Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
3. **(1 week)**	Differentiate and integrate legal, privacy and ethical aspects in the context of cyber security to develop a securitypolicy • Legal and ethical aspects of computer security • Evaluate current legislation and judicial decisions in the context of government regulations • Policies/standards/risk Management • Security policy formulation	Lecture/discussion, collaborative work. Critical reflection of relevant literature and on-line research, databases and industry inquiry.	Individual assignment and Final Exam
4. **(1 week)**	Review basic security issues related to wired, wireless and mobile networks • Telecommunications systems, VOIP • Network Security • Wireless Security • Host security & server security • Mobile security and emerging technologies (BYOD & BYOA, cloud, virtualisation) • Application level security	Lecture/discussion, collaborative work. Critical reflection of on-line research, databases and industry inquiry; practical lab exercises in the use of commercial, open source and freely available security tools	Individual assignment and Final Exam

5.
(5 weeks)
	Analyse different mitigation mechanisms and prevention methods to determine and evaluate possible security solutions
	• Detect, deny, defend (disrupt, degrade, deceive, destroy) strategies
	• Authentication mechanisms
	  ○ NT LANMAN
	  ○ Kerberos v5
	• Digital signatures
	• Introduction to cryptography
	• Physical and logical security controls
	• Fundamentals of firewalls
	• Fundamentals of IDS/IPS Systems
	• Fundamentals of antivirus: signatures and sandboxing
	• Incident response
	• Testing for security: Vulnerability and penetration testing
		Lecture/discussion, collaborative work. Critical reflection of literature research, on-line research, practical lab exercises in the use of commercial, open source and freely available security tools; blue / red team exercises)	Individual assignment and Final Exam

Updated in May 2014