This Statement rests on a core principle: that the underlying purpose of an academic environment is to encourage the development of critical thought, philosophical reflection, and practical skills for the students in that environment.

**Student Rights** This purpose is predicated on students’ right to several freedoms, namely: to question, to explore, and to investigate. The instructor also has a right to guide and foster those activities. In the context of information systems security and assurance, students have the right to develop the ability to question trust and security assumptions and dependencies of computer and information systems. This course seeks to provide the environment and materials to nurture these abilities.

These rights, however, are subject to important considerations and restrictions, particularly when the subject under study involves the use of computer machinery and information analysis and manipulation techniques that might enable certain types of unethical behavior that have the potential for causing harm to individuals and institutions.

Therefore, keeping the above rights and freedoms in mind, the attached Agreement sets out several important guidelines that govern student behavior in the course and subject matter at hand. The Agreement should impart an overriding ethical concern for the welfare and property of others; students should govern their use of the tools and techniques taught in this course with such concerns. Students should generally use these tools and techniques only on systems and software they themselves own, or where the terms of a license permit such action, or on software and systems where they have the explicit permission and informed consent of the system’s owner.

**Ethical Hacking Principles** Hacking is, unfortunately, a loaded term. We make a distinction between a special kind of knowledge, mindset, and skill from ill-advised, nuisance, or criminal behavior that might abuse this knowledge. For example, a doctor knows ways to harm humans, and might criminally abuse this knowledge. A locksmith is equipped to crack bank vaults. A policeman is trained to use and is armed with deadly weapons. Yet none of them is defined by the potential misuse of the special skills they possess. Similarly, hacking is a special technological skill that can be misused, but should not be defined by its misuses. For our discussion throughout this course, we use the term “hacking” to refer to the skill to question security and trust assumptions expressed in software and hardware.

Trust plays a significant role in societies and economies. It has an equally large role in software and computer engineering, since no engineer can build a complex system without relying on the components outside his or her control or scope of expertise to operate as expected. Incorrect trust assumptions lead to disasters in both societies and technologies; ubiquitous lack of trust (“low trust”) makes it hard to both bootstrap successful social structures and build complex systems (if nothing about the system’s state can trusted, its internal logic cannot meaningfully function; if nothing about a processing pipeline can be relied on, processing cannot meaningfully proceed). Engineers often formalize their trust assumption as “layer models” that their designs follow. The borders of these layers become natural boundaries of both trust and expertise (blocks below boundaries are counted on by developers to not “move”).

*It is the essence of the hacker mindset and skill to question such assumptions of engineering trust. It is the purpose of this course to provide students with an appreciation for the responsibilities such skills entail.*