OJT LIST OF COMPETENCIES

Course Title: WSDip in Security Systems Engineering **Level:** Diploma

S/N	LIST OF COMPETENCIES (STANDARD)	Company to indicate '✓' it is able to provide
	Design physical security system solution	
1.	Conduct security risk/safety assessment (BCA building safety code)	
2.	Develop security risk control plans	
3.	Propose security system measures	
	Manage video surveillance system	
4.	Develop video surveillance system plan	
5.	Install video surveillance system	
6.	Commission video surveillance system	
	Manage access control and intrusion detection system	
7.	Install access control system	
8.	Maintain access control system	
9.	Install intrusion detection system	
10.	Maintain intrusion detection system	
	Manage network infrastructure	
11.	Establish network infrastructure requirements	
12.	Deploy network infrastructure	
13.	Manage network services	
	Manage cloud services	
14.	Set up cloud infrastructure and services	
15.	Manage cloud security threats	
16.	Manage data protection measures	
	Manage cybersecurity ops and incident	
17.	Configure log sources	
18.	Analyse security events	
19.	Report security events with solutions	
20.	Handle cybersecurity incident	
	Enhance cybersecurity of physical security system solution	
21.	Conduct cybersecurity risk assessment for physical security system	
22.	Propose cybersecurity measures for physical security system	
23.	Implement cybersecurity measures for physical security system	
24.	Maintain cybersecurity systems	
25.	Monitor cybersecurity systems	
	Perform cyber-physical security system integration	
26. .	Coordinate cyber-physical security system integration	
27.	Perform integration of cyber-physical security components	
28.	Test integrated cyber-physical security system	

MODULE SYNOPSIS – WSDip in Security Systems Engineering

Course Objective

The course equips trainees with the skills, knowledge and professional attributes to design, deploy, manage implementation and maintenance of physical security projects, as well as apply AI and automation into the systems to optimise operational efficiency and reliability.

Modules Synopsis

Network Infrastructure
On completion of the module, trainees should be able to set up, configure and manage wired and wireless Local Area Network (LAN). They should also be able to explain networking terminologies, concepts and technologies.
Video Surveillance & AI Analytics
On completion of the module, trainees should be able to set up, configure, test and troubleshoot video surveillance systems and video analytics. They should also be able to explain video surveillance terminologies and concepts.
Intrusion & Access Control with AI
On completion of the module, trainees should be able to set up, configure, test and troubleshoot Intrusion and Access Control Systems. They should also be able to explain access control terminologies and concepts.
Cybersecurity for Security Systems
On completion of the module, trainees should be able to configure, test and troubleshoot Cybersecurity solutions to protect security systems. They should also be able to explain security threats and vulnerabilities, technologies and tools used in implementing effective Cybersecurity solutions.
Cloud Services Management
On completion of the module, trainees should be able to set up and configure cloud infrastructure and services according to organizational needs. They will also be equipped to identify and manage cloud security threats, as well as implement appropriate data protection measures to ensure confidentiality, integrity, and availability of cloud-based systems.
Security Risk Assessment & System Design
On completion of the module, trainees should be able to conduct security risk assessment and system audit. They should also be able to identify security gaps and propose security system solution.
Security Ops & Incident Management
On completion of the module, students should be able to take up tasks in the Security Operations Centre (SOC) environment including monitoring and identifying security risks, analysing and classifying security risks through security monitoring systems. They should also be able to apply appropriate counter measures to mitigate identified threats.

MODULE SYNOPSIS – WSDip in Security Systems Engineering

Security System Integration & Testing
On completion of the module, trainees should be able to coordinate and perform the integration of cyber-physical security components. They will apply established methodologies to test the integrated system.
Company Project
On completion of the module, trainees should have applied their acquired competencies in an authentic project that would value-add to the company.

TRAINING PATTERN SCHEDULE

WSDip in Security Systems Engineering

Block Release - Trainees attend daily lessons at ITE for a continuous period and then resume the next block of OJT at the workplace.

April'26 Intake	April – June 2026	ITE Vacation (June) 4 weeks	July – September 2026	ITE Vacation (Sept) 2 weeks	October – December 2026	ITE Vacation (Dec) 4 weeks	January – March 2027	ITE Vacation (March) 2 weeks
1st Year Off-JT @ ITE	**8 Weeks Block** **(Exams TBC on 9th Week)**		**OJT in Company**		**OJT in Company**		**OJT in Company**	

April'26 Intake	April – June 2027	ITE Vacation (June) 4 weeks	July – September 2027	ITE Vacation (Sept) 2 weeks	October – December 2027	ITE Vacation (Dec) 4 weeks	January - March 2028	ITE Vacation (March) 2 weeks
2nd Year Off-JT @ ITE	**OJT in Company**		**OJT in Company**		**8 Weeks Block** **(Exams TBC on 9th Week)**		**OJT in Company**	

April'26 Intake	April – June 2028	ITE Vacation (June) 4 weeks	July – September 2028	ITE Vacation (Sept) 2 weeks	
3rd Year Off-JT @ ITE	**OJT in Company**		**8 weeks Block**		**WSDip Programme 2026** **Start: 1 April 2026** **End: 30 September 2028** **Duration: 2.5 years** ⚠ **Final results release may be later than programme end date**