L	T	P	C
3	1	0	4

Course Code: INT430
Semester: VI

INFORMATION SECURITY

Course Objectives

This course will help the learner to understand the key features of information systems security, security issues of wired/wireless network, biometrics access control, cryptographic systems, digital signatures, information security model/metrics, and cyber laws

UNIT - I **15 Periods**

Information systems in global context: globalization of business and the need for distributed information systems, global information systems: role of Internet and web services, information systems security and threats, threats to information systems: new technologies open door to the threats, information-level and network-level threats, **information systems security**: threats and attacks, classifications of threats and assessing damages, protecting information systems security, information security management in organizations, **building blocks of information security**, information security risk analysis, Security challenges posed by mobile devices

UNIT - II **15 Periods**

Security considerations in mobile and wireless computing: organizational measures for handling mobile devices related security issues, laptops: physical security countermeasures, use of RFID in mobile commerce and information asset protection, **security in cloud computing**: protecting information security and data privacy in cloud computing, smartphone security, **security of wireless network**: wired world versus wireless world - putting wireless networks in information security context, security and privacy challenges - understanding security and privacy issues in **IoT**, intelligent buildings: security threats, **smart cities**: privacy and security

UNIT - III **15 Periods**

Biometrics for security: Biometrics identification and authentication techniques, biometrics system: architectural design issues, biometric measurement issues, benefits of biometrics over traditional authentication methods, **network security in perspective**: need for security in the networked world, establishing security perimeter for network protection, **cryptography and encryption**: role of cryptography in information security, **digital signature** - a method for information security, cryptographic algorithms, **intrusion detection** (ID) for securing the networks: ID for information systems security, **firewalls for network protection**: why firewalls are needed? examining firewalls in the context of IDS, use firewalls effectively

UNIT - IV **15 Periods**

Security models, frameworks, standards and methodologies: ISO 27001, ISMMM, SSE-CMM, IA-CMM,**methodologies**: IAM, IEM, OCTAVE, OSSTMM, SIPES, **security metrics**: security metrics basics, classifications, importance, implementing security metrics program, key success factors in implementing infosec metrics, pitfalls and challenges in organizational security metrics program, **laws, and legal framework for information security**: understanding the laws for information security, the Indian IT Act, laws for IPR, patent law, copyright law, Indian Copyright Act, privacy issues and laws in Hong Kong, Japan and Australia, European outlook on laws for IS, data protection act in Europe, HIPPA, GLBA, building security into software/system development life cycle

TEXTBOOKS

1. Nina Godbole, Information systems security - security management, metrics, Framewrorks and Best Practices, Wiley India Pvt. Ltd., 2nd ed., 2017
2. Sood,Cyber Laws Simplified, Mc Graw Hill, 2017

REFERENCES

1. Umesha Nayak and UH Rao, The InfoSec Handbook: An Introduction to Information Security, Apress; 1st ed. edition (10 September 2014)
2. Gaurav Gupta and Sarika Gupta, Information Security and Cyber Laws, Khanna Publishing; First edition (2019)
3. Mark Rhodes-Ousley, Information Security: The Complete Reference, McGraw-Hill Education; 2 edition (16 September 2012)

UNITWISE LEARNING OUTCOMES

Upon successful completion of each unit, the learner will be able to

UNIT I	• Comprehend various threats to the information systems. • Become aware of the information security protection mechanism.
UNIT II	• Know mobile and wireless computer security considerations. • Grasp the protection and privacy concerns in cloud comp., and IoT.
UNIT III	• Understand biometrics identification and authentication techniques. • Understand different cryptographic systems, IDS, and firewalls.
UNIT IV	• Become aware of different info. security models and metrics. • Gain knowledge of the global laws for information security.

COURSE LEARNING OUTCOMES

Upon successful completion of the course, the learner will be able to

- Explain the globalizastion of business and the need for distributed information systems.
- Understand the various information security techniques for protecting distributed information systems.
- Comprehend various security issues of wired/wireless networks, cloud computing, smart-phone, smart-cities, and IoT devices.
- Understand the biometric identification and authentication techniques for preventing impersonation attacks.
- Understand some common cryptographic systems and digital signatures for information security.
- Grasp the information security models/metrics, and different global laws for information systems security.