List of Competencies for On-the-Job Training (OJT)
Work-Study Diploma in Security Systems Engineering

S/N	List of Competencies (Standard)	Company to indicate '✓' for OJT competencies it can provide
Design physical security system solution		
1.	Conduct security risk/safety assessment	☐
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 & 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	☐
Set up server and storage system		
14.	Set up storage system	☐
15.	Maintain storage system	☐
16.	Set up server infrastructure	☐
17.	Maintain server infrastructure	☐
Manage security system project		
18.	Plan security system project	☐
19.	Oversee security system project	☐
20.	Deliver project	☐
Enhance cybersecurity of physical security system solution		
21.	Conduct cybersecurity risk assessment for physical security system	☐

S/N	List of Competencies (Standard)	Company to indicate '✓' for OJT competencies it can provide
22.	Propose cybersecurity measures for physical security system	☐
23.	Implement cybersecurity measures for physical security system	☐
Perform system integration & programming		
24.	Perform security system integration	☐
25.	Perform integration of security components	☐
26.	Perform testing and commissioning of integrated security system	☐
27.	Maintain integrated security system	☐
	Sub-total of Competencies (Standard)	0
List of Competencies (Company-specific)		
1		
2		
3		
4		
5		
6		
7		
	Sub-total of Competencies (Company-specific)	0

Note:

a) Company must be able to provide OJT for at least **75%** of the List of Competencies (Standard).

b) If company is unable to meet the 75%, please propose alternate **course-related** competencies which are unique to company operations. Alternate competencies are capped at 25%.
[i.e. 50% of the list of competencies (standard) + 25% alternate competencies (Company-specific)].

c) All alternate competencies (Company-specific) must be reviewed and endorsed by ITE.

d) Trainees must receive OJT and be assessed for **All** competencies selected in this List.

Total no. of competencies selected by company for OJT	0
Total no. of competencies listed *(standard & company specific)*	27
Percentage of selected competencies	0%

Completed By:

Name	**Company**
Designation	**Date**

For ITE's Completion					
Reviewed by CED / College *(For Company-specific Competencies)*				**Verified by IBT Officer**	
Name:				Name & Date:	
Designation:		Date:			

Version: June'23

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.

Module Synopsis

Module 1: 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.

Module 2: 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.

Module 3: 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.

Module 4: 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.

Module 5: Server & Storage Management

On completion of the module, trainees should be able to set up and maintain server and storage systems in a systematic manner.

Module 6: Project Management & Technical Writing

On completion of the module, trainees should be able to plan, execute and monitor security system project using the various project management tools and techniques to meet the project scope, schedule and cost requirements. They should also be able to prepare and write technical reports.

Module 7: 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.

Module 8: Security System Integration & Programming

On completion of the module, trainees should be able to design, implement an integrated security system solution and write program to integrate devices into security systems by applying programming concepts and languages.

Module 9: 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.

Module 10: On-the-Job Training
On completion of the module, trainees should be able to apply the skills and knowledge acquired at ITE College and workplace to take on the full job scope, including supervisory function, where appropriate, at the company.

WSDip in SECURITY SYSTEMS ENGINEERING

TRAINING PATTERN (BLOCK RELEASE)