SUNWAY

INT'L BUSINESS SCHOOL

Programme Name: **BCS HONS**

Course Code: **CSC 1015**

Course Name: **Ethics and Professional Conducts**

Open Book Examination

Date of Submission: **5/25/2021**

Submitted By:

Student Name: **CSC_1013_Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester: **Third Semester**

Intake: **September 2019**

Submitted To:

Faculty Name: **Khushal Regmi**

Department: **LMS**

1. **With the concept of End-User License Agreements, list out major ethical issues that are presented with EULAs.**

Answer:

A legally binding agreement between the owner of a product and the end-user more specifically, a contract between the product's licensor and the licensee is known as an End-User License Agreements

With the concept of End-User License Agreements, list of major ethical issues that are presented with EULAs are given below:

- Is it ethical to buy software with an educational license and then use it for corporate or commercial purposes later?
- Is it ethical to sell my older version of software after buying a newer version?
- Is it ethical to write an End-User License Agreement that is so lengthy that no one reads it?
- Is it ethical for me to use graphics, fonts, and other stock files that come with a software program in my commercial designs?
- Is it ethical to distribute software-generated works without paying additional license fees?
- Is it ethical to sell an unwanted software program to another person?

2. **Professional ethics is concerned with the standards and moral conduct that govern the profession and its members. List out the especial aspects of professional ethics which should apply to professionals as well as to ordinary individuals.**

Answer:

As we know, Professional ethics are a set of standards that are used for making decisions in the workplace. The especial aspects of professional ethics which should apply to professionals as well as to ordinary individuals are Given Below:

- **Teamwork**

a professional should be a team worker, helpful and confident, and also should displays a customer service attitude, and seeks continuous learning are some other especial aspects of professional ethics which should apply to professionals.

- **Justice**

It's also possible to think of the principle of justice (also known as "social justice") as stemming from the fundamental value of human autonomy. We all have (or should have) equal moral worth as humans because we all have (or should have) autonomy. As a result, proposals for unequal treatment of people must bear the burden of proof once more. As a result, professionals must treat everyone equally.

- **Organizational Skills**

A professional can quickly and easily find what is needed. Your work area should be neat and organized, and your briefcase should contain only what is needed for your appointment or presentation.

- **Appearance**

A professional is neat in appearance. Be sure to meet or even exceed the requirements of your company's dress code, and pay special attention to your appearance when meeting with prospects or clients, and take your cue from the way they dress.

- **Social Responsibility**

Employees can be socially responsible by making decisions that enhance the welfare of the people around them. Socially responsible behavior enhances teamwork and improves the overall productivity of the organization. Effective managers perform business and social audits to obtain an over-all picture of how their team is performing. The scope for social responsibility extends beyond the workplace as well. People who are socially responsible work toward developing their communities and neighborhoods.

- **Reliability**

As a professional, you will be counted on to find a way to get the job done. Responding to people promptly and following through on promises in a timely manner is also important, as this demonstrates reliability. It's about meeting expectations, which requires effective communication skills. Never assume. Clarify everything, especially when things change, to make sure you are always on the same page as your customer, and to eliminate nasty surprises.

Some other aspects of professional ethics which should apply to professionals as well as to ordinary individuals are Maintain confidentiality in professional relationships, fulfill commitments in a reliable, responsive and efficient manner, be fully accountable for actions, use of resources and financial dealings, Avoid potential or apparent conflicts of interest and show respect and understanding toward all people and honor diversity.

3. With the concept of Digital Divide explain the concern growing in the society.

Answer:

The digital divide is the gap that has been created between those who have access to technology, those who do not have access and those with limited access. The digital divide has created a new distinction basis in the society that has critically influenced daily operations and livelihood of persons in globally. The digital divide has contributed significantly to stratification in the community whereby there arises a class of persons with access to the internet and another class unable to use the ICT services either due to affordability issues or literacy levels. Some other factors that contribute to the digital divide in the society include age, race, and ethnicity. The internet offers a rich reservoir of information and knowledge. Skills and expertise are well organized and conveyed over the internet making the use of computers to be a ubiquitous activity in the developed world. The access and availability of ICT have been associated with academic success and robust research activities since users can quickly make references. The digital divide has led to a rise of new alignments in the community whereby people are classified depending on ability to access internet services this is coupled with associated benefits, and therefore those with limited access to technology continue to lag behind in development matters. People in rural areas who do not have access to the Internet are cut off from the rest of the world. Disconnected urban people experience something similar, which leads to social isolation.

4. **With the concept of Tiered password systems, explain the AAA of Password Security.**

Answer:

Authentication, authorization, and accounting (AAA) is a security framework that controls access to computer resources, enforces policies, and audits usage. AAA and its combined processes play a major role in network management and cybersecurity by screening users and keeping track of their activity while they are connected.

Authentication involves a user providing information about who they are. Users present login credentials that affirm they are who they claim. As an identity and access management (IAM) tool, a AAA server compares a user's credentials with its database of stored credentials by checking if the username, password, and other authentication tools align with that specific user.

Authorization follows authentication. During authorization, a user can be granted privileges to access certain areas of a network or system. The areas and sets of permissions granted a user are stored in a database along with the user's identity. The user's privileges can be changed by an administrator. Authorization is different from authentication in that authentication only checks a user's identity, whereas authorization dictates what the user is allowed to do.

Accounting keeps track of user activity while users are logged in to a network by tracking information such as how long they were logged in, the data they sent or received, their Internet Protocol (IP) address, the Uniform Resource Identifier (URI) they used, and the different services they accessed. Accounting may be used to analyze user trends, audit user activity, and provide more accurate billing. This can be done by leveraging the data collected during the user's access. For example, if the system charges users by the hour, the time logs generated by the accounting system can report how long the user was logged in to the router and inside the system, and then charge them accordingly.

So in simple, AAA is a standard based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization) and capture the actions performed while accessing the network (through accounting).

5. **Copyright law addresses the ownership of Intellectual Property. Explain the brief about Copyright and write down the FIVE (5) exclusive rights that copyright owners enjoy.**

Answer:

A copyright is a formal declaration that the owner is the only one with the right to publish, reproduce, or sell a particular artistic work. The protection of a copyright is granted by the government, and covers original literary (writings), dramatic (stage and film) musical, artistic, and other creations. To explore this concept, consider the following copyright definition.

Therefore, five exclusive rights that copyright owners have are given below:

- **The right to create derivative works** like sequels, spin-offs, translations, and other forms of adaptation. The derivative work right grants the copyright owner the ability to control the transformation of their works into new works.

- **The right to reproduce works**. The reproduction right grants the copyright owner the ability to control the making of a copy of the work. It is arguably the most important of the rights as it is implicated in most copyright infringement disputes

- **The public performance right** grants the copyright owner the ability to control the manner in which a work is publicly performed. The performance right applies to all works that can be performed, except for sound recordings. Some activities that implicate the public performance right include showing a motion picture in a public area or streaming movies, sports events, concerts or music over the internet.

- **Owners of rights in sound** recordings have the exclusive right of public performance by means of digital transmission. This enables, for instance, sound recording owners to license their work to streaming music services. This right only applies to sound recordings.

- **The distribution right grants** the copyright owner the ability to control the manner in which a work or a copy of a work is transferred to others, whether by sale, rental, lease, or lending. This right allows the copyright holder to not only prevent the distribution of unauthorized (i.e., infringing) copies of a work, but also allows the copyright holder to control the unauthorized distribution of authorized copies.

6. **IT security is a set of cyber security strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. Explain the threats to IT Security.**

Answer:

The threats to IT Security are:

- **Computer virus**

A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process.

- **Denial of Service**

A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS. Several other techniques may be used, and some cyber attackers use the time that a network is disabled to launch other attacks

- **Data diddling**

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

- **Man in the Middle**

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

- **Phishing**

Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number.

- **Privilege misuse**

Privileged accounts can be compromised when credentials are misused or reused. The ability to detect lateral movement and suspicious or abnormal behavior in the network prior to exfiltration can defend against an insider threat.

- **Hackers and predators**

Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change, or destroy information as a form of cyber-terrorism. These online predators can compromise credit card information, lock you out of your data, and steal your identity.

7. **Most organizations have a policy defining what they consider to be acceptable computer use where the public concern about the ethical use of information technology includes Email and Internet access monitoring. Explain the legal problems that arise from computer use.**

Answer:

the legal problems that arise from computer use are:

- unauthorized access
- unauthorized use of software
- inappropriate behavior
- inappropriate content
- allowing someone to illegally share personal data
- helping to steal financial information, such as credit card numbers or bank account details
- helping to illegally copy and distribute films, television programs and music
- extorting information or blackmailing someone
- misuse of internet

8. **Hacker ethic is a term for the moral values and philosophy that are common in hacker culture. Explain the Principles of Hacker Ethics.**

Answer:

As we know, Hacker ethic is a term for the moral values and philosophy that are standard in the hacker community.

The Principles of Hacker Ethics are

- **Above all else, do no harm**

Do not damage computers or data if at all possible

- **Information should be free**

Free information means the freedom to copy existing code and to share that information with others.

- **Computers can change your life for the better**

Hackers see computer programming not merely as a technical pursuit, but also as a tool for making the world a better place.

For example, hackers can write code to automate redundant tasks and they spread free information with the goal of improving the quality of human life

- **Hackers should be judged by their hacking, not based on degrees, age, race, sex, or position**

Hackers judge each other by the quality of their code. A hacker doesn’t need permission to hack. Your ability is not defined by who you know, or your expensive computer science degree.

- **Be wary of authority – encourage decentralization**.

Hackers promote decentralization in order to dilute the concentration of power and fight to redistribute that power among the many.

- **You can create art and beauty with a computer**.

Hacking is equated with artistry and creativity. Furthermore, this aspect of the ethos elevates it to the level of philosophy (as opposed to simple pragmatism), which is about humanity's search for the good, the true, and the beautiful (at least in some quarters).

- **Leave No Traces**

Leave no trace of your presence. Do not draw attention to yourself or your exploits. Keep quiet so that everyone can appreciate what you've got. This is an ethical principle in the sense that the hacker follows it not only to protect himself, but also to protect other hackers from being caught or losing access.

9. **Cyber Crimes is committed through the Internet and many web sites educate users about cybercrime and cybercriminals. Cybercrimes can be committed for the sake of recognition and also for the desire of making quick money by youngsters. Explain the types of Cybercrime**

Answer:

As we know, Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
the types of Cybercrime are:

- **Cyberbullying**

Cyberbullying occurs when people use social media or the internet to intimidate, harass, threaten or belittle others.

- **Identity theft**

Identity thieves often use computers to steal and/or sell social security numbers, bank account information or credit card information. Though it is illegal to steal and use other people’s sensitive personal information, identity theft continues to grow in popularity, and it is rapidly becoming one of the most frequently perpetrated computer crimes.

- **Malware attacks**

A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.

- **Phishing**

A phishing campaign is when spam emails, or other forms of communication, are sent on mail, with the intention of tricking recipients into doing something that undermines their security or the security of the organization they work for. Phishing campaign messages may contain infected attachments or links to malicious sites. Or they may ask the receiver to respond with confidential information.

- **Distributed DoS attacks**

Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (internet of things) devices are used to launch DDoS attacks. A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests.

- **Web jacking**

Web jacking derives its name from “hijacking”. Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

- **Cyber stalking**

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn’t physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It’s an invasion of one’s online privacy.

10. **Businesses back up their data to enable its recovery in case of potential loss. Businesses also back up their data to comply with regulatory requirements. It’s all about recovery. Explain the prevention of Data Loss**

Answer:

Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. Once those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use. DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response. Data loss prevention strategies protect organizations against both data leakage and data loss. In a data loss event, something like a ransomware attack causes critical data to be lost. Data leakage is more likely to occur as sensitive information moves between an organization’s critical records systems, for example. Data loss prevention focuses on preventing both types of illicit data transfer outside organizational boundaries. DLP may help prevent theft or accidental disclosure by employees and other authorized users with access to sensitive information. All browsing, corporate communications, and related activities by internal employees should be monitored, and risky or non-productive activities should be blocked.

In simple, Data loss prevention is a package of processes and tools designed to see that critical information is not accessed, misused, or lost by unauthorized users

Thank You