manoa.hawaii.edu/policies/conduct_code/>

1. University of Hawaii at Manoa acceptable computer policy use will be in effect, which can be found at:
2. General responsibilities for all members policy will be in effect can be found on the first page of this document.
3. Due to the special nature of computer security certain additions to the above policies will be in effect, they are the following:
   * Where appropriate, every experiment run will have certain rules and regulations regarding its conduct. These will be explained when the assignments are given and members are expected to comply with any additional restrictions.
   * To the extent that department computers are used to stage attacks under controlled circumstances, they will be physically disconnected from all external networks. All Grey Hats users must maintain this lack of connection and must verify this lack of connection (with either the club officers or advisor’s help) before running any malicious code or exploit.
   * Members may be allowed to attempt to run harmful software and obtain root access on department computers isolated from the network; as long as the members in question agree to fix any problems they cause (e.g. hardware damaging code).
   * Security flaws and other problems should be pointed out immediately to the club’s advisor.
   * Any member running an exploit in connection with an exercise must file an Exploit Approval form with the advisor, before running any malicious code or attempting any exploit on any of the ICS department’s computers.
   * Students are responsible for the consequence of any actions they take without the knowledge of the advisor.

I,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, hereby certify that I have read and understand this policy and the relevant university of Hawaii at Manoa policies referenced above reguarding computer lab use and will abide by them.

Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student ID No\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dated\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_