Miami Dade College

Course Description

IS3215 |Ethics in CyberSecurity | 4.00 credits

This course provides the study of the risk factors for digital and ethical misconduct and it explores ethics, relevant laws, regulations, policies, standards, moral, and social issues and responsibilities faced by CyberSecurity professionals. Coverage includes examination of CyberSecurity policies; Federal Laws and Authorities and International Standards; ethical and legal compliance and enforcement; business issues; contractual management of assets and liabilities; and issues involving privacy, disclosure, free speech and individual rights.

Course Competencies:

Competency 1: The student will demonstrate an understanding of policy, legal, ethics, and compliance by:

1. Describing the applicable laws and policies related to cyber defense and identify the major components of each, including data at rest (storage) and data in transit (transmission of data).
2. Describing responsibilities related to data handling concerning legal, ethical and agency auditing issues.
3. Describing how the various types of legal disputes (civil, criminal, private) affect the evidence used to resolve them.
4. Describing current events in Cybersecurity law and ethics, including:
    - a. Computer Security Act
    - b. Sarbanes-Oxley Arc
    - c. Gramm-Leach-Bliley Act
    - d. Privacy Acts: COPPA, HIPAA, and FERPA
    - e. USA Patriot Act
    - f. Americans with Disabilities Act, Section 508
    - g. Other Federal laws and regulations
5. Describing Payment Card Industry Data Security Standard (PCI DSS) and protection issues
6. Describing Bring Your Own Device (BYOD) issues and management
7. Describing state, local, federal, and international jurisdictional issues

Competency 2: The student will demonstrate an understanding of CyberSecurity Ethics by:

1. Describing how ethics is involved with CyberSecurity in a global perspective
2. Describing the ethical obligation to provide CyberSecurity
3. Describing rights, rules, and responsibilities for CyberSecurity personnel
4. Describing and determining appropriate action when faced with ethical issues, including:
    - a. Incident response and disclosure to colleagues and consumers of breaches
5. To what extent should a breach be investigated
    - a. The actions a business should take if it suffers an incident
    - b. The information that must be shared with stakeholders
    - c. Determining steps to take to prevent future breaches
    - d. Encryption Issues:
        - i. The rights and obligations involved when the government requests encrypted information from a business
        - ii. The responsibility for encrypting information stored within your business.
    - a. Roles and Responsibilities:
        - I. The roles and responsibilities associated with the IT department.
        - II. The extent IT staff, management, and managers are responsible for data breaches
        - III. The level of personal responsibility of other staff members (not IT) for breaches that result from their actions or inaction, such as falling prey to a phishing attack or unwittingly giving access to company information
6. Describing tools that help provide ethical decisions

Competency 3: The student will demonstrate an understanding of Cybercrime by:

1. Describing how the Internet (Cyber Environment) is used for Cybercrime, Cyber- stalking, and other abusive behaviors
2. Evaluating the effectiveness of CyberSecurity in preventing crime and abuse
3. Describing the types, incidences, and impacts of computer crime, including:
    a. Intrusions
    b. Ransomware
    c. Espionage
    d. Intellectual Property Theft
    e. Fraud
    f. Financial Theft
4. Differentiating illegal and unethical behavior, such as:
    a. Cyber stalking
    b. Cyberbullying
    c. Sexual exploitation
    d. Identity theft
    e. Cyber-assisted crimes
    f. Cyber terrorism
5. Examining current trends in computer crime and potential avenues of computer crimes
6. Performing legal research of case law interpreting CyberSecurity regulations
7. Describing applicable CyberSecurity laws andcompliance issues

Competency 4: The student will demonstrate an understanding of the legal, ethical, and moral issues involved with CyberSecurity by:

1. Describing how laws, ethics, morality, protection of rights, and standards of behavior are involved in cyber security
2. Describing basic ethical standards for technology, including: codes of conduct, industry practices, and professional responsibility
3. Analyzing the social impact of technology and formulating policies for its ethical use
4. Identifying ethical issues specific to CyberSecurity
5. Discussing the issues of free speech, privacy, intellectual property rights, fair use, acceptable use, and content control and moderation
6. Identifying the parties involved and describing their roles, rights, duties and responsibilities
7. Describing the legal and ethical issues of acquiring, storing, and securing digital information
8. Describing the purpose of laws, regulations, and policies enacted to protect and preserve rights

Competency 5: The student will demonstrate an understanding of the statutes, laws, and regulations that impact CyberSecurity by:

1. Describing relevant U.S. laws, including:
    a. Electronic Communications Privacy Act (ECPA)
    b. Computer Fraud and Abuse Act (CFAA)
    c. Cyber Intelligence Sharing and Protection Act (CISPA)
    d. Children's Online Privacy Protection Act (COPPA)
2. Describing information security and privacy mandates such as:
    a. The Gramm-Leach-Bliley Act (GLBA)
    b. Health Insurance Portability and Accountability Act (HIPAA)
    c. Federal Information Security Management Act (FISMA)
    d. General Data Protection Regulation (GDPR)

    e. Payment Card Industry Data Security Standard (PCI-DSS)

3. Identifying legal issues about CyberSecurity.
4. Describing legal terminology about CyberSecurity compliance and enforcement, including:
    a. Causation
    b. Proof
    c. Foreseeability
    d. Negligence
    e. Assumption of risk
    f. Privacy of contract
5. Describing civil law and procedure, as it relates to CyberSecurity
6. Describing criminal law and procedure as they relate to cybercrime

Competency 6: The student will demonstrate an understanding of legal compliance and enforcement of CyberSecurity laws, policies, and policy development by:

1. Describing standard regulatory and compliance mandates
2. Describing methods of assuring employee
3. compliance with an organization’s rules, policies and codes of conduct
4. Developing security policies with manageability, defensibility, and recourse
5. Describing the risks and legal impacts of current and emerging technologies on information assets and individuals (human rights)
6. Describing methods of protecting an organization's information assets in contracts, agreements, employment policies, and terms of service
7. Describing e-Discovery and record retention laws and regulations, including organizational control methods to comply with retention requirements
8. Describing methods of protecting an organization’s intellectual property
9. Drafting an organization’s CyberSecurity policy

Competency 7: The student will demonstrate an understanding of CyberSecurity in the cloud by:

1. Describing cloud services, deployment models, security, and storage
2. Describing incident response techniques and evaluating suspected compromised virtual servers
3. Describing different methods for logging, monitoring, alerting, and troubleshooting virtual servers
4. Describing a secure network infrastructure
5. Describing identity and access management techniques for authorization and authentication system access
6. Describing data encryption solution for data at rest and in transit

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Formulate strategies to locate, evaluate, and apply information
- Demonstrate knowledge of ethical thinking and its application to issues in society