Revised 8/2023

NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 267 – LEGAL TOPICS IN NETWORK SECURITY (3 CR.)

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. Total 3 hours per week.

General Course Purpose

The purpose of this course is to train the student on legal, regulatory, and policy standards that impact his or her role as a network administrator or security professional. As such, there should be less of an emphasis on case law or precedent as found within business-oriented cyberlaw courses, and more of an emphasis on legal requirements, policy, and regulations that have direct impact on technical roles or responsibilities with safeguarding sensitive information to meet legal and regulatory compliance expectations.

Course Prerequisites/Corequisites

Ability to read and write at a college level.

Course Objectives

Upon successful completion of this course, the student will have a working knowledge of:

A. Legal statutes as they apply to network security
B. computer crime rules of evidence
C. evidence seizure, handling, and court presentation
D. privacy, individual rights, and free speech

Course Content

- Legal System
- Rules of Evidence
- Evidence Seizure and Handling
- Court Presentation
- Privacy, Individual Rights, Free Speech and the Law.

Student Learning Outcomes

1. Legal System (PLE)
   1.1. Identify major national, state, and international laws that relate to information security.
   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.

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.
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.
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)
1.20. Understand the main elements of the Computer Security Act as it applies to security.
1.21. Understand the main elements of Sarbanes-Oxley as it applies to security.
1.22. Understand the main elements of FERPA as it applies to security.
1.23. Understand the main elements of COPPA as it applies to privacy.
1.24. Understand the main elements of PCI DSS as it applies to security.

2. Rules of Evidence (PLE)
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 (PLE)
3.1. Identify various laws and authorities and understand who has jurisdiction of a case.
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 (PLE)
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 (PLE)
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).

CAE2Y Knowledge Unit Domain Index

KU Category	Course Content KU Mapping	CAE2Y KU Name	Description
Core Non-Technical CDE Knowledge	PLE	Policy, Legal, Ethics, and Compliance	Provide students with and understanding of information assurance in context and the rules and guidelines that control them.

NOTE: the course content KU mapping represents the KU Domain topic as shown in the Center of Academic Excellence (CAE) KU mapping matrix (Excel file).

Required Time Allocation per Topic

In order to standardize the core topics of ITN 267 so that a course taught at one campus is equivalent to the same course taught at another campus, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best as an integrated whole, often revisiting the topic several times, each time at a higher level. There are normally 45 student-contact-hours per semester for a three credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 3 = 45 hours. Sections of the course that are given in alternative formats from the standard 16 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The category, Other Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic	**Time in Hours**	**Percentages**
Legal System	8	18%
Rules of Evidence	8	18%
Evidence Seizure and Handling	8	18%
Court Presentation	3	7%
Privacy, Individual Rights, Free Speech, and the Law	6	13%
Other Optional Content (NIST Framework)	4	8%
Exams and Quizzes	8	18%
Total	45	100%