

SEVERN BUSINESS COLLEGE

Level 6 Graduate Diploma in Cyber Security

Course Handbook

Qualification
SBC Level 6 Graduate Diploma in Cyber Security

Level
6

Total Qualification Time
1200

Credit Value
120

Aim of the Course
The Level 6 Graduate Diploma in Cyber Security is designed to equip learners with the advanced knowledge, analytical skills, and technical competencies required to identify, manage, and mitigate cyber threats in complex digital environments. This qualification develops learners' ability to design secure systems, manage incidents, evaluate organizational risks, and ensure compliance with global cybersecurity standards. Graduates will be well-positioned to pursue professional roles such as Cyber Security Analyst, Network Security Engineer, or Information Security Consultant.

Assessment
Assessment is through practical assignments, with no exams - to more accurately reflect the real working environment.

Course Structure

SBC Level 6 Graduate Diploma in Cyber Security			
Unit number	**Units**	**Unit level**	**Unit credit**
1	Cyber Security Principles and Practices	6	20
2	Network and Infrastructure Security	6	20
3	Ethical Hacking and Penetration Testing	6	20
4	Digital Forensics and Incident Response	6	20
5	Cyber Security Management and Governance	6	20
6	Emerging Technologies and Future Threats	6	20

Assessment Grades

Grade	Marking Criteria
Pass	All learning outcomes are achieved. All assessment criteria are met.
Fail	All learning outcomes are not achieved. All assessment criteria are not met.
No Marks	Plagiarism

UNIT SPECIFICATIONS

Unit Title
Cyber Security Principles and Practices

Level
6

Learning Time Hours
200

Credit Value
20

Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand the core principles of cyber security	1.1 Explain key concepts and terminology in cyber security. 1.2 Analyse the relationship between security, confidentiality, integrity, and availability. 1.3 Evaluate the role of cryptography in securing data. 1.4 Assess emerging trends influencing cyber security principles.

2. Examine cyber threat landscapes	2.1 Identify common types of cyber threats and vulnerabilities. 2.2 Analyse current threat actors and their motivations. 2.3 Evaluate the global impact of cybercrime. 2.4 Assess how threat intelligence informs security strategy.
3. Understand security frameworks and standards	3.1 Compare major international security standards (ISO 27001, NIST). 3.2 Evaluate compliance requirements for organizations. 3.3 Assess the importance of policy and governance frameworks. 3.4 Develop recommendations for implementing a security policy.
4. Analyse risk management approaches	4.1 Define risk management in a cyber security context. 4.2 Apply risk assessment methodologies. 4.3 Develop a risk mitigation plan. 4.4 Evaluate the effectiveness of risk management processes.

UNIT SPECIFICATIONS

Unit Title
Network and Infrastructure Security

Level
6

Learning Time Hours
200

Credit Value
20

Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand network security fundamentals	1.1 Explain the structure and function of network architectures. 1.2 Evaluate security mechanisms within different network layers. 1.3 Assess vulnerabilities in network configurations. 1.4 Propose secure network design solutions.
2. Implement network security controls	2.1 Configure firewalls, routers, and intrusion detection systems. 2.2 Demonstrate the use of VPNs and encryption protocols. 2.3 Apply security hardening techniques to network devices. 2.4 Test and validate network security controls.
3. Analyse wireless and cloud security risks	3.1 Identify security challenges in wireless networks. 3.2 Evaluate the security implications of cloud adoption. 3.3 Propose countermeasures for hybrid environments. 3.4 Assess cloud provider compliance and responsibility models.
4. Monitor and maintain secure networks	4.1 Implement network monitoring tools. 4.2 Analyse network traffic for anomalies. 4.3 Create an incident response plan for network breaches. 4.4 Evaluate the effectiveness of ongoing monitoring practices.

UNIT SPECIFICATIONS

Unit Title
Ethical Hacking and Penetration Testing

Level
6

Learning Time Hours
200

Credit Value

20

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand the principles of ethical hacking	1.1 Explain the legal and ethical frameworks of penetration testing. 1.2 Distinguish between black-box, white-box, and grey-box testing. 1.3 Evaluate hacker methodologies and attack vectors. 1.4 Assess the role of social engineering in security testing.
2. Plan a penetration test	2.1 Define penetration testing objectives and scope. 2.2 Identify target systems and tools for testing. 2.3 Develop a test plan in compliance with ethical guidelines. 2.4 Justify risk mitigation measures during testing.
3. Conduct penetration testing activities	3.1 Execute reconnaissance and vulnerability scanning. 3.2 Exploit vulnerabilities in a controlled environment. 3.3 Document testing results and evidence. 3.4 Evaluate the security posture of the tested environment.
4. Report and evaluate penetration test results	4.1 Prepare a comprehensive penetration test report. 4.2 Recommend technical and strategic remediation measures. 4.3 Communicate findings to stakeholders. 4.4 Reflect on ethical and professional responsibilities.

UNIT SPECIFICATIONS

Unit Title

Digital Forensics and Incident Response

Level

6

Learning Time Hours

200

Credit Value

20

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand digital forensic principles	1.1 Explain forensic investigation processes. 1.2 Assess legal and ethical implications in digital forensics. 1.3 Identify evidence types and acquisition methods. 1.4 Evaluate the importance of chain of custody.
2. Conduct forensic analysis	2.1 Use appropriate forensic tools for data recovery. 2.2 Analyse system and network logs for anomalies. 2.3 Identify indicators of compromise. 2.4 Document findings in accordance with forensic standards.
3. Develop incident response procedures	3.1 Design an incident response plan. 3.2 Assess different incident types and escalation levels. 3.3 Evaluate communication protocols during incidents. 3.4 Test and improve response effectiveness.
4. Report and present forensic findings	4.1 Prepare a forensic investigation report. 4.2 Present technical evidence in a legal context. 4.3 Recommend organizational improvements post-incident. 4.4 Reflect on challenges in digital investigations.

UNIT SPECIFICATIONS

Unit Title
Cyber Security Management and Governance

Level
6

Learning Time Hours
200

Credit Value
20

Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand governance frameworks	1.1 Explain corporate governance in relation to cyber security. 1.2 Evaluate roles and responsibilities within security management. 1.3 Assess the impact of leadership on cyber security culture. 1.4 Analyse governance frameworks such as COBIT and ISO 38500.
2. Develop and implement security policies	2.1 Design effective security policies and procedures. 2.2 Evaluate the policy lifecycle and review mechanisms. 2.3 Integrate security policies with organizational objectives. 2.4 Assess compliance with internal and external regulations.
3. Manage cyber security operations	3.1 Analyse operational security metrics and KPIs. 3.2 Develop a security operations centre (SOC) model. 3.3 Evaluate resource and staffing requirements. 3.4 Propose improvement strategies for security operations.
4. Evaluate the role of ethics and sustainability	4.1 Discuss ethical challenges in managing security. 4.2 Evaluate data privacy and protection laws. 4.3 Assess the role of sustainability in cyber practices. 4.4 Propose strategies for ethical leadership.

UNIT SPECIFICATIONS

Unit Title
Emerging Technologies and Future Threats

Level
6

Learning Time Hours
200

Credit Value
20

Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand emerging technologies in cyber security	1.1 Analyse the impact of AI and machine learning on security. 1.2 Evaluate blockchain applications for secure transactions. 1.3 Assess IoT security vulnerabilities. 1.4 Examine quantum computing implications for encryption.
2. Evaluate current and future cyber threats	2.1 Identify global trends in cyber-attacks. 2.2 Assess the evolution of ransomware and advanced persistent threats (APTs). 2.3 Analyse state-sponsored cyber activities. 2.4 Predict future threat landscapes.

3. Propose innovative security solutions	3.1 Develop adaptive security strategies using emerging tools. 3.2 Evaluate the feasibility of AI-driven threat detection. 3.3 Recommend innovation-based risk reduction techniques. 3.4 Assess ethical considerations in deploying emerging technologies.
4. Conduct a research project on future security issues	4.1 Define a research question relevant to future cyber threats. 4.2 Apply appropriate research methods and data analysis. 4.3 Present findings with evidence-based conclusions. 4.4 Reflect on research implications for industry and policy.

Version:2510a