St. Francis Institute of Technology
(An Autonomous Institution)
AICTE Approved | Affiliated to University of Mumbai

A+ Grade by NAAC: CMPN, EXTC, INFT NBA Accredited: ISO 9001:2015 Certified

Department of Information Technology

A.Y. 2025-2026
Class: BE-IT A/B, Semester: VIII
Subject: Secure Application Development Lab

Student Name:**Keith Fernandes** Student Roll No:**25**

Experiment – 1: Study of different laws and standards of Cyber Security

Aim: To study of different laws and standards of cyber security

Objective: After performing the experiment, the students will be able to –

- To know Cyber security
- Read and understand Different cyber law and standards
- To understand the cyber Security

Lab objective mapped: To **apply** secure programming of application code

Prerequisite: Basic knowledge Information Security

Requirements: Personal Computer, Windows operating system browser, Internet Connection etc.
.

Pre-Experiment Theory:

What is Cyber Security?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Role of Cyber Laws in Cybersecurity

Cyber laws are integral to the use of the internet and serve a variety of purposes. Most of these laws are there to protect users from becoming victims of cybercrimes, while others are made to regulate the usage of the internet and computers in general. Cyber laws cover these three primary areas:

- **Fraud:** Cyber laws protect users from falling victim to online fraud. They exist to prevent crimes such as credit card and identity theft. These laws also declare federal and state criminal charges for anyone that attempts to commit such fraud.
- **Copyright:** Cyber laws also prevent copyright infringement and enforce copyright protection. They provide individuals and businesses with the right to protect their creative works and to profit from them.
- **Defamation:** Cyber laws are also enforced in online defamation cases, which provide individuals and businesses protection against false allegations made online that can be harmful to their reputations.

Cyber Security Laws in India

India has four predominant laws when it comes to cybersecurity:

- **Information Technology Act (2000):** Enacted by the parliament of India, the information technology act was made to safeguard the e-governance, e banking, and e-commerce sectors; but now, its scope has been enhanced to encompass all the latest communication devices.
- **Indian Penal Code (IPC) (1980):** This cybercrime prevention act has primary relevance to cyber frauds concerning identity theft and other sensitive information theft.
- **Companies Act (2013):** With the companies act enacted back in 2013, the legislature ensured that all the regulatory compliances are covered, including e-discovery, cyber forensics, and cybersecurity diligence. The Companies Act provides guidelines for the responsibilities of the company directors and leaders concerning confirming cybersecurity obligations.
- **NIST Compliance:** The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), contains all the guidelines, standards, and best practices necessary to responsibly address cybersecurity risks.

Procedure

- **Define Cyber Security.**

Cyber security is the practice of safeguarding digital systems, networks, devices, and data from unauthorized access, cyberattacks, or damage. It ensures the confidentiality, integrity, and availability of information in an increasingly connected world. This field involves deploying technologies, processes, and policies to protect against threats like hacking, malware, and data breaches. Cyber security is essential for individuals, businesses, and governments relying on digital infrastructure. It mitigates risks that could lead to financial loss, reputational damage, or compromised privacy. Key components include network security, application security, endpoint protection, and user education. Cyber security also involves monitoring and responding to incidents in real time to minimize harm. As cyber threats

evolve, so must the strategies to counter them, requiring constant updates and vigilance. Effective cyber security prevents unauthorized access to sensitive data, such as personal or financial information. It employs tools like firewalls, encryption, and intrusion detection systems to secure systems. Organizations often conduct risk assessments to identify vulnerabilities and implement safeguards. For individuals, cyber security includes using strong
passwords and avoiding suspicious links. The rise of remote work and cloud computing has made robust cyber security more critical than ever. It protects against disruptions that could halt business operations or compromise national security. Cyber security also fosters trust in digital platforms, enabling safe online transactions and communication.
Ultimately, cyber security is a shared responsibility, requiring collaboration between governments, organizations, and individuals. It addresses both external threats, like cybercriminals, and internal risks, such as employee negligence. Regular training and awareness campaigns help users stay informed about best practices. Compliance with standards like ISO 27001 enhances security frameworks. By prioritizing cyber security, society can safely leverage technology's benefits while minimizing its risks. Cyber security is not a one-time effort but an ongoing process to adapt to new challenges.

- **Discuss different types of Cyber threats. (minimum 5)**

1.Phishing
Phishing involves cybercriminals sending deceptive emails, text messages, or other communications that appear to come from legitimate sources. These messages trick users into providing sensitive information, such as login credentials or financial details. For example, an email may mimic a bank's branding to lure users into entering their account information on a fake website. Phishing attacks exploit human trust and often use urgent language to prompt quick action. They can lead to identity theft, financial loss, or unauthorized access to systems. Awareness and verification of sender authenticity are key to avoiding phishing scams. Regular training helps users recognize suspicious messages.

2.Malware
Malware, including viruses, ransomware, and spyware, is malicious software designed to infiltrate and harm systems. Viruses corrupt files, ransomware locks data until a ransom is paid, and spyware steals sensitive information. Malware often spreads through infected downloads, email attachments, or compromised websites. It can cause significant data loss, system downtime, or financial damage. For instance, ransomware attacks have cost organizations billions globally. Antivirus software, regular updates, and cautious downloading habits are essential defenses. Backing up data regularly can mitigate ransomware impacts.

3.Distributed Denial-of-Service (DDoS) Attacks
DDoS attacks flood a target system, server, or website with excessive traffic to overwhelm it and disrupt service availability. Cybercriminals use botnets—networks of infected devices—to generate this traffic. These attacks can cripple online services, such as e-commerce platforms or government websites, causing financial and reputational harm. DDoS attacks are often used as distractions for other cybercrimes. Mitigation includes using traffic filtering and scalable cloud-based protections. Organizations must monitor network traffic to detect and respond to unusual spikes quickly.

4.Man-in-the-Middle (MitM) Attacks

MitM attacks occur when attackers intercept communications between two parties to steal data or manipulate messages. For example, on unsecured Wi-Fi, hackers can capture sensitive information like passwords or credit card details. These attacks compromise data integrity and confidentiality, often going unnoticed by victims. Secure connections, such as those using HTTPS or VPNs, help prevent MitM attacks. Users should avoid public Wi-Fi for sensitive transactions and ensure end-to-end encryption is in place. Regular monitoring of account activity can detect unauthorized access.

5.SQL Injection

SQL injection exploits vulnerabilities in web applications by injecting malicious code into database queries. Attackers use this to access, modify, or delete sensitive data, such as user credentials or financial records. Poorly coded websites are prime targets, allowing hackers to bypass authentication or extract entire databases. SQL injections can lead to significant data breaches and system compromise. Developers must use parameterized queries and input validation to prevent these attacks. Regular security audits and patching of web applications are critical to reducing risks.

6.Password Attacks

Password attacks involve cybercriminals attempting to steal or guess user credentials to gain unauthorized access. Techniques include brute force, where attackers try multiple password combinations, or using stolen credentials from data breaches. Weak or reused passwords make accounts vulnerable. These attacks can lead to account takeovers, data theft, or further system exploitation. Strong, unique passwords and two-factor authentication (2FA) are effective countermeasures. Password managers help users maintain secure credentials without memorization.

- **What happen if anyone breaks a cyber-law?**

Breaking cyber laws can lead to serious legal, financial, and social consequences.
Offenders may face criminal charges, such as fines or imprisonment, depending on the severity of the crime. For instance, hacking into systems violates laws like the U.S. Computer Fraud and Abuse Act, which carries penalties of up to seven years in prison. Data breaches caused by negligence can result in hefty fines under regulations like GDPR, which can impose
penalties of up to €20 million or 4% of annual revenue. Organizations may also face lawsuits from affected individuals or businesses seeking compensation for damages.
Reputationally, companies that violate cyber laws often lose customer trust, leading to reduced
business and long-term financial losses. Regulatory bodies may impose sanctions, such as barring organizations from certain operations or requiring costly audits. Individuals involved in cybercrimes, like distributing malware, may face civil lawsuits or restrictions on future employment in tech-related fields. In cases of international cybercrime, offenders may be extradited to face charges in another country. Repeat offenders often receive harsher penalties,
including lifelong bans from certain professions.
The consequences extend beyond the offender, impacting victims who suffer data loss or financial harm. Cyber laws aim to deter such activities by holding perpetrators accountable. Enforcement agencies, like the FBI or Interpol, actively investigate cybercrimes, increasing the likelihood of prosecution. Compliance with cyber laws is essential to avoid these

repercussions and maintain a secure digital environment. Organizations and individuals must stay informed about applicable laws to avoid unintentional violations.

- **Importance of Cyber Law and standards**

Cyber laws and standards are vital for regulating the digital world and ensuring accountability. They establish legal frameworks to deter cybercrimes, such as hacking, identity theft, and data breaches. These laws protect individuals' privacy and sensitive information, fostering trust in digital platforms like e-commerce and online banking. Standards, such as
ISO 27001, provide guidelines for organizations to implement robust security measures, reducing vulnerabilities. Compliance with these standards helps prevent financial losses, which globally amount to billions annually due to cyber incidents.
Cyber laws also facilitate international cooperation to combat cross-border cybercrimes, as cybercriminals often operate across jurisdictions. They protect intellectual property, ensuring creators and businesses retain control over their digital assets. Standards like NIST's Cybersecurity Framework help organizations manage risks systematically, enhancing resilience. Cyber laws promote responsible digital behavior by educating users about legal and ethical online practices. Without these frameworks, the internet would be far more vulnerable to exploitation.
Moreover, cyber laws and standards ensure fair competition by regulating how businesses handle data and technology. They mandate transparency in data breaches, protecting consumers from harm. Compliance with standards can also enhance an organization's reputation, attracting customers and partners. By enforcing accountability, cyber laws deter malicious actors and encourage proactive security measures. Ultimately, they create a safer digital ecosystem, enabling innovation and trust in technology.

- **What are the areas involving in Cyber Law?**

Cyber law encompasses a wide range of legal domains related to digital activities. Data protection and privacy laws regulate how personal data is collected, stored, and shared, ensuring user rights. Cybercrime laws address offenses like hacking, phishing, and online fraud, imposing penalties for violations. Intellectual property laws protect digital content, such as software, music, and designs, from unauthorized use. E-commerce regulations govern online transactions, ensuring consumer protection and fair trade practices. Cybersecurity laws require organizations to secure systems against breaches and vulnerabilities.
Other areas include digital signatures, which validate electronic transactions and contracts legally. Online defamation laws tackle harmful or false content spread on digital platforms. Jurisdiction issues address challenges in applying laws across borders, critical for global cybercrimes. Telecommunications laws regulate internet service providers and network infrastructure operations. Emerging technologies, like artificial intelligence and the Internet of Things (IoT), are increasingly covered to address new legal challenges.
These areas collectively ensure a comprehensive legal framework for the digital world. They balance innovation with security, protecting users while enabling technological growth. Cyber law evolves to address new risks, such as those posed by quantum computing or deepfakes.
Understanding these areas helps individuals and organizations navigate legal obligations effectively.

- **What are Standards you study in Cyber Law?**

Cyber law incorporates various standards to ensure secure and compliant digital practices. ISO/IEC 27001 provides a framework for establishing and maintaining information security management systems. NIST Cybersecurity Framework offers guidelines for managing cyber risks, particularly in critical infrastructure sectors. GDPR sets stringent requirements for data protection and privacy for EU citizens, influencing global standards. PCI DSS ensures secure handling of payment card data, mandatory for businesses processing transactions. HIPAA protects sensitive health information in the U.S., enforcing strict compliance in healthcare.
Additional standards include CIS Controls, which offer prioritized security practices to mitigate common cyber threats. SOC 2 focuses on secure data management for service organizations, ensuring trust in cloud services. ISO 31000 provides a risk management framework applicable to cyber security contexts. COBIT aligns IT governance with business goals, enhancing security compliance. FedRAMP standardizes security for cloud services used by U.S. federal agencies.
These standards guide organizations in meeting legal and regulatory requirements while strengthening defenses. They promote consistency in security practices across industries and jurisdictions. Compliance with these standards often requires regular audits and certifications. Studying them in cyber law helps professionals understand best practices and legal expectations.

- **How to protect yourself on the Internet?**

Protecting yourself online requires proactive steps to secure your data and devices. Use strong, unique passwords for each account, ideally managed by a password manager. Enable two-factor authentication (2FA) to add an extra layer of security to your accounts. Avoid phishing scams by not clicking suspicious links or sharing sensitive information via email. Keep all software, including operating systems and apps, updated to patch security vulnerabilities. Install reputable antivirus software to detect and remove malware from your devices.
Use a Virtual Private Network (VPN) when accessing public Wi-Fi to encrypt your internet connection. Regularly back up important data to external drives or cloud services to recover from ransomware attacks. Limit personal information shared on social media to reduce the risk of identity theft or targeted scams. Verify website security by ensuring URLs start with HTTPS and display a padlock icon. Stay educated about cyber threats and practice safe browsing habits to avoid malicious sites.
Additionally, be cautious of unsolicited requests for personal information, even if they appear legitimate. Use secure payment methods for online transactions and monitor accounts for suspicious activity. Disable unnecessary device features, like location services, when not in use. Regularly review privacy settings on apps and platforms to control data sharing. By adopting these practices, you can significantly reduce your exposure to online risks.

Post-Experiments Exercise

Extended Theory: Nil

Results/Calculations/Observations:

Post Experimental Exercise-

Questions:

Discuss the real world incidence related to cyber threat?

Conclusion:

Explain the importance of cyber security laws and standards based on your learnings from this experiment.

References:

○ **https://www.udemy.com/course/secure-coding-secure-application-development/**

○ **https://kirkpatrickprice.com/blog/secure-coding-best-practices/**