

INSTALLATION OF CYBER SECURITY SYSTEM

UNIT CODE: SEC/CU/CU/CR/08/6/A

Relationship to Occupational Standards

This unit addresses the unit of competency: Install Cyber security system

Duration of Unit: 130 hours

Unit Description

This unit covers the competencies required to Install cyber security system. It involves identifying and analysing information to be protected, establishing systems to be installed, assessing system compatibility, installing established systems, performing system testing and debugging, monitoring system performance, documenting system installation report, establishing a cyber security backup and restoration plan and conducting training of the system users.

Summary of Learning Outcomes

1. Identify and analyze information to be protected
2. Establish systems to be installed
3. Assess system's compatibility
4. Install established systems
5. Perform systems testing and debugging
6. Monitor system performance
7. Document system installation report
8. Establish a cyber-security back up and restoration plan
9. Conduct training of system users

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify and analyze information to be protected	<ul style="list-style-type: none">• Meaning of terms• Establishment of information platforms• Determination of information attributes	<ul style="list-style-type: none">• Observation• Written tests• Oral questioning

	<ul style="list-style-type: none"> • Technology in information storage and analysis • Information access control • Information analysis 	<ul style="list-style-type: none"> • Practical tests
2. Establish systems to be installed	<ul style="list-style-type: none"> • Meaning of terms • Factors to consider in establishment of cyber security system • Trends and threats in security system • Hardware and software requirement is security system installation 	<ul style="list-style-type: none"> • Observation • Written tests • Oral questioning • Practical tests
3. Asses system's compatibility	<ul style="list-style-type: none"> • Meaning of terms • Compatibility assessment of cyber security system • Factors to consider in assessment of cyber security system compatibility • Components specification in system assessment • Procedures of cyber security system assessment 	<ul style="list-style-type: none"> • Observation • Oral questioning • Practical tests • Written tests
4. Install established systems	<ul style="list-style-type: none"> • Meaning of terms • Acquisition of cyber security management system • Tools in installation of cyber security system • System installation scheduling • Cyber security system configuration 	<ul style="list-style-type: none"> • Observation • Oral questioning • Practical tests • Written tests
5. Perform systems testing and debugging	<ul style="list-style-type: none"> • Meaning of terms • Types of tests on a cyber-security system • Factors to consider in testing and debugging of cyber security system • Testing process of the cyber security system • Debugging and error troubleshooting 	<ul style="list-style-type: none"> • Observation • Oral questioning • Practical tests • Written tests
6. Monitor system performance	<ul style="list-style-type: none"> • Meaning of terms • System monitoring process • System simulation • Logs auditing • Patch management 	<ul style="list-style-type: none"> • Observation • Oral questioning • Practical tests • Written tests

7. Document system installation report	<ul style="list-style-type: none"> • Meaning of terms • Report preparation • Report dissemination • Report filing 	<ul style="list-style-type: none"> • Observation • Written tests • Oral questioning • Practical tests
8. Establish a Cyber security back up and restoration plan	<ul style="list-style-type: none"> • Meaning of terms • Establishment of cyber security back up management system • Factors to consider in establishment of cyber security system <ul style="list-style-type: none"> • Information in cyber security back up and restoration plan • Backup media and process • Back up testing <ul style="list-style-type: none"> • Validation • Performance • Integrity • Back up procedures 	<ul style="list-style-type: none"> • Observation • Written tests • Oral questioning • Practical tests
9. Conduct training of system users	<ul style="list-style-type: none"> • Meaning of terms • Cyber security system user training preparation • Training manuals are prepared • Filing of cyber security system operation manual 	<ul style="list-style-type: none"> • Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instruction

- Demonstration by trainer
- Practice by the trainee
- Field trips
- On-job-training
- Discussions

Recommended Resources

<p>Equipment</p> <ul style="list-style-type: none"> • Computers • Printers • Cameras • Phones • Photocopiers 	<p>Materials and supplies</p> <ul style="list-style-type: none"> • Stationery
--	---

Reference materials	
----------------------------	--

- Manufacturers' manuals
- Relevant catalogues
- Tables
- National and international standards

easytvvet.com