**Chapter 4 - Laws, Regulations, and Compliance**

* Categories of Laws
  + **Criminal law** - deals with crimes such as murder, robbery, assault, etc. Computer frauds fall under criminal laws.
  + **Civil law** - deals with society matters such as contract disputes, real estate transactions, employment matters, etc. Trademark and Patent law are civil laws that govern business transactions.
  + **Administrative law** - ensures civil and criminal laws are followed properly
* The Computer Fraud and Abuse Act (CFAA) was the first major piece of cybercrime-specific legislation in the United States.
* The Federal Information Security Management Act (FISMA), passed in 2002, requires that federal agencies implement an information security program that covers the agency’s operations. It also governs information security operations at federal agencies.
* Intellectual Property (IP)
  + **Copyright** - Copyright law guarantees the creators of “original works of authorship” protection against the unauthorized duplication of their work.However, copyright law protects only the actual source code and not the idea or process behind the software.
  + **Trademarks** - Provides protection for trademarks, which are words, slogans, and logos used to identify a company and its products or services. Trademarks do not need to be officially registered to gain protection under the law. You can use the ™ symbol to show that you intend to protect words or slogans as trademarks. If you want official recognition of your trademark, you can register it and use the ® symbol denoting registered trademark.
  + **Patents** - It protects the intellectual property rights of inventors. They provide exclusive usage rights to inventors for a period of 20 years from the time of the invention (from the date of initial application). Invention must meet three requirements, it must be new, useful and non-obvious.
  + **Trade secrets** - Filing a copyright or patent application requires that you publicly disclose the details of your work or invention. Plus they are valid for a limited time period. Trade secrets are not required to be registered with any entity and are kept secret by the organization.
* Licensing
  + **Contractual** license agreements use a written contract between the software vendor and the customer, outlining the responsibilities of each.
  + **Shrink-wrap** license agreements are written on the outside of the software packaging. They commonly include a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.
  + **Click-through** (also known as browser wrap) license agreement terms are included in the software documentation and need to be accepted at the time of Installation.
  + **Cloud services license** agreements take click-through agreements to the extreme. Legal terms are flashed at the time of registration and need to be accepted before being able to utilize cloud services.
* The European Union passed a new, comprehensive law covering the protection of personal information in 2016. The General Data Protection Regulation (GDPR) went into effect in 2018 and replaced the Data Protection Directive (DPD) on that date.
* GDPR is of particular concern when transferring information across international borders. Organizations need to adopt one of the below
  + **Standard contractual clauses** that have been approved by the EU
  + **Binding corporate rules** if the data is being shared between the internal units of the same firm. It is a difficult choice as the rules must be approved by every EU member nation where they will be used.
* In the past, the EU and US signed a safe harbor agreement called Privacy Shield. Organizations were able to certify their compliance with privacy practices through independent assessors and, if awarded the privacy shield, were permitted to transfer information. However, in 2020 the EU declared privacy shield invalid.
* The Bureau of Industry and Security (BIS) has the authority to regulate the export of encryption software. There was pretty strict regulation at the beginning.
* Administrative laws do not require an act of the legislative branch to implement but they are subject to judicial review and must comply with existing civil and criminal laws.
* California Consumer Privacy Act (CCPA) was the first US state law passed as a comprehensive privacy law modeled after GDPR.
* The Gramm–Leach–Bliley Act regulates financial institutions, regarding the way financial institutions can handle private information belonging to their customers.
* The Fourth Amendment to the U.S. Constitution states that the officers must obtain a warrant before searching a property.
* The Privacy act prevents government agencies from disclosing personal information of individuals.
* Children’s Online Privacy Protection Act (COPPA) was designed to protect the privacy of children using the internet. For Childrens below 13 years, parental consent must be taken before collecting any data other than basic information required to obtain the consent.
* Copyright protection generally lasts for 70 years after the death of the last surviving author of the work.