In recognition that academic computer forensics involves activities which have the potential to be harmful to computer networks and infrastructure, the Computer Forensics Addendum to the CIS IT Acceptable Usage Policy establishes additional policies, limitations and guidelines in order to minimize the risk of adverse events on UAB or CIS infrastructure or personnel.

All UAB CIS faculty, staff, students and guests who participate in computer forensics activities are bound by the terms and conditions set forth in this addendum and are responsible for ensuring that they are enforced.

Note: For the purposes of this document, “computer forensics resources” refers to the network, computers, software, disk space, web space, computer labs, special purpose hardware and any other equipment, resource or service owned or provided by the Computer Forensics group to its users.

Section 1. Authorized Usage Only

The privilege to participate in computer forensics activities is granted to students on an individual basis by the Director of Computer Forensics. Accounts and access to computer forensics resources are issued to you and are to be used solely by you. You must not share access to these resources with non-authorized people, or use accounts or resources for which you have not been authorized. You must not alter hardware, software or network configurations without permission or engage in computer forensics activities on networks or resources which are not designated for those activities.

Section 2. Academic Use Only

Computer forensics resources are provided for the sole purpose of supporting your academic computing needs related to the computer forensics curriculum and research program. Computer forensics resources are not be used for personal purposes unrelated to your academic work. Use of computer forensics resources for personal purposes may be treated as theft of services.

Section 3. Approval for Malware Research Activities

No malware will be executed without submitting a research plan for approval from the Director of Research in Computer Forensics. The plan must document: (a) the malware to be launched, (b) the research purpose, (c) the external systems that may be impacted, (d) the measures taken to ensure the safety of the public and UAB Computer Forensics systems, (e) the personnel who will participate in this study.

Section 4. Illegal Activities

It is strictly forbidden to use computer forensics resources for illegal purposes. Examples of illegal usage include, but are not limited to, attempts to gain access to computer systems for which you are not authorized, launching or propagating unapproved malware attacks, sharing or downloading of copyrighted material such as music, videos or books, or the distribution of sensitive or confidential information, including that protected by HIPAA or FERPA. Any illegal activities will be treated as attempted theft of services.

Revised 3/10. The most recent version of this document can be obtained at http://www.cis.uab.edu/it/CIS_AUP_Computer_Forensics.pdf
Section 5. Ethical Computing

Computer forensics research may lead to the discovery of personal, sensitive or confidential information, or knowledge about system or network vulnerabilities, which may be damaging to the owner if revealed. In such cases, you should inform your supervisor immediately. You must take every precaution to ensure the privacy and safety of such information or systems, and you must not share this knowledge with anyone outside those authorized by your supervisor.

Violations of this policy may result in loss of access to computer forensics resources as well as other disciplinary action as dictated by departmental and University policies and procedures.