

**CYS 2310**  
**Policy, Legal, Ethics and Compliance**

**Lecture #4**  
**Cybersecurity Ethics**

## Learning Objectives:

Upon completion of this lecture, you will be able to:

- ✓ Understand Significance of Cybersecurity Ethics.
- ✓ Recognize Cyber Security Ethical Issues.
- ✓ Learn about Common Ethical Challenges.



## Introduction

- Cyber security Ethics play a key role in all fields of work, more importantly in professions that affect the lives of others.
- Ethics is of utmost importance when applied to cyber security as seemingly unimportant actions can lead to consequences for the professionals and the organizations both they work for.
- Thus, cyber security experts can figure out what is expected of them professionally by understanding the rules of ethical behaviour.

## Significance of Cybersecurity Ethics

- In cyber attacks, the targeted data is usually very sensitive and personal.
- It is necessary that the employees working in the field of cyber security have a strong sense of ethics and respect for the privacy of customers as cyber security professionals have access to the sensitive personal data.
- It is very necessary that the cyber security professional can determine what is in the best interest of customers and the company as a whole.

## Cyber Security Ethical Issues

- Ethical issues refer to the consequences, whether damages or benefits, that can come from the choices of cyber security professionals.
- In the same way, ethical issues take place in cyber security too, and below are some of the key issues:
  - Harm to privacy
  - Harm to property
  - Cyber security interests

## Common Ethical Challenges

- Following challenges are faced by cyber security professionals on a daily basis:
  - Ethical challenges in confidentiality
  - Ethical challenges in threats
  - Ethical challenges in network monitoring and user privacy

# Review

- **Significance of Cybersecurity Ethics**
- **Cyber Security Ethical Issues**
- **Common Ethical Challenges**

# End of Lecture