Virginia Western Community College
ITN 267
Legal Issues in Information Security

Prerequisites
ITN260

Course Description
Conveys an in-depth exploration of the civil and common law issues that apply to network security. Explores statutes, jurisdictional, and constitutional issues related to computer crimes and privacy. Includes rules of evidence, seizure and evidence handling, court presentation and computer privacy in the digital age.

Semester Credits: 3 Lecture Hours: 3 Lab/Clinical/Internship Hours: 0

Required Materials

Textbook:
Legal Issues in Information Security Second Edition, Joanna Lyn Grama, Jones & Bartlett Learning, Information Systems Security & Assurance Series. ISBN: 978-1-284-05474-3

Other Required Materials:
Students enrolled in this course will be provided handouts of case law to review in class

Course Outcomes

At the completion of this course, the student should be able to:

1 Legal System
1.1. Identify major national, state, and international laws that relate to information security.(PL7)
1.2. Understand the difference between law and ethics.
1.3. Understand the role of culture as it applies to ethics.
1.4. Understand the difference between Civil, Criminal, Tort, Private and Public laws as they apply to security and evidence.)
1.5. Understand the role copyright laws play in security.
1.6. Understand the role that the Freedom of Information Act of 1966 (FOIA) plays in security.
1.7. Understand the main elements of the Federal Privacy Act of 1974 as it applies to individual privacy and its subsequent impact upon security.
1.8. Understand the main elements of the Electronic Communication Privacy Act of 1986 as it applies to privacy and security.
1.9. Understand the main elements of the Computer Fraud and Abuse Act of 1986 as it applies to security.

1.10. Understand the main elements of the Computer Decency Act of 1987 as it applies to security.
1.11. Understand the main elements of the National Information Infrastructure Protection Act of 1996 as it applies to security.
1.12. Understand the main elements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as it applies to privacy and security.(PL1
1.13. Understand the main elements of the Economic Espionage Act of 1996 as it applies to security.
1.14. Understand the main elements of the Financial services Modernization Act of 1999 (Gramm-LEACH-Bliley) as it applies to privacy and security. (PL4)
1.15. Understand the main elements of the Security and Freedom through Encryption Act of 1999 as it applies to security.
1.16. Understand the main elements of the U.S.A. Patriot Act of 2001 as it applies to security. (PL9)
1.17. Understand the difference between policy and law.
1.18. Understand how ethical concepts apply to security.
1.19. Understand the main element of the Americans with Disabilities Act (Section 508),(PL1.19)
1.20. Understand the main elements of the Computer Security Act as it applies to security(PL3).
1.21. Understand the main elements of Sarbanes-Oxley as it applies to security. (PL3)
1.22. Understand the main elements of FERPA as it applies to security.(PL2)
1.23. Understand the main elements of COPPA as it applies to privacy.(PL5)
1.24. Understand the main elements of PCI DSS as it applies to security(PL6).

2. Rules of Evidence
2.1. Understand how role of evidence in both a criminal and civil case.
2.2. Identify and understand the different categories of evidence.
2.3. Understand when evidence is or is not admissible in court.
2.4. Understand the role of forensic standards as they apply to evidence gathering.
2.5. Understand the role of the first responders, investigators and crime scene technicians as they apply to evidence.
2.6. Understand the difficulty in recovering, documenting and preserving digital evidence.
2.7. Describe how the type of legal dispute (civil, criminal, and private) affects the evidence used to resolve it.

3. Evidence Seizure and Handling
3.1. Identify various laws and authorities and understand who has jurisdiction of a case.(PL8)
3.2. Identifying and understanding the steps in the investigative process.
3.3. Understand how to prepare a search warrant.
3.4. Understand rules of particularity and how they relate to evidence seizure and the search warrant.
3.5. Understand the process for seizing evidence in the execution of a search warrant.
3.6. Understand the value of cooperating witnesses and technical experts.
3.7. Describe the process of documenting the seized evidence through document tags, document logs, videotapes and photographs.
3.8. Describe the issues associated with maintaining an evidence chain of custody.

4. Court Presentation

4.1. Understand the trial process to include preliminary hearing, burden of proof and the role of the prosecutor and defense attorney.
4.2. Understand the role of the evidentiary witness and the expert witness.
4.3. Understand the qualifications required of an expert witness.
4.4. Identifying techniques for enhancing the credibility of a witness giving direct testimony.
4.5. Understand the tactics employed during cross examination.
4.6. Understand the value of notes and visual aids during court testimony in a computer crime case.

5. Privacy, Individual Rights, Free Speech and the Law
5.1. Understand privacy and its role in society.
5.2. Understand Individual rights and their basis in the constitution and the law.
5.3. Understand the balance between privacy in the work place and the needs of the organization.
5.4. Understand the balance between the need of the organization to protect its business and customer information and the need of law enforcement and the intelligence community.
5.5. Understand the relationship between free speech and the law as it applies to a web site and email.
5.6. Understand ethics as it applies to software licenses, corporate resources and malware.
5.7. Explain common practices employed to deter unethical or illegal behavior.
5.8. Explain the value of a code of ethics and its relationship to employee behavior and organizational liability.
5.9. Describe an employee's responsibilities related to the handling of information about vulnerabilities and the necessity for confidentiality.
5.10. Discuss issues relating to Bring Your Own Device (BYOD).(PL10)

Topical Description

Week	Topic	Reference (Chapter)
1	Information Security Overview	Ch 1
2	Privacy Overview	Ch 2
3	American Legal System	Ch 3
4	Criminal Law and Tort Law Issues in Cyberspace Information Security Governance	Ch 12-13
5	Security and Privacy of Consumer Financial Information Security and Privacy of Information Belonging to Children in Education Records Security and Privacy of Health Information	Ch 4-6
6	Corporate Information Security and Privacy Regulations Federal Government Information Security and Privacy Regulations State Laws Protecting Citizens Information and Breach Notification Law	Ch 5-9
7	Intellectual Property Law The Role of Contracts	Ch 10-11
8	Risk Analysis, Incident Response, and Contingency Planning Computer Forensic and Investigation	Ch 14-15

Individual Exam		

Notes to Instructors

none