WORK-STUDY DIPLOMA IN CYBER SECURITY & FORENSICS

MODULE OBJECTIVES

Module 1: Risk Management & Compliance

On completion of the module, trainees should be able to drive security education and awareness in an organisation by providing advice and guidance on potential risks, mitigation strategies and best practices. They should also be able to manage security program, solutions, products and services, as well as to facilitate stakeholder expectations and needs.

Module 2: Network Security Management

On completion of the module, trainees should be able to set up, configure, secure, and monitor network system and wireless network for anomalous traffic and identification of intrusions. They should also be able to configure security appliances such as firewall, end-point security, as well as intrusion detection and prevention system, as well as to address identity management requirements and perform logging for network traffic monitoring.

Module 3: System Security Management

On completion of the module, trainees should be able to implement system security and detect unauthorised system intrusion. They should also be able to set up, configure and secure a virtualised infrastructure.

Module 4: Security Operation Management

On completion of the module, trainees should be able to monitor security operation. They should also be able to automate threat analysis using innovative technologies and tools.

Module 5: Security Incident Management

On completion of the module, trainees should be able to manage incidence of cyber-attack or breach. They should also be able to automate incident handling using appropriate tools.

Module 6: Security Assessment

On completion of the module, trainees should be able to perform security scanning to uncover vulnerabilities and weaknesses. They should also be able to elevate extraction and analysis manually and using automated tools.

Module 7: Security Testing

On completion of the module, trainees should be able to facilitate security testing to uncover weaknesses using intrusive approach. They should also be able to automate the process.

Module 8: Cyber Forensics Procedure

On completion of the module, trainees should be able to gather cyber-attack evidence from various sources, escalate the cyber security incident and prepare forensics report for further investigation and analysis.

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.

Course Title: Cyber Security & Forensics **Level:** Work-Study Diploma

S/n	List of Competencies (Standard)
1.	Manage security education and awareness
2.	Prepare and present cyber security solutions
3.	Facilitate stakeholder management
4.	Manage wired network security infrastructure
5.	Manage wireless network security infrastructure
6.	Manage IT security infrastructure
7.	Maintain network documentation
8.	Manage server security
9.	Manage virtualisation security infrastructure
10.	Maintain system security documentation
11.	Manage threat detection
12.	Automate threat detection
13.	Prepare threat detection report
14.	Manage incident response
15.	Automate incident handling
16.	Implement Incident recovery
17.	Perform vulnerability assessment
18.	Automate vulnerability assessment
19.	Prepare security assessment report
20.	Facilitate penetration testing
21.	Automate penetration testing
22.	Perform security control management
23.	Plan cyber forensics operation
24.	Extract digital forensics evidence
25.	Prepare forensics report
26.	Detect network intrusion using forensics tools
27.	Detect unauthorised system intrusion using forensics tools
28.	Develop script to elevate extraction and analysis