Bachelor of Information Technology (Network Security)

Course Structure

Year 1: Level 100 – Foundation knowledge subjects

SEMESTER 1
ITICT101A  Fundamentals of Computer Organisation
ITPRD101A  Critical Thinking for the IT Professional
ITICT102A  Introduction to Programming
ITICT103A  Internetworking 1

SEMESTER 2
ITICT104A  Internetworking 2
ITPRD102A  Communication for the IT Professional
ITICT105A  File Systems and Data Concepts
ITNET101A  Introduction to Cryptography

Year 2: Level 200 – Development subjects

SEMESTER 1
ITICT201A  Advanced Internetworking 1
ITPRD201A  Project Management (Group work)
ITICT202A  Wireless Networks
ITNET201A  Introduction to Network Security

SEMESTER 2
ITICT203A  Advanced Internetworking 2
ITPRD202A  Professional Issues in IT
ITNET202A  Enterprise Security
And one elective chosen from:
ITICT204A World Wide Web Programming
ITPRD203A Knowledge Management
ITPRD204A Future eTrends and Issues

Year 3: Level 300 – Network Security synthesis subjects

SEMESTER 1
ITNET301A  Mobile Computing and Security
ITNET302A  Advanced Network Security 1
ITNET303A  Major Security Project 1

SEMESTER 2
ITNET304A  Advanced Network Security 2
ITNET305A  Emerging Technologies Security
ITNET306A  Major Security Project 2
And one elective chosen from:
ITNET 307A National Data Infrastructure Security
ITNET 308A eCommerce and eGovernment Security
ITNET 309A Computer and Network Forensics
ITICT301A Internetworking Troubleshooting
And one elective chosen from the list not already selected in year 3 semester 1
Subject Summaries

ITICT101A – Fundamentals of computer organisation
This subject introduces students to the key theoretical and practical elements of computer technology including computer hardware and software development and operations, PC maintenance and correct, safe handling procedures, systems assembly and configuration, and computer processor technologies. Students explore computer operating systems and are introduced to the different types of computers and associated peripheral devices. The subject introduces students to the fundamentals of computer networks and computer security and focuses on the appropriate use of terminology and communication in a technology environment.

ITICT102A – Introduction to programming
IT102A Introduction to programming is a core subject in the TAFE NSW Higher Education Bachelor of Information Technology (Network Security) programme. In this subject students will explore the software development lifecycle and key approaches to software development and analysis including the object-oriented approach. Students are introduced to the fundamentals of computer programming and how they can be used to solve business problems. Students are introduced to a number of key programming languages and their environments, but will focus on the use of Java. Students will explore what constitutes good programming style and syntax. Students will be given the opportunity to apply their knowledge and understanding of software engineering to develop correct, readable and reusable solutions from problem specifications. The subject provides experience in the design, construction, testing, and evaluation of computer programing using Java through individual and group practical assessments.

ITICT103A – Internetworking 1
The subject introduces students to the exciting world of computer networks and the internet. Students begin by exploring the nature of networks, in both the human world and the computer world, before looking at the different types of networks and network architectures. They explore a number of specific network configurations and data protocols include Ethernet technology, OSI, and TCP/IP. Students also explore how data signals and packets are transmitted through routers and other forwarding devices. Students will be introduced to the critical factors necessary for implementing, verifying, and troubleshooting routing operations in small-to-medium-sized networks.

ITPRD101A – Critical Thinking for the IT Professional
In this subject students are introduced to the different types of problems they may face in the IT field. Students explore critical thinking techniques and systematic approaches and methods that are used to solve problems. Students are introduced to logic and mathematics in computing and the fundamental concepts of discrete mathematics that are the tools of the IT specialist. Students learn to apply algorithmic solutions to solve problems, and techniques to develop, test, and implement algorithmic solutions.

ITICT104A – Internetworking 2
Students explore in more detail several different types of networks and network concepts, including VLANs, wireless networks, and wide area networks (WANs) and their associated technologies. Students will focus on the use of switches and basic switching concepts and configurations (including Layer 2 switching protocols) as well as network management and administration, and network threats and security. Students conclude the subject by examining emergent networking technologies and discussing associated issues and challenges.
ITNET101A – Introduction to Cryptograph
In this subject students will explore the history and nature of cryptography and its applications in the modern world. Students will engage in discussions on the theories and fundamentals of cryptography and the key roles of logic and discrete mathematics. Students will explore topics such as random number theory, stream and block ciphers, private and public-key encryption, and various security protocols.

ITICT105A – File systems and database concepts
Students develop a sound understanding of the theories associated with database management systems and their application to real world contexts. Students explore the concepts of relational databases and database design and explain how Structured Query Language (SQL) is used. They discuss various application development tools and consider a number of database models, especially Entity-Relationship and Relational models. Students will undertake practical activities to ensure that they understand data organisation and can perform SQL and other database queries in real life scenarios.

ITPRD102A – Communication for the IT professional
This subject introduces students to the research and writing skills required for successful undergraduate-level study in information technology. It focuses on both academic and technical literacy, both of which are underpinned by skills in searching for, identifying, evaluating, and selecting appropriate information sources. Students learn how to use referencing systems and how to construct documentation according to the requirements of the IT industry. They are introduced to the writing process of planning, drafting, and editing their work with the aim of their documents achieving their purpose and meeting the needs of their audience.

ITPRD201A – Project Management (group work)
This subject introduces students to the field of project management, its theory, practice, and development. Students will be introduced to the project life cycle, the often complex role of the project manager, and strategies for how to work and cooperate in teams, and, when necessary, how to overcome conflict.

ITICT201A – Advanced internetworking 1
Students will learn to implement advanced routing protocols such as EIGRP, a multi-area OSPF network, an eBGP-based solution, an IPv6-based solution, an IPv4 or IPv6-based redistributions solution, as well as an Implement Layer 3 Path Control Solution. Students will also examine the use of advanced internetworking solutions in various industry-related contexts and will explore the requirements for and appropriateness of various networking solutions.

ITICT202A – Wireless networks
The subject introduces students to the key theoretical and practical elements of WLAN technology including WLAN devices, related software and WLAN operations, configuration, troubleshooting and maintenance. Students will explore types of antennas used in WLAN networks and will be introduced to the different types of WLAN protocols WLAN security.
**ITNET201A – Introduction to network security**
This subject introduces students to the critical importance of network security. Students start by describing the nature of security threats and the vulnerabilities experienced by various types of networks. Students explore the role of effective network management and administrative and restrictive access in threat and risk mitigation and discuss the importance of developing and implementing an effective network security policy. Students will revise the role of cryptography in network security including scripting, and discuss how to implement effective firewall technologies and intrusion prevention systems (IPS). The unit also introduces students to the ‘triple A’ approach to network security: authentication, authorisation, and accounting. Students examine security measures for virtual private networks (VPNs), data and confidentiality issues, and LAN security.

**ITICT203A – Advanced internetworking 2**
Students are introduced to Campus Networks and their effective design and implementation, as well as (Cisco) High Availability networks. Students will also examine the design and implementation of VLANs together with Inter-LAN routing and Spanning Tree technologies. Students assess how WLANs, Voice, and Video technologies may be integrated into Campus Networks and develop practical skills in troubleshooting and problem solving.

**ITPRD202A – Professional issues in IT**
This subject introduces students to a range of issues that arise in the IT environment and that regularly challenge IT professionals, particularly legal, social, and ethical issues. Students develop a sense of professional responsibility within established local and international legal and ethical codes and social frameworks. Students explore issues relating to privacy, computer crime, the reliability of systems, laws relating to network systems such as intellectual property and copyright laws, technology and the work environment, occupational health and safety, and some of the issues surrounding the increasing use of technology in society. Students apply communication skills associated with a professional IT environment, and conclude with a discussion of the ethical aspects of emerging and converging technologies.

**ITNET202A – Enterprise security**
This subject introduces students to enterprise-wide network security systems and the concept of an Enterprise System Architecture (ESA), the structures and systems, both physical and procedural, that contributes to the security of information and data across a distributed computing environment. Students will explore concepts such Enterprise Application Architecture, Enterprise Application Integration and Enterprise Collaboration systems. They will discuss the technical and operational differences between authentication and access principles, and various access control concepts such as DAC, MAC, and RBAC. Students also examine the various security considerations associated with different systems architectures, e.g., VPN, WLAN, etc.

**ITPRD203A – Knowledge management**
Students explore how knowledge is created and what constitutes the knowledge environment of businesses. Students discuss workplace structures, cultures, and human resources that support and enable knowledge sharing and management. Students identify and describe the tools that are used to create knowledge management systems and explain how their effectiveness can be evaluated.
ITICT204A – World Wide Web programming
This subject introduces students to the world of programming for the World Wide Web and how to create effective websites. The subject also introduces students to the use of client-side and server-side scripts. Students explore key aspects of webpage design and discuss website planning and the production of clear user specifications. Students then examine key web programming protocols including XHTML, HTTP, CSS, and XML and develop basic web pages. Students will discuss key copyright and ethical issues relating to the use of data on websites, before concluding with an examination of issues relating to website management, maintenance, and administration.

ITPRD204A – Future eTrends and issues
Students start with a brief examination of key eTrends and technologies including e-commerce and e-shopping, e-learning, social networks, online community forums, email and associated forms of communication. Students then explore and discuss the threats that can be associated with these technologies such as identify theft, fraud, malware, data theft and destruction, and even physical threats and risks.

ITNET301A – Mobile computing and security
This subject introduces students to the rapidly expanding array of mobile communications devices and the prolific range of threats to the secure operation of these devices. Students begin with a discussion of various devices and the security flaws and weaknesses that may allow unauthorised access. Students identify and implement basic and best practice security techniques to protect mobile devices and discuss various standards for mobile security. Students examine a range of specific devices such as BlackBerry, Android and iphone and ways in which security may be breached as well as ways that these devices may attack a WLAN. Students also look at the security of mobile data, email, SMS, and multimedia and examine various security testing techniques.

ITNET302A – Advanced network security 1
Students engage in a detailed and in-depth examination of advanced network security issues, with a focus on security analysis, penetration testing, and intrusion detection and prevention. Students begin with a review of the state of network security, including current threats, protective methods, types of attack and attacker and possible results. Emphasis is on the need for thorough security analysis and testing to determine, and then eliminate various threats and vulnerabilities. Students examine the requirements of an effective security policy, including monitoring network activity, and security auditing and management. Students investigate the rationale and principles of penetration testing as well as tools and methods, such as advanced Googling, ‘sniffing’, and ‘snort analysis’ or ‘port scanning’. The use of simple coding and scripting is applied. They examine the principles of intrusion detection and prevention systems (IDPS), their key functions, and common detection methodologies. Students look at various types of IDPS, including network-based and wireless and network behaviour analysis; and explore various IDPS products. Students conclude the subject with a debate of salient legal and ethical issues.

ITNET303A – Major security project 1 (group)
Students work in small groups and with a member of the academic staff to identify and develop their own security-related project.
ITNET304A – Advanced network security 2
In this subject, students engage in a detailed and in-depth examination of advanced network security issues. Students examine key aspects of a secure network, which include secure network architecture, relevant standards and protocols, encryption, authentication, access control, and WLAN, email, and IP security. Furthermore, they examine system security management, cybercrime, and issues related to recovering from a security breach.

ITNET305A – Emerging technologies security
In this subject students examine several of the most critical specific risks that are associated with emerging technologies. Students will be introduced to and will examine issues such as: self-encryption hard drives, built-in biometrics, mobile device security, RFID security, USB authentication token (two-factor authentication), cloud computing, VoIP security issues, IPv6 security concerns, multicast and broadcast security, identity management, and Internet 2 security.

ITNET306A – Major security project 2 (individual)
This subject offers students the opportunity to undertake a large-scale, complex security project. The subject will also introduce students to essential professional skills and concepts such as understanding their own personality types and how they work, how to manage stress and pressure, how to manage time and workloads, how to cultivate ethical professional practice, goal setting, professional development and identifying skill deficiencies, how to develop personal and professional networks, and project evaluation.

ITNET307A – National data infrastructure protection
This subject introduces students to the concept of information warfare and the importance of organisational and national data and information infrastructure protection and integrity. Students explore the people or organisations who might commit data or cyber attacks, the objectives of those attacks, and the actual targets of those attacks. Students consider the strategic, tactical, and operations implications of data and information security infrastructure, and the relevant national legislation and regulations governing data security and protection. Students also examine the government regulatory bodies and agencies responsible for protecting national information infrastructure and for prosecuting those who breach legislation.

ITNET308A – eCommerce and eGovernment security
This subject addresses the imperative of providing information security for e-customers as well as e-business providers. Students begin by a discussion of eCommerce and eGovernment technology and the requirements for information security, secure transactions, protection from fraud, protection of intellectual property, and so on. They examine common threats and vulnerabilities such as credit card fraud, hacking, and identity theft, and explore principles of information security, including privacy, integrity, authentication, and non-repudiation. Students examine the fundamental mechanisms of e-security such as encryption and public key cryptography, digital signatures and digital certificates, and PCI compliance. They discuss information security management and explore ways of detecting and preventing cyber crime as well as the legal requirements and ethical issues of eCommerce, including Australian government initiatives and eGovernment strategy.
ITNET309A – Computer and network forensics
Students begin by examining contemporary computer crime, including malware attack, identify theft, fraud, child pornography, organised crime, and cyber-terrorism, followed by cyber-crime within the Australian and international legal framework. Students analyse the cyber incident response process, from setting up a forensic toolkit, through the processes of detection, investigation, and gathering court-admissible evidence, to forensic reporting. They explore techniques of data collection and evidence handling particularly with regards to forensic duplication. They employ techniques and tools for investigation of storage devices, operating systems, data and image files, network intrusion, and wireless and mobile devices. Students discuss forensic analysis techniques including email and web browsing activity reconstruction.

ITICT301A – Internetworking troubleshooting
This subject introduces students to the key theoretical and practical elements of IP-based Internetwork maintenance and troubleshooting. Students will explore different methodologies, tools, equipment and procedures to aid and help in maintaining the health and continuity of IP-based internetworks.