AMC DENTAL COLLEGE AND HOSPITAL

ACADEMIC YEAR 2018-19

"Value added course in Learn to Deal on Cyber Space"

1. Nomenclature of the Course:

"Value added course in **Learn to Deal on Cyber Space"**

2. Background:

Cyber law essentially encompasses laws relating to electronic and digital signatures, cybercrimes, intellectual property, data protection and privacy . The major areas of cyber laws includes defamation, fraud, copy right harassment or stalking , trade secrets, freedom of speech, contracts and employment law.

3. Objectives of program

This comprehensive three-day course and workshop aim to equip participants with a deep understanding of cyber space security, practical skills in mitigating cyber threats, incident response strategies, ethical considerations, and future trends. Interactive workshops, case studies, and discussions ensure active engagement and practical application of knowledge.

4. Who Can Participate in the Course

Any interested students, post graduates, faculties at Amc Dental College and Hospital can participate in the course.

5. Duration of the Course

The total duration of the course is 18 hours

6. Admission Process of the Course

All students at Amc dental college are eligible to the course.

7. Course Fee:

There will be no fee for the course

8. Award of Certificate

The students completing 80 % attendance will be awarded the course completion certificates.

9. Course Content

Day 1: 8 hours

Understanding Cyber Space Security

Session 1: Introduction to Cyber Space Security

- **Overview of Cyber Security**: Defining cyber space security, its scope, and its importance in the digital age.
- **Threat Landscape**: Understanding prevalent cyber threats, including malware, phishing, ransomware, and social engineering attacks.

Session 2: Cyber Threats and Attack Vectors

- **Types of Cyber Attacks**: Exploring different attack methodologies with case studies and examples.
- **Vulnerabilities and Exploits**: Understanding how attackers exploit weaknesses in systems and networks.
- **Identifying Attack Vectors**: Analyzing various entry points for cyber attacks and their implications.

Session 3: Cyber Security Measures and Best Practices

- **Defensive Strategies**: Discussing preventive measures and best practices in cyber security.
- **Security Hygiene**: Emphasizing the importance of strong passwords, regular updates, and safe online behavior.
- **Encryption and Authentication**: Explaining the significance of encryption and multi-factor authentication for data protection.

Day 2: 4 hours

Session 4: Cyber Security Tools and Technologies

- **Security Software**: Exploring various cyber security tools, including antivirus software, firewalls, and intrusion detection systems.
- **Security Assessments**: Understanding the role of vulnerability assessments and penetration testing in identifying and addressing weaknesses.

Session 5: Interactive Workshop: Hands-on Cyber Security Practices

- **Simulated Scenarios**: Conducting interactive exercises to simulate cyber security incidents.
- **Practical Implementations**: Guided sessions on implementing security measures and responding to potential threats.

Day 3: 6 hours

Proactive Measures and Incident Response

Session 6: Proactive Cyber Security Measures

- **Threat Intelligence and Analysis**: Utilizing threat intelligence to predict and prevent potential cyber threats.
- **Security Policies**: Discussing the formulation and implementation of effective security policies within organizations.

Session 7: Incident Response and Management

- **Incident Handling Process**: Outlining the steps involved in responding to a cyber security incident.
- **Role of Incident Response Teams**: Understanding the responsibilities and actions of response teams during and after a security breach.

Session 8: Cyber Ethics and Legal Aspects

- **Ethical Considerations**: Discussing the ethical responsibilities involved in managing cyber security issues.
- **Legal Framework**: Understanding cyber laws, data protection regulations, and compliance requirements.

Session 9: Cyber Security Awareness and Education

- **Promoting Awareness**: Exploring strategies to educate and raise awareness among employees, students, and the general public.
- **Training Programs**: Designing effective cyber security training programs.

Session 10: Interactive Case Studies and Group Discussions

- **Real-life Case Studies**: Analyzing recent cyber security breaches and their implications.
- **Group Discussions**: Engaging participants in discussions to brainstorm solutions and preventive measures for hypothetical scenarios.

Session 11: Future of Cyber Space Security

- **Emerging Technologies and Threats**: Exploring potential future cyber threats and advancements in security technologies.
- **Career Opportunities**: Discussing career paths and opportunities in the cyber security field.

Session 12: Evaluation, Certificates, and Conclusion

- **Assessment and Evaluation**: Conducting a quiz to evaluate participants' understanding.
- **Certificates of Completion**: Providing certificates to attendees who completed the course.

Program Coordinator
AMC Dental College

Department of Periodontology
AMC Dental College & Hospital
Khokhra, Ahmedabad

Dean
AMC Dental College

Dean,
A.M.C. Dental College