

DEMONSTRATE UNDERSTANDING OF CYBER SECURITY LAWS, POLICIES AND REGULATIONS

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

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.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	These are assessable statements which specify the required level of performance for each of the elements <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Demonstrate understanding of cyber security laws, policies and regulation	1.1 Key national and international cybersecurity laws and frameworks (GDPR, HIPAA, NIST, ISO/IEC 27001, Data Protection Acts) are identified and explained. 1.2 Organizational security policies, standards, and procedures are reviewed and interpreted in relation to compliance requirements. 1.3 Legal obligations regarding data privacy, intellectual property, cybercrime, and digital forensics are explained with relevant examples. 1.4 Consequences of non-compliance with cybersecurity laws and policies are analyzed, including legal, financial, and reputational impacts. 1.5 Roles and responsibilities of stakeholders (management, IT teams, end-users, regulators) in cybersecurity compliance are described. 1.6 Emerging regulations and industry-specific

	requirements are researched and summarized. 1.7 Case studies of cybersecurity breaches and legal implications are reviewed to reinforce understanding. 1.8 Understanding is demonstrated through discussions, presentations, or written reports aligned with organizational and legal frameworks.
2. Develop Cyber Security policy	2.1 Organizational security needs and regulatory requirements are identified through consultation with stakeholders. 2.2 Scope, objectives, and applicability of the cybersecurity policy are defined in line with organizational goals. 2.3 Policy statements addressing confidentiality, integrity, availability, and accountability are formulated. 2.4 Access control, authentication, and authorization guidelines are incorporated into the policy. 2.5 Provisions for acceptable use, data protection, incident response, and disaster recovery are included. 2.6 Security measures for emerging technologies (cloud, IoT, mobile, AI) are integrated where relevant. 2.7 Roles and responsibilities of employees, administrators, and management are clearly defined. 2.8 Compliance with applicable laws, regulations, and standards is ensured in policy development. 2.9 Draft policy is reviewed with stakeholders and revised based on feedback. 2.10 Final cybersecurity policy is documented, approved by management, and communicated across the