Review the following outline providing some guidelines for ethical standards in the computing environment. Then answer the questions on the following page.

ETHICS in COMPUTING

1. **Respect for intellectual property:**
    a. Honor copyright laws and product licensing.
    b. Refuse to participate in software piracy or illegal copying of digital media.
    c. Avoid plagiarism of all or part of code belonging to someone else.
    d. Credit the source of ideas or code, even if from the Internet (provide website URL at the very least).
2. **Protection of data privacy:**
    a. Access to confidential data, even if part of your job, does not justify snooping or sharing of data in ways not required by your official responsibilities.
    b. Guard data from unauthorized access:
        i. Shred paper copies of personal or confidential information (also a good idea for your own printouts as you work on labs; do not throw away in trashcan for someone else to pick up).
        ii. Keep physical backup media (drive backups, disks, USB's etc.) in a secure place. Consider encryption of all backups.
        iii. Use proper passwords and other security measures to restrict database access and files with sensitive information.
        iv. Be aware of new risks with public WIFI hotspots. While using public networks, avoid transmitting personal information or working with applications (such as online banking) that contain confidential data. If you must use such applications, change your password afterwards.
        v. Do not place anything on a USB memory stick that you would not want made public. They are too easy to leave behind if you forget to unplug them, and easy to misplace or damage because of their small size. Create a file on your USB identifying it as yours, and make regular backups of the contents.
        vi. Keep laptops under your control at all times when traveling; they are a target for theft.
3. **Guarding system and network resources under your control from misuse:**
    a. Secure systems and networks with well-defined and up-to-date access lists.
    b. Use strong passwords, encryption, firewalls, and other techniques to lockdown network resources.
    c. Make sure applications you write are free of security loopholes.
    d. Keep security software and fixes up-to-date.
    e. Define guest accounts with restricted privileges for visitors needing Internet or other casual system access.
    f. Watch and track unusual computer use and attack attempts. Investigate them and remove any security holes.
4. **Respect for computer and network resource ownership:**
    a. Unauthorized use is same as trespassing on owner's property: intrusion may seem harmless with no intent for damage, but how would YOU feel if someone used YOUR system without your permission?
    b. Use caution about personal use of an employer's computer or network resources (company policies on this vary; be sure you understand them and comply).
5. **Respect for individuals, organizations, and other entities possibly affected by information posted on the Internet:**
    a. This includes you: think about all the searches you make and information you submit as being public and permanent, despite assurances to the contrary (for example, Facebook pages).
    b. Consider the impression your Internet presence will make on potential future employers or others checking your background.
    c. Think carefully before posting negative, personal, or potentially embarrassing photos or information about someone else or an organization. Check your facts, as damage can rarely be completely undone, and may in fact violate some law. A person's reputation, or even life, can be destroyed by such actions.
    d. When developing new friendships with others over the Internet, do not mislead them by pretending to have an age, gender, or background that you do not (obviously this does not include role-playing games).

Questions from Fall 2011, when Facebook made an update which affected users' security settings without user knowledge, and it seemed everyone was plagiarizing info from the Internet.

3. a. **Scenario:** Social networking sites such as *Facebook* have changed the way millions of individuals and organizations present and exchange information about themselves. Periodically these sites, as well as traditional email providers, may perform updates that result in a change in the security settings of users, or which affect user privacy in other ways. If the users are unaware of the impact of these changes, they may assume that the privacy settings they selected are still in place. In many cases, users pay nothing for the services offered by such sites. Do social networking or email service providers have any obligation to inform users or resolve problems due to changes affecting data privacy or security, given that they provide the service free of charge?

Assume that you are the Chief Technical Officer of an organization such as *Facebook*. For this scenario, present:

- At least **three** arguments explaining why you think that your organization has NO responsibility for security issues related to updates.
- At least **three** arguments why you think your organization has some responsibility, based on consideration of ethical computing standards. Use the guidelines in the outline to support your answer.

b. **Scenario:** Easy access to abundant information on the Internet has blurred the boundary lines of intellectual or artistic property ownership for many people. In order to answer previous questions about the history of computing, you may have looked up some information yourself using a site such as *Wikipedia*. Often no author is listed on these sites, which may give the impression that there is no one to credit for the ideas. Sometimes people include the information from these sites, literally word for word, in their own research papers or other assignments, rather than expressing the ideas in their own words and citing sources. If the website is freely accessible to everyone and the author is anonymous, is there anything wrong with using the information as if it were your own?

For this scenario, present:

- At least **three** arguments why you might justify presenting the information as your own ideas.
- At least **three** arguments why doing this might not be following ethical computing standards. Use the guidelines in the outline to support your answer.

Questions from Spring 2011, when Apple was saving map location info, and hackers broke into the Sony database.

3. a. **Scenario:** Assume that you work for a company which manufactures mobile devices requiring the collection of GPS data to support many location-dependent apps (such as maps, for example). Most customers are unaware that this data is being collected and saved. The data collection originally was not intended to track the movements of individuals, according to your company. However, it is large, not encrypted, and can be analyzed over time to provide a pattern of a person's locations. One third-party company would like to purchase the data collected by these devices for the purpose of targeted advertising, and assures your company that any identifying information tied to an individual would be deleted. Yet another company wants to buy the location data from you for the purpose of pricing auto insurance. You are a key person in making these decisions. Is there anything wrong with selling the information to other companies? For this scenario, present:

- At least **three** arguments why you might justify this action.
- At least **three** arguments why doing this might not be following ethical computing standards. Use the guidelines in the outline to support your answer.

b. **Scenario:** As an accomplished systems and network programmer, you also happen to be part of a shadow online hacking group made up of members from around the world. Members of the group share tips and challenge each other to perform increasingly difficult tasks of breaking into computer or network resources of individuals, organizations, or government entities--just for the prestige. You are especially proud of your recent work accessing personal and credit-card data for Sony PlayStation Network consumers, and hope that the publicity of your actions will cause companies to take greater precautions in securing their data. Although you realize a company's losses from such a security breach could run into the billions of dollars, you do not plan to use this information for your own personal gain. You take personal pride in breaking in without malicious intent or creating damage, and assume that others in this elite hacking group do the same. Is there anything wrong with your actions? For this scenario, present:

- At least **three** arguments why you might justify your actions.
- At least **three** arguments why doing this might not be following ethical computing standards. Use the guidelines in the outline to support your answer.

Question from Fall 2010, when the Wikileaks controversy started.

3. Scenario: Although you have a relatively low-level summer staff position in a company providing IT services for a branch of government, you have a great deal of access to information, much of it labeled confidential, in many government databases. You are approached by a third party website owner (similar to Wikileaks), who offers to pay you for downloading content from these databases, saying it's for the sake of free speech. You are a strong advocate of free speech, and also you may not be able to finish your degree without the money offered. Is there anything wrong with giving the information to this website? For this scenario, present:

- At least **three** arguments why you might justify this behavior (could be personal reasons, reasons based on some other ethical standard, etc.).
- At least **three** arguments why doing this might not be following ethical computing standards. Use the guidelines in the outline to support your answer.