QUALIFICATION SPECIFICATION SECTION A							
QUALIFICATION DEVELOPER	Botswana International University of Science and Technology						
TITLE	Bachelor of Science in Cyber Security and Digital Forensics				**LEVEL**	7	
FIELD	Information and Communications Technology		**SUB-FIELD**	Cyber Security and Digital Forensics			
New qualification	✓	Review of existing qualification					
SUB-FRAMEWORK	General Education		TVET		Higher Education	✓	
QUALIFICATION TYPE	Certificate		Diploma		Bachelor	✓	
	Bachelor Honours		Master		Doctor		
CREDIT VALUE					510		

1. RATIONALE AND PURPOSE OF THE QUALIFICATION

Developing countries such as Botswana are also experiencing cyber threats and need experts in the field. There is a demand for experts in Botswana who specialize in Cyber Security and Digital Forensics. This statement is supported by the documented discussions with the members of the Departmental Stakeholder Advisory Committee (DSAC) held on October 13, 2016 and March 3, 2017. Cyber Security and Digital Forensic qualification contributes to the achievement of the goals stated in the National Information and Communications Technology (ICT) Policy (Maitlamo) which calls for the protection of personal privacy and security of information systems and networks, NDP 11 and ETSSP.

The need for Cyber Security and Digital Forensics is also reflected in the HRDC priority skills and employment trends document, under the ICT sector of Table 4, which outlines the technical and soft skills for the top occupations in demand for Botswana. The Cyber Security and Digital Forensics qualification will produce highly skilled graduates who are capable of defending our critical information technology

infrastructure and this contributes to the National Vision 2036 Pillar 4. Criminal activities are getting complex with the advancement of technology hence the need for experts in the field of Cyber Security and Digital Forensics to be able to defend and investigate crimes committed within the digital domain and this qualification is in line with the National Vision 2036 Pillar 4. There is also a high demand of Cyber Security and Digital Forensics experts worldwide. This statement is supported by the National Institute of Standards and Technology (NIST) version 1.1 2018.

The introduction of this qualification will place Botswana at the forefront on dealing with cyber threats. With the growing numbers and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information as well as safeguard national security. The proposed qualification will give students the skills and expertise to safeguard the nations against cyber-attacks. Students will also study digital forensics, which is concerned with the investigation of criminal activities.

Qualification Purpose

The purpose of this qualification is to provide candidates with advanced theoretical knowledge while they gain the high level skills, and advanced practical experience to excel in areas that range from cyber security and digital forensic. This qualification will imbue candidates with the advanced knowledge and expertise to identify breaches, vulnerabilities and threats and build high level digital investigation skills that will minimize their impact on organizations. Furthermore, this qualification offers high-level research learning and analysis skills to candidates. It also empowers candidates to become entrepreneurs.

The graduates will be able to do the following:

- Apply risk assessment methodologies in selecting and configuring security controls to protect information assets.
- Monitor a network infrastructure for cyber-attacks.
- Mitigate the effects on a network infrastructure due to a cyber-attack.
- Evaluate an end-to-end computer forensics investigation.
- Prepare a digital forensics evidence report.

2. ENTRY REQUIREMENTS (including access and inclusion)
1. Certificate IV, NCQF level 4 (General Education or TVET), BGCSE or equivalent 2. Admission through RPL and CAT will be provided through ETP policies in line national RPL and CAT Policies.

3. QUALIFICATION SPECIFICATION SECTION B	
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**
LO1. Conduct cyber security advanced risk assessment according to international professional board in small and medium scale organisations	AC1. Apply knowledge of risk management standards and approaches while doing cybersecurity assessment AC2. Create a threat landscape for an organization taking into consideration their dynamic nature AC3. Characterize and classify cyber threats
LO2. Develop a security architecture for an organization to meet its strategic goals	AC1. Demonstrate advanced knowledge of different cybersecurity controls including physical, operational, logical and technical operational controls

	AC2. Apply technical controls (cryptography, access management, firewalls, anti-virus software and intrusion prevention systems) and describe their purpose in the cyber architecture AC3. Support technical and theoretical cyber investigations AC4. Incorporate incident response and management procedures AC5. Systematic define components and steps of a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP)
LO3. Implement cyber security solutions according to international standards in small and medium scale organisations	AC1. Develop security controls to protect systems and information AC2. Apply standards to enhance security in the development process AC3. Identify common trade-off and compromises in incorporating security in the development
LO4. Design and implement operational and strategic cyber security strategies and policies according to international standards in small and medium scale organisations	AC1. Implement security and information assurance within IT governance AC2. Adopt standards such as ISO/IEC 27014 information cybersecurity governance, ITGI Information Security Governance, the ISO/IEC 27036 series for cybersecurity governance AC3. Incorporate various cyber security legislation AC4. Design a structured approach to managing security risks and information technology

	operations within the context of an organization's objectives
LO5. Demonstrate specialised understanding of technology and how it works to its lowest level	AC1. Demonstrate advanced knowledge of how data is stored in different storage media at a file system level AC2. Extract files from a corrupt media through advanced techniques such as carving AC3. Identify files through file signatures AC4. Recognise steganography through examining file signatures
LO6. Carry out cyber security investigation using the national law enforcement guidelines in small and medium scale organisations	AC1. Respond to a cyber incident AC2. Application of various digital forensic tools and theories AC3. Analyse the evidence to discover patterns of suspicious activities AC4. Present results at the level of an expert AC5. Report the forensic findings
LO7. Demonstrate advanced programming skills to develop new information recovery techniques	AC1. Write scripts to extract data from new file systems AC2. Write scripts to analyse new forms of data AC3. Write scripts to recognise malicious activities AC4. Write scripts correlate log data for network forensics
LO8. Conduct advanced digital data extraction and analysis from memory chips	AC1. Use specialised tools to physically remove the chip AC2. Acquire the raw data using specialised chip programmers and adapters

	AC3. Analyse raw data using industry standard and custom tools AC4. Verify the results and produce a forensic report
LO9. Recognize and apply the legal, social, ethical and professional issues in cyber security	AC1. Apply professional, ethical and legal practices to exploit a computer system AC2. Demonstrate specialised knowledge of different cyber security legislations
LO10. Conduct a scientific research in cybersecurity in accordance with academic standards	AC1. Produce an academically acceptable research proposal AC2. Undertake a literature review to assess the significance of the research problem AC3. Apply the knowledge in the subject area to address the problem AC4. Produce an academically acceptable report for the project AC5. Present findings in clear and comprehensive manner
LO11. Work as a member of a team	AC1. Demonstrate tolerance to viewpoints expressed by other members of the team AC2. Participate actively in discussions AC3. Provide assistance and encourage other team members AC4. Contribute towards group deliverables AC5. Understand issues in team roles AC6. Demonstrate leadership skills and ability to manage conflicts AC7. Ability to produce a final project as a team
LO12. Communicate effectively	AC1. Demonstrate effective presentation skills to a range of audiences

	AC2. Show confidence in wide range of cyber security core concepts AC3. Demonstrate good report writing skills and organization AC4. Demonstrate time management by submitting deliverables on time AC5. Apply project management skills such as work-breakdown approaches
LO13. Demonstrate business intelligence (entrepreneurship skills)	AC1. Develop, innovate solution and turn it into a business idea AC2. Conduct market research AC3. Develop a business plan AC4. Carry out SWOT analysis for the business

4. QUALIFICATION STRUCTURE

SECTION C

FUNDAMENTAL COMPONENT Subjects / Units / Modules /Courses	**FUNDAMENTAL COMPONENT**	**Level**	**84**
	Calculus	5	24
	Physics	5	12
	Writing and Communication	5	12
	Programming Skills	5	6
	Business and Entrepreneurship	5	30
CORE COMPONENT Subjects / Units / Modules /Courses	**CORE COMPONENT**		**360**
	Programming Skills	6	24
	Data Structures and Algorithms	6	12
	Computer Architecture	6	12
	Discrete Mathematics for Computer Science	6	12
	Programming for Cyber Security (Python)	6	24
	Databases	7	12
	Computer Networks	7	24
	Operating Systems	7	12
	Statistics and Probability	7	12
	Web Application Security	7	12
	Cryptography	7	24
	Cyber Psychology	7	12
	Network Security	7	24
	Digital Forensics	7	24
	Individual Project in Cyber Security and Digital Forensics	7	24
	Research Methodology	7	12
	Industrial Attachment	7	60
	Professional Issues and Ethics in IT	7	12

	Internet of Things Security and Privacy	7	12
ELECTIVE COMPONENT Subjects / Units / Modules /Courses	**ELECTIVE COMPONENT**		**99**
	Cloud Computing	6	9
	Distributed Systems and High Performance Computing	6	9
	Internet Programming	6	9
	Formal Methods	6	9
	Mobile Forensics	7	9
	Internet of Things Security and Privacy	7	9
	Multimedia Forensics	7	9
	Wireless and Mobile Security	7	9
	Security by Design	7	9
	Machine Learning	7	9
	Safe E-Services	7	9
	Cloud Security	7	9
	Cloud Forensics	7	9
	Emerging Technologies	7	9
	Data Analytics	7	9
	Biology I	5	12
	Chemistry I	5	12

4.1 Rules of combinations, Credit distribution (where applicable):

The qualification consists of a total of **510 credits** with **96 credits** Fundamental Components, **360 credits** Core Components and **66 credits** made from choosing several Elective Components.

Table 1 Credit Distribution

Level	Credit
5	96 (12 taken from electives)

6	81 (9 taken from electives)
7	333 (45 taken from electives)
Total	**510** (66 taken from electives)

Rule

Students will be awarded the qualification after completing and attaining the minimum 510 credits.

Electives

Candidates are required to select a minimum of 66 credits of electives. A minimum of 12 credits from level 5, 9 credits from level 6, 45 credits from level 7. One must take either Biology I or Chemistry I.

5. ASSESSMENT AND MODERATION ARRANGEMENTS

ASSESSMENT

All assessments, formative and summative, leading/contributing to the award of credits or a qualification should be based on learning outcomes and/or sub-outcomes.

Formative Assessment

Formative assessment or continuous assessment contributing towards the award of credits should be based on course outcomes. This can include tests, assignments and projects as well as simulated and real work settings. The contribution of formative assessment to the final grade shall be 40%.

Summative Assessment

Candidates may undergo assessment including written and practical and simulated projects. The final examination contributes 60% of the final mark.

MODERATION

The following shall apply for both internal and external moderation in accordance with institutional and national policies.

Assessors and moderators must be registered and accredited with all relevant bodies such as Botswana Qualifications Authority (BQA).

6. RECOGNITION OF PRIOR LEARNING (if applicable)

Candidates may submit evidence of prior learning and current competence and/or undergo appropriate forms of RPL assessment for the award of credits towards the qualification in accordance with applicable ETP RPL policies and relevant national policy and legislative framework.

7. PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Learning Pathways

Horizontal Articulation:

- Bachelor of Science Cyber Security
- Bachelor of Science Digital Forensics
- Bachelor of Science Information Security Management
- Bachelor of Science Computer Science

Vertical Articulation:

- Bachelor of Science Honours in Cyber Security
- Bachelor of Science Honours in Digital Forensics
- Bachelor of Science Honours in Information Security Management
- Bachelor of Science Honours in Computer Science

Employment Pathways

There are several opportunities in for the specialists in Cyber Security and Digital Forensics including:

- Information Security Analyst
- Penetration Tester
- Computer Systems Security Analyst
- Threat Intelligence Analyst
- Insider Threat Analyst
- Security Incident Responder
- Business Process and Security Analyst
- Risk Manager Analyst
- Security Operations (SOC) Analyst
- Healthcare Information Systems Security Office
- Web Mobile Application Security Analyst
- Malware Analyst
- Disaster Recovery Analyst
- Digital Forensics Investigator
- Industrial Cyber Security Analyst
- Network Security Analyst
- Cyber Security Architect
- Secure Software Developer
- Cryptographer
- Entrepreneur

8. QUALIFICATION AWARD AND CERTIFICATION

Minimum Standards of Achievement for the Award of the Qualification

To be awarded a Bachelor of Science (Cyber Security and Digital Forensics) qualification, a candidate is required to achieve a minimum of **510** credits inclusive of **96** credits for Fundamental courses, **360** credits for Core courses, and **66** credits for Optional/ Elective Courses.

Certification

Candidates meeting prescribed requirements will be awarded the qualification in accordance with standards prescribed for the award of the qualification and applicable policies.

9. REGIONAL AND INTERNATIONAL COMPARABILITY

BENCHMARKING

Regional

Regional there was no university that was offering Bachelor of Science in Cyber Security and Digital Forensics.

International

Majority of the top international universities offer Bachelor of Science in Cyber Security and Digital Forensics as a Bachelor of Science Honours in Cyber Security and Digital Forensics. The following university of an ordinary degree in Bachelor of Science in Cyber Security and Digital Forensics.

1. **Middlesex University, London (Bachelor of Science in Cyber Security and Digital Forensics)**
2. **Stevenson University (Bachelor of Science in Cyber Security and Digital Forensics)**

Qualification Overview Analysis

Middlesex University and Stevenson University offer Bachelor of Science in Cyber Security in Digital Forensics. Middlesex University qualification is 3 years full time with options of 4 years full year with 1 year industrial place or 5 years part-time. Stevenson University qualification is 4 years. The proposed qualification is planned to take 4 years on a full-time basis. Middlesex University qualification includes industrial placement which is a year long while Stevenson University does not have industrial placement. The proposed qualification has industrial attachment which is one semester. Both Middlesex University and Stevenson University have project work which is also included in the proposed qualification.

Similarities with the proposed program

The proposed qualification has a high rate of similarity with the qualification offered by Middlesex University and Stevenson University.

Difference with the proposed program

The main difference include Physics, Chemistry or Biology and calculus which are present in the proposed qualification. These courses are fundaments and necessary for student who do not have NCQF Level 5 qualification. They offer the fundamental background to science-based qualifications. It was also necessary to include courses such as programming, databases, statistics, and cyber psychology to provide learners with a wide range of options for specialisation. For instance, a leaner who is more interested in databases might progress and end up specializing in database forensics or security. The proposed qualification also offers industrial attachment to give them industrial experience.

10. REVIEW PERIOD

This qualification shall be reviewed every five years