

Bachelor of Science Program in Digital Science and Technology (Thai Program)

Academic Year 2026 – 2030

Faculty of Information and Communication Technology, Mahidol University

Course Description

(3) Cyber Security Courses

Number of credits (Theory – Practice – Self Study)

ITDS 350	Advanced Cybersecurity	3 (3 – 0 – 6)
Prerequisite: ITDS 273 Computer and Communication Security 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 354	Cyber Risk Management and Operation	3 (3 – 0 – 6)
Prerequisite: ITDS 273 Computer and Communication Security Co-requisite: None		
Risk management concepts; risk assessment; risk analysis; identifying threats and vulnerabilities; risk response; countermeasure selection; the security control assessment; monitoring; risk management frameworks; risk assessment reporting; risk treatment plan		
ITDS 356	Practical Cybersecurity	3 (0 – 6 – 3)
Prerequisite: ITDS 273 Computer and Communication Security 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		

ITDS 358 IT Auditing**3 (3 – 0 – 6)**

Prerequisite: ITDS 273 Computer and Communication Security

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, scope, team, tasks, and deadlines; tools and techniques used in auditing IT; risks and controls; the change control management; information systems operations; the information security; documentation; reporting and presentation

ITDS 359 Special Topic in Cybersecurity**3 (3 – 0 – 6)**

Prerequisite: ITDS 273 Computer and Communication Security

Co-requisite: None

Recent advanced knowledge and techniques in cybersecurity; practical deployment of cyber security; other related topics that can be varied depending on the interests of faculties and students

ITDS 392 Secure Software Development**3 (3 – 0 – 6)**

Prerequisite: ITDS 273 Computer and Communication Security

Co-requisite: None

The secure software and system development life cycle; secure software concepts; secure software requirements specification using abuse case and misuse cases analysis; secure software design principles such as 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, threat modeling and potential attack vectors analysis; secure software implementation including defensive coding practices, prevention and mitigation techniques, and common software vulnerabilities and controls; secure software testing including software quality assurance testing types, security testing, performance testing, test-driven development for security testing; secure software deployment and operations including the deployment approval, change management, continuous security monitoring and response and secure software disposal

ITDS 393 Fundamentals of Digital Forensics**3 (3 – 0 – 6)**

Prerequisite: ITDS 273 Computer and Communication Security

Co-requisite: None

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