Unit-7
Professional and Ethical Responsibilities

- Community values and the laws by which we live
- The nature of professionalism in IT
- Various forms of professional credentialing
- The role of the professional in public policy
- Maintaining awareness of consequences
- Ethical dissent and whistle-blowing
- Codes of ethics, conduct, and practice (IEEE, ACM, SE, AITP, and so forth)
- Dealing with harassment and discrimination

Community values and the laws by which we live

- Ethics and laws are found in virtually all spheres of society. They govern actions of individuals around the world on a daily basis.
- They often work hand-in-hand to ensure that citizens act in a certain manner, and likewise coordinate efforts to protect the health, safety and welfare of the public.
- Though law often embodies ethical principles, law and ethics are not co-extensive.
- Based on society's ethics, laws are created and enforced by governments to mediate our relationships with each other, and to protect its citizens.
- While laws carry with them a punishment for violations, ethics do not. Essentially, laws enforce the behaviors we are expected to follow, while ethics suggest what we ought to follow, and help us explore options to improve our decision-making.

The nature of professionalism in IT

- Profession is any type of work that needs special training or a particular skill, often one that is respected because it involves a high level of education. Ex: Engineer, lawyers, doctors, dentists, accountants, architects & etc.
- Professionalism may be considered as behaving in an appropriate manner and adhering to accepted principles and practices.
- It is not only vital in the field of Information Technology but it is also very important in other fields. Some of the key aspects of IT Professionalism are competence in IT, knowledge, various skills such as soft skills, ethical behavior and certification.

Why IT professionalism is needed and why is it important?

- In order to enhance the growth and add value to an organization.
- It helps to provide better services to clients.
- It increases trust with employers and employees within an organization.
- Create company's own brand value.
- IT professionalism forms the pillar for company's own vision and mission.
- It improves customer satisfaction.

Nature of IT Profession

1. Self-directed & continuous learning about new technologies.
2. Communication skills & language proficiency.
3. Has honesty and performs his/her duties

4. Responsible and dedicated towards work.
5. Organizational skills.
6. Team contribution and leadership.
7. Has self-respect and treats others with respect.
8. Critical thinking and decision making
9. Customer relations
10. Long working hours and stress management
11. Competitive working environment with multi skilled colleagues

Various forms of professional credentialing

- A credential is a piece of any document that details a qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so.
- Examples of credentials include academic diplomas, academic degrees, certifications, security clearances, identification documents, badges, passwords, user names, keys, powers of attorney, and so on.
- Professional credentialing is the process by which a person proves that he or she has the knowledge, experience and skills to perform a specific job and the tasks in which they have been trained.
- The proof comes in the form of a certificate which is earned by passing one or more exams that were developed by an organization or association that monitors and upholds the prescribed standards for the particular industry involved.

Various forms of professional credentialing

Diplomacy

- In diplomacy, credentials, also known as a letter of credence, are documents that ambassadors, diplomatic ministers etc. provide to the.
- It contains a request that full credence be accorded to his official statements. Until his credentials have been presented and found in proper order, an envoy receives no official recognition.

Medicine

- In medicine, the process of credentialing is a detailed review of all permissions granted a medical doctor, physician, assistant or nurse practitioner at every institution at which he or she has worked in the past, to determine a risk profile for them at a new institution.

Information technology

- Information systems commonly use credentials to control access to information or other resources.
- The classic combination of a user's account number or name and a secret password is a widely used example of IT credentials.
- An increasing number of information systems use other forms of documentation of credentials, such as biometrics (fingerprints, voice recognition, retinal scans), public key certificates, and so on.

Cryptography

- Credentials in cryptography establish the identity of a party to communication. Usually, they take the form of machine-readable cryptographic keys and/or passwords. Cryptographic credentials may be self-issued, or issued by a trusted third party.

Operator licensing.

- Operators of vehicles such as automobiles, boats, and aircraft must have credentials in the form of government-issued licenses in many jurisdictions.
- Often the documentation of the license consists of a simple card or certificate that the operator keeps on his person while operating the vehicle, backed up by an archival record of the license at some central location.
- Licenses are granted to operators after a period of successful training and/or examination.

Journalism

- In many democratic nations, press credentials are not required at the national or federal level for any publication of any kind. However, individual corporations, and certain government or military entities require press credentials, such as a press pass, as a formal invitation to members of the press which grants them rights to photographs or videos, press conferences, or interviews.

Titles

- Titles are credentials that identify a person as belonging to a specific group, such as nobility or aristocracy, or a specific command grade in the military, or in other largely symbolic ways.
- They may or may not be associated with specific authority, and they do not usually attest to any specific competence or skill (although they may be associated with other credentials that do). A partial list of such titles includes
    - Personal titles, such as Lord, Knight, Right Honorable, indicating an earned or inherited rank or position within a formal power structure.
    - Command ranks, such as Captain, Sergeant, etc., indicating likewise a very specific position in a command hierarchy, e.g. police rank or military rank;
    - An academic degree or professional designation such as PhD, M.D., whether this be purely honorary or symbolic, or associated with credentials attesting to specific competence, learning, or skills.
    - Citizenship, as in the case of passports and birth certificates.

The role of the professional in public policy

- Public policy is a governmental decision to pursue a specific course of action in order to solve a problem or achieve a goal.
- More importantly, these governmental decisions express certain values and beliefs about different groups of people in society that impact policy design.
- Public policy professionals should have strong problem-solving, presentation, and oral and written communication skills.

Roles

Public Administration

- Public policy helps to learn to plan, implement, and assess programs.
- They gain the skills needed to lead multidisciplinary teams, train employees, and allocate resources.
- They also learn to align an organization's policies with government regulations and standards.

Policy Analysis

- Developing an understanding of the legislative process, including how social, political, economic, and technological factors affect government regulations and laws.
- Public policy professionals analyze the effects of public policies on individuals and communities. That also helps to guide policy formation by examining key legislative and executive institutional objectives.

Communication

- Communication skills enables to convey information clearly and persuasively in written, oral, and multimedia forms.
- Public policy professionals must communicate complex and technical ideas to individuals and teams. They also need to tactfully engage with government officials and community members to cultivate productive relationships.

Ethical Leadership

- Public policy professionals must be able to assess the ethical implications of individual, organizational, and social actions. They analyze a leader's decisions, including how external and internal pressures affect decision-making processes.

Strategic Decision-Making

- Public policy professionals may be responsible for making decisions that have widespread and long-lasting effects.
- They should identify the most important features of a decision based on setting and context.
- They must also evaluate the psychological factors that impact a decision's quality.

Maintaining awareness of consequences

- Cybersecurity is a global phenomenon representing a complex socio-technical challenge for governments, but requiring the involvement of individuals.
- Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness remains limited.
- Almost everybody has heard of cybersecurity, however, the urgency and behavior of persons do not reflect high level of awareness.
- The Internet is all too often considered as a safe environment for sharing information, transactions and controlling the physical world.
- Yet, cyberwars are already ongoing, and there is an urgent need to be better prepared. The inability to frame cybersecurity has resulted in a failure to develop suitable policies.

Best practices for maintaining awareness

Implement basic cyber security training

- Conducting training sessions will ensure that employees use approved software, and have strong passwords.
- We could also look at implementing common sense practices surrounding technology access

Implementing secure technologies and following best practices

- Implementing the secure technologies reduces the risks of data loss in an organization.
- And we should always follow the best practices of the technologies to make good use of them.

Have a data backup and recovery strategy

- Many businesses don’t have a procedure or back-up plan, if their data get lost or damaged.
- With more and more businesses relying on the cloud, it’s crucial to ensure cloud-based data is adequately protected or not.

Detect and plan for what you can’t prevent

- Hackers will always try and find a vulnerability, and when they do, we need to make sure we have the resources and knowledge to detect their activities as quickly as possible.
- This way, you can contain the damage and get back to normal business without experiencing a massive loss event.

Ethical dissent and whistle-blowing

- Ethical dissent likely starts as the result of an employee noticing that things are not what they ought to be, and then attempting to get them changed by talking to people in the organization.
- It can end easily, with changes made quickly, or it can end by involving an unfolding number of agencies, lawyers, legal systems, and public proceedings.
- Sometimes, the direction it takes after the beginning is in your own hands.
- But ethical dissent does not need to go as far as making public allegations about wrongdoing in your company.
- It can involve as little as making a well-supported suggestion that policy be changed in your organization.
- Ethical dissent becomes whistleblowing when you make your dissent public by going outside the organization and contacting others such as media or any government agencies to convince them to help you reform the organization.

- Whistle blower is a person who exposes the misconduct or illegal activities occurring in an organization.
- The matters that are of substantial important to public interest only fall under the whistle blowing. It can also be done by a member or a former member of an organization.

Codes of ethics, conduct, and practice (IEEE, ACM, SE, AITP, and so forth)

IEEE: Institute of Electrical and Electronics Engineers.
ACM: Association for Computing Machinery
SE: Software Engineering
AITP: Association of Information Technology Professionals

- A number of resources help IT professionals searching for ethical guidance within the scope of their job duties.
- For example, IEEE has a code of ethics for its members; the Association of Information Technology Professionals (AITP) has a code of ethics and standards of conduct; and SANS has published an IT code of ethics.
- There are other examples beyond these three, and many elements in these codes could be useful to higher education IT professionals.
- Among other elements that describe ethical behavior in the profession, in general these codes assert that IT professionals need to commit to:
    - Integrity
    - Competence
    - Professional responsibilities
    - Work responsibilities
    - Societal responsibilities

Dealing with harassment and discrimination

- Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person.
- Online threats and mean, aggressive, or rude texts, tweets, posts, or messages all count. So does posting personal information, pictures, or videos designed to hurt or embarrass someone else.
- Cyberbullying also includes photos, messages, or pages that don't get taken down, even after the person has been asked to do so. In other words, it's anything that gets posted online and is meant to hurt, harass, or upset someone else.
- Intimidation or mean comments that focus on things like a person's gender, religion, race, or physical differences count as discrimination, which is against the law in many states. That means the police could get involved, and bullies may face serious penalties.

What Can I Do About Cyberbullying?

1. **Tell someone**. Most experts agree: The first thing to do is tell an adult you trust. This is often easier said than done. People who are cyberbullied may feel embarrassed or reluctant to report a bully. Some may hesitate because they're not 100% sure who is doing the bullying. But bullying can get worse, so speak up until you find someone to help. Sometimes the police can track down an anonymous online bully, so it's often worthwhile to report it.
2. **Walk away**. Ignoring bullies is the best way to take away their power, but it isn't always easy to do — in the real world or online.
3. **Resist the urge to retaliate or respond**. Walking away or taking a break when you're faced with online bullying gives you some space so you won't be tempted to fire back a response or engage with the bully or bullies. Responding when we're upset can make things worse.
4. **Report Harassment** Social media sites take it seriously when people post cruel or mean stuff or set up fake accounts. If users report abuse, the site administrator may block the bully from using the site in the future. You can report to the police about the activities done by some one on the internet if things are getting serious.
5. **Block the bully**. Most devices have settings that let you electronically block the bully or bullies from sending notes. If you don't know how to do this, ask a friend or adult who does.

6. **Be safe online**. Password protect your smartphone and your online sites, and change your passwords often. Be sure to share your passwords only with your parent or guardian. It's also wise to think twice before sharing personal information or photos/videos that you don't want the world to see.