

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 in demonstrate understanding Cyber security laws, policies and regulations. It involves demonstrating the understanding of different cyber security policies and regulations, developing cyber security policy, implementing Cyber security policies and regulations, evaluating Cyber security policies, evaluating compliance in Cyber security policies and regulations and monitoring effectiveness of Cyber security policy in an 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 analysed, 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 organization.
3. Implement Cyber Security policy and regulations	3.1 Cybersecurity policies, standards, and regulatory requirements are communicated to all relevant stakeholders. 3.2 Roles and responsibilities for policy enforcement are assigned and clearly defined. 3.3 Security controls (technical, administrative, and physical) are implemented in accordance with the policy. 3.4 Training and awareness programs are conducted to ensure compliance among employees and system users. 3.5 Compliance checks and audits are performed to verify adherence to policies and regulations. 3.6 Violations or deviations from policy are identified, reported, and managed according to defined procedures. 3.7 Continuous monitoring mechanisms are established to ensure ongoing compliance. 3.8 Feedback from implementation and monitoring is documented to guide improvements in policies and practices.
4. Evaluate Cyber security policy	4.1 The effectiveness of implemented cybersecurity policies is assessed against organizational objectives and regulatory requirements. 4.2 Compliance audits, monitoring reports, and incident records are reviewed to identify gaps or weaknesses. 4.3 Stakeholder feedback (employees, management, IT teams) is collected to evaluate policy clarity, usability, and enforcement. 4.4 Metrics and key performance indicators (KPIs) are

	analyzed to measure policy effectiveness. 4.5 Changes in legal, regulatory, or technological environments are considered to ensure ongoing relevance. 4.6 Recommendations for policy updates, improvements, or amendments are documented. 4.7 Evaluation results are communicated to management and other relevant stakeholders for decision-making. 4.8 Continuous improvement processes are initiated to align the cybersecurity policy with evolving threats and organizational needs.
5. Evaluate compliance in Cyber security policy and regulations	5.1 Compliance requirements from relevant laws, regulations, and standards (e.g., GDPR, ISO/IEC 27001, HIPAA) are identified and documented. 5.2 Organizational adherence to cybersecurity policies and regulatory obligations is assessed through audits, reviews, and inspections. 5.3 Gaps, non-compliance issues, or deviations from established policies are identified and analysed. 5.4 Impact of non-compliance on organizational operations, legal obligations, and reputation is evaluated. 5.5 Corrective and preventive actions are recommended to address compliance gaps. 5.6 Continuous monitoring processes are established to maintain compliance with evolving laws and regulations. 5.7 Compliance evaluation results are documented and communicated to stakeholders, management, and regulatory bodies as appropriate. 5.8 Lessons learned are incorporated into policy updates, training programs, and governance

	frameworks.
6. Monitor effectiveness of Cyber security policy in an organization	6.1 Mechanisms are established to continuously monitor adherence to cybersecurity policies across all organizational units. 6.2 Security metrics, KPIs, and performance indicators (e.g., number of incidents, policy violations, response times) are defined and tracked. 6.3 Monitoring tools and systems (e.g., SIEM, audit logs, automated alerts) are utilized to detect non-compliance or policy breaches. 6.4 Reports on policy effectiveness, compliance status, and security incidents are generated regularly for management review. 6.5 Feedback from employees, IT teams, and stakeholders is collected to identify gaps or challenges in policy implementation. 6.6 Trends, risks, and emerging threats are analysed to assess the continued relevance of the cybersecurity policy. 6.7 Recommendations for policy improvement or updates are documented and communicated to decision-makers. 6.8 Monitoring activities are reviewed periodically to ensure continuous alignment with organizational goals and regulatory requirements.
7. Monitor effectiveness of Cyber security	7.1 Continuous monitoring mechanisms are established to track overall cybersecurity performance across the organization. 7.2 Security incidents, policy compliance, system vulnerabilities, and threat trends are regularly reviewed. 7.3 Key metrics and indicators (e.g., incident response

	times, number of breaches, compliance levels) are analyzed to assess effectiveness. 7.4 Emerging threats, new technologies, and regulatory changes are incorporated into monitoring processes. 7.5 Reports on cybersecurity effectiveness are generated for management and stakeholders, highlighting strengths and areas for improvement. 7.6 Recommendations for improving security posture, policy updates, or additional controls are documented and communicated. 7.7 Monitoring activities are periodically reviewed to ensure alignment with organizational goals, risk appetite, and legal/regulatory requirements.
--	--

RANGE

This section provides work environment and conditions to which the performance criteria apply. It allows for different work environment and situations that will affect performance.

Variable	Range
Organizational security policies may include but not limited to:	• Policies • Standards • Procedures
Policy development considerations may include but not limited to:	• Access control • Authentication • Authorization • Acceptable use • Data protection • Incident response • Disaster recovery
Policy review and revision may include but not limited to:	• Alignment with regulations • Incorporation of stakeholder feedback • Updates based on emerging threats

Continuous monitoring mechanisms may include but not limited to:	• SIEM tools • Audit logs • Automated alerts
Monitoring activities may track but not limited to:	• Security metrics • Key performance indicators (KPIs) • Incident response times • Policy violations
Periodic evaluation of monitoring and reporting may include but not limited to:	• Alignment with organizational goals • Alignment with risk appetite • Alignment with legal and regulatory requirements

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Knowledge of organizational security policies, standards, and procedures that govern secure operations.
- Understanding of key factors in policy development, including access control, authentication, authorization, acceptable use, data protection, incident response, and disaster recovery.
- Review and revise security policies to ensure alignment with regulations, incorporation of stakeholder feedback, and adaptation to emerging threats.
- Monitoring mechanisms, such as SIEM tools, audit logs, and automated alerts, to maintain organizational security oversight.
- Monitoring activities, including tracking security metrics, key performance indicators (KPIs), incident response times, and policy violations.

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in ICT;
- Time management;
- Analytical

- Problem solving;
- Planning;
- Decision making;
- Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Organizational security policies, standards, and procedures are reviewed to interpret compliance requirements. 1.2 Legal obligations concerning data privacy, intellectual property, cybercrime, and digital forensics are described with examples. 1.3 Emerging regulations and industry-specific requirements are researched and summarized. 1.4 Case studies of cybersecurity breaches and associated legal implications are reviewed. 1.5 Organizational security needs and regulatory requirements are identified in consultation with stakeholders. 1.6 Access control, authentication, and authorization guidelines are incorporated. 1.7 Provisions for acceptable use, data protection, incident response, and disaster recovery are included. 1.8 Compliance with applicable laws, regulations, and standards is ensured in policy development. 1.9 Draft policy is reviewed and revised based on stakeholder feedback. 1.10 Policies, standards, and regulatory requirements are communicated to relevant stakeholders. 1.11 Violations or deviations are identified, reported, and managed per defined procedures. 1.12 Continuous monitoring mechanisms are established for
--	--

	ongoing compliance for policy updates or improvements documentation 1.13 Evaluation results are communicated to management and stakeholders. 1.14 Continuous improvement processes are initiated to align policies with evolving threats and organizational needs. 1.15 Continuous monitoring processes are established to maintain regulatory adherence 1.16 Security metrics, KPIs, and performance indicators (incidents, policy violations, response times) are tracked. 1.17 Monitoring tools (SIEM, audit logs, automated alerts) are utilized to detect non-compliance. 1.18 Reports on policy effectiveness, compliance status, and security incidents are generated for management review. 1.19 Recommendations for policy updates or improvements are documented and communicated. 1.20 Monitoring activities are reviewed periodically to ensure alignment with organizational and regulatory goals. 1.21 Emerging threats, technologies, and regulatory changes are incorporated into monitoring processes. 1.22 Reports on cybersecurity effectiveness are generated for management and stakeholders, highlighting strengths and gaps. 1.23 Monitoring and reporting activities are periodically reviewed to ensure alignment with organizational goals, risk appetite, and legal/regulatory requirements.
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of	Competency may be assessed through:

Assessment	3.1 Oral questioning 3.2 Written tests 3.3 Practical demonstration 3.4 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

CORE UNITS OF COMPETENCY