Module Synopsis

- **Specialist Diploma in Cyber Security Management (NSCSM)**
- **Work-Study Post-Diploma (Specialist Diploma in Cyber Security Management) (WSP-NSCSM)**

PDC 1:	**Post-Diploma Certificate in Infocomm Security & Defences**	**(135 hours)**
1.	**IT8001 Infocomm Security & Network Essentials**	**(45 hours)**
	This module introduces participant to the fundamental concepts of infocomm security such as identification, authentication, authorisation, integrity and confidentiality. Participants will also learn security essentials like networking, Enterprise Network Architecture and basic Linux operating system commands. The module emphasises hands-on practice and will be taught in a combination of e-learning and onsite practical sessions. Participants will learn the concepts and knowledge through e-learning before proceeding to do exercises to reinforce their learning and gain hands-on experience during the practical.	
2.	**IT8002 Cyber Defence & Range Exercises**	**(90 hours)**
	This module introduces participants to tools to discover and exploit vulnerabilities in networks and operating systems. They will be taught the security issues found in software, especially web applications. Security components like firewalls and IDS (Intrusion Detection Systems) will also be introduced as countermeasures to defend against cyber-attacks. Participants will also get to learn Enterprise Network Penetration testing with AI. They will have the opportunity to integrate the knowledge and technical skills learned by taking part in scenario-based exercises. The module emphasises hands-on practice and will be taught in a combination of e-learning and onsite practical sessions. Participants will learn the concepts and knowledge through e-learning before proceeding to do exercises to reinforce their learning and gain hands-on experience during the practical. Class range exercises will be conducted for participants to apply what they have learnt by analysing the various types of vulnerabilities and networks and to recommend and apply countermeasures.	

PDC 2:	**Post-Diploma Certificate in Security Incident Management**	**(135* / 150^ hours)**
1.	**IT8008 Digital Forensics & Investigation**	**(60 hours)**
	This module equips participants with the fundamental concepts and techniques of computer and mobile forensics. Participants will learn to acquire, analyse, and present computer and mobile data as evidence. The module emphasises hands-on practice and will be taught in a combination of e-learning and onsite practical sessions with AI assisted forensics. participants will learn the concepts and knowledge of electronic evidence discovering, gathering, acquiring, analysing and reporting through lectures, e-learning before proceeding to do exercises to reinforce their learning and gain hands-on experience during the practical.	
2.	**IT8009 Security Policy & Incident Management***	**(75 hours)**
2.	**IT8007 Security Policy & Incident Management (Practicum)^**	**(90 hours)**

Module Synopsis

- **Specialist Diploma in Cyber Security Management (NSCSM)**
- **Work-Study Post-Diploma (Specialist Diploma in Cyber Security Management) (WSP-NSCSM)**

This module equips participants with the fundamental concepts and techniques of security policy and incident management. Participants will learn the essentials of security policy development, risk assessments and security models. Participants will also learn to monitor security events, perform network forensics analysis and proactive detection of attacks, and be introduced to security incident response. Participants will also develop competencies in the application of AI-assisted tools for cybersecurity incident response and reporting, the operation of Security Information and Event Management (SIEM) platforms for real-time security monitoring and analysis, and the practice of Threat Intelligence and Threat Hunting to proactively identify and mitigate emerging cyber threats

The module will be taught in a combination of e-learning, onsite lectures, and practical sessions. Participants will learn the concepts and knowledge about security policy and incident management through e-learning and in-class discussion, quiz before proceeding to do exercises to reinforce their learning and gain hands-on experience during the practical.

***For NSCSM:**

- Participant must complete PDC 1: IT8001 and IT8002 + PDC2: IT8008 and IT8009

^For WSP-NSCSM:

- Participant must complete PDC 1: IT8001 and IT8002 + PDC2: IT8008 and IT8007