Bachelor of Science in Digital Science and Technology (DST)

(3) Cyber Security

Course description of Major Elective Courses

Number of credits (Lecture – Laboratory – Self-study)

ITDS 351 Advanced Cybersecurity 3 (2 – 2 – 5)

Prerequisite: ITDS 271

Co-requisite: None

Cyber threats and attacks; the cybersecurity including DHCP, LDAP, the domain controller; the network security both wired and wireless such as Firewall, VLAN, WPA2; the database access control; cloud security. web application security; cyber attack techniques via network attacks such as sniffing, ARP poisoning, spoofing, and the rouge access point; system attacks such as the unauthorized access and exploitation; web application attacks according to the OWASP top 10; social engineering attacks such as phishing and fake accounts; malware including virus, trojan, worm, ransomware; advance the persistent threat (APT); ethical hacking; the basic vulnerability assessment, penetration testing and tools; real case studies of cyber-attacks with lesson learns

ITDS 352 Secure Software Development 3 (2 – 2 – 5)

Prerequisite: ITDS 271

Co-requisite: None

The secure software and system development life cycle; risk characteristics and often system and software vulnerabilities; security requirements according to related security standards such as ISO27001 and PCIDSS; related laws; the development security checklist; analysis and design phases; protection principles to help software secure and reliable including confidentiality, integrity, availability, authentication, authorization, accountability, and nonrepudiation; security design principles including the least privilege, the separation of duties, the defense in depth, the fail safe, the least common mechanism, the elimination of the single point of failure, use cases, misuse cases, the attack surface validation, the implementation and coding phases including the secure coding, the source code review, security testing standards, the vulnerability assessment, and the vulnerability management; the deployment phase including the deployment approval and change management; the operation phase including the continuously security monitoring and response; the disposal phase

ITDS 353 Fundamentals of Digital Forensics 3 (2 – 2 – 5)

Prerequisite: ITDS 271

Co-requisite: None

Digital investigations, digital evidence collections, digital evidence preservations, the computer hardware, the file system analysis, thefile recovery, the memory analysis, digital forensic analysis tools, digital forensic reports, software tools for digital forensics

ITDS 354 Cyber Risk Management and Operation 3 (3 – 0 – 6)

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

Co-requisite: None

Risk management concepts; risk assessment; risk analysis; identifyings threats and vulnerabilities; risk response; countermeasure selection; the security control assessment; monitoring; risk management frameworks; risk analysis reporting

ITDS 355 IT Auditing 3 (2 – 2 – 5)

Prerequisite: ITDS 271

Co-requisite: None

The IT environment; functions of internal and external audits; roles of IT auditing; professional IT auditing; legislation related to IT; the IT audit process: planning, scheduling, budgeting, scope, team, tasks and deadlines; tools and techniques used in auditing IT; IT governance and strategy; risks and controls; the change control management; information systems operations; the information security; systems acquisition and outsourcing; documentation; reporting and presentation; case studies

ITDS 356 Practical Cybersecurity 3 (0 – 6 – 3)

Prerequisite: ITDS 271

Co-requisite: None

Using the software tools to install the wire and wireless network communication; simulating and testing for vulnerability; intelligence gathering; network traffic information sniffing; using the software tools for testing the database accessibility and for finding the vulnerability of the web application; the techniques to identify the social engineering attacks; using the software tools for penetration testing