

DEMONSTRATE UNDERSTANDING OF SECURITY LAWS, POLICIES AND REGULATIONS

ISCED UNIT CODE: 0612554 09A

TVET CDACC UNIT CODE: SEC/CU/CS/CU/01/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Demonstrate understanding of security laws, policies and regulations.

Duration of Unit: 120 hours

Unit Description

This unit covers the competencies required to apply cybersecurity laws, policies, and regulations. It involves demonstrating an understanding of relevant legal and regulatory frameworks, formulating organizational security guidelines, implementing and enforcing these measures, assessing their effectiveness, ensuring compliance with applicable requirements, and continuously monitoring their impact within the organization.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Demonstrate understanding of cyber security laws, policies and regulations	20
2. Develop Cyber Security policy	10
3. Implement Cyber Security policy and regulations	30
4. Evaluate Cyber security policy	20
5. Evaluate compliance in Cyber security policy and regulations	10
6. Monitor effectiveness of Cyber security policy in an organization	20
7. Monitor effectiveness of Cyber security	10
Total Hours	120

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Demonstrate understanding of cyber security laws	1.1 Meaning of terms 1.1.1 World legal system 1.1.1.1 Common law 1.1.1.2 Religious law 1.1.1.3 Hindu law 1.1.1.4 Islamic law 1.2 Types of Cyber security laws 1.2.1 National 1.2.2 International 1.3 Cyber crimes 1.3.1 Types of cyber crimes 1.3.2 Challenges in prosecuting cyber crime 1.4 Cyber-crime laws 1.4.1 Local Cybercrime laws 1.4.2 International Cybercrime laws 1.5 Application of cyber security laws 1.6 Compliance of cyber security laws 1.7 Impacts of cyber crime 1.7.1 Positive and Negative	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests
2. Demonstrate understanding of different Cyber security policies and regulations	2.1 Meaning of terms 2.2 Fundamentals of cyber security 2.3 Types of cyber security policies and regulation 2.4 Application of different cyber security policies 2.5 Stakeholders involved in cyber security policies and regulations 2.6 Regulatory board in cyber security	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	policies	
3. Develop Cyber Security policy	3.1 Meaning of terms 3.2 Components of cyber security and information classification 3.3 Cyber security policy alignments to the vision and mission 3.4 Procedures of drafting cyber security policy 3.5 Cyber security review process	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests
4. Implement Cyber Security policy and regulations	4.1 Meaning of terms 4.2 Cyber security policy implementation process 4.3 Cyber security policy implementation team 4.4 Importance of schedule in the implementation process of cyber security policy 4.5 Verification of cyber security implementation 4.6 Relevant regulations in implementation of cyber security policy	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests
5. Evaluate Cyber security policy	5.1 Meaning of terms 5.2 Review and updates of cyber security policy 5.3 Process of evaluation of cyber security policy 5.4 Factors to consider in evaluation of cyber security policy	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests

Learning Outcome	Content	Suggested Assessment Methods
6. Evaluate compliance in Cyber security policy and regulations	6.1 Meaning of terms 6.2 Infrastructure and landscape audit 6.3 Calculation of risk factors 6.4 Calculation of non – compliance factors 6.5 Compliance level recommendation	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests
7. Monitor effectiveness of Cyber security policy in an organization	7.1 Meaning of terms 7.2 Compliance level 7.3 Cyber security policy monitoring impact on: 7.3.1 Process 7.3.2 People 7.3.3 Technology 7.4 Monitoring effectiveness of cyber security policy	▪ Observation ▪ Oral questioning ▪ Written tests ▪ Practical tests

Suggested Delivery Methods

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions
- Case study.

Recommended resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	Learning Materials			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	Learning Facilities & infrastructure			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	Consumable materials			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	Tools and Equipment			
11.	Computers		25 pcs	1:1
12.	Projector		1 pc	25:1