SECTION A:	***QUALIFICATION DETAILS***																	
QUALIFICATION DEVELOPER (S)	ABM University College																	
TITLE	Bachelor of Science in Cyber Security													***NCQF LEVEL***				
FIELD	Information and Communications Technology			***SUB-FIELD***	Cyber Security									***CREDIT VALUE***				*480*
New Qualification			✓	*Review of Existing Qualification*														
SUB-FRAMEWORK	*General Education*			*TVET*									*Higher Education*					✓
QUALIFICATION TYPE	*Certificate*	*I*		*II*		*III*		*IV*		*V*			*Diploma*		*Bachelor*			✓
	Bachelor Honours			*Post Graduate Certificate*									*Post Graduate Diploma*					
	Masters							*Doctorate/ PhD*										

RATIONALE AND PURPOSE OF THE QUALIFICATION

RATIONALE:

Cybercrime is one of the most critical problems facing businesses in Botswana. According to the Botswana Cyber Security Report 2018, the cost of cybercrime in Africa has soared to $3.3 Billion, while Botswana suffered losses of up to P250 Million.

The National Development Plan 11 covering years 2017-2023, states that cyberspace threats and risks should be dealt with during the NDP implementation. The NDP 11 further notes that since cyber security threats are imminent and worrisome, it is appropriate for legislation to combat cyber security to be developed during NDP 11.

Furthermore, the National Cyber Security Strategy notes that the country, has limited capacity on Cyber Security expertise. The issues of Cyber Security require a multi-stakeholder approach due to the diverse nature of the cyberspace.

IT security is very significant in any organisation using information systems and cyber crime is on the rise worldwide; hence there is a higher demand of cyber security professionals.

A research study was conducted to find out if BSc In Cyber Security will be relevant and in high demand in Botswana job market. This involved consulting various sources such as participants, information resources (newspapers), Human Resources Consultants, seasoned Information Technology professionals and others. The findings reveal that BSc In Cyber Security was among the list of qualifications highly needed in the job market. Hence, it is ideal to develop the qualification BSc In Cyber Security for Botswana and SADC region.

.

PURPOSE:

The purpose of this qualification is to produce graduates with specialised knowledge, skills and competences to be able to;

- Detect, troubleshoot, and prevent cyber security incidents.
- Identify Information Technology (IT) systems' vulnerabilities.
- Formulate IT strategies to enhance the IT security to reduce the overall exposure to cybercrime.
- Implement and manage security practices effectively.

ENTRY REQUIREMENTS (including access and inclusion)

1. A minimum of NCQF Level 4 or equivalent with at least a credit in Mathematics.
2. Applicants who do not meet the above minimum requirements will be considered for entry through Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer (CAT) in accordance with ETP and national policies on RPL and CAT.

SECTION B	***QUALIFICATION SPECIFICATION***
GRADUATE PROFILE (LEARNING OUTCOMES)	***ASSESSMENT CRITERIA***
3.1 Design, develop and implement Information Technology (IT) systems, applications, policies and procedures that meet identified strategic objectives and reflecting emerging trends and issues in cyber security.	3.1.1 Produce good quality software solutions in different programming platforms. 3.1.2 Develop a database that can address different business cases. 3.1.3 Design a Web-based application that can align with organisational needs 3.1.4 Develop relevant tools for System Analysis and Design to meet critical organisational requirements. 3.1.5 Infuse Software Engineering and Computer Programming tools to generate solutions to business problems
3.2 Demonstrate in-depth knowledge and understanding of cyber security application development and the business, financial and social context in which information systems are developed and secured.	3.2.1 Apply basic knowledge and skills of cyber security application development. 3.2.2 Assess the security threats on existing cloud systems. 3.2.3 Troubleshoot maintenance and updating of the security of business information systems 3.2.4 Deploy network and system monitoring tools in order to offer real time security to the organizations' information.
3.3 Evaluate cyber security risk management policies and strategies in order to provide adequate security to organisations'	3.3.1 Distinguish between the different types of cyber-attacks/threats.

confidential information and asses the security needs of an information system in an organisation	3.3.2 Assess computer, information, and network security threats in existing systems. 3.3.3 Formulate solutions to existing and other possible security attacks. 3.3.4 Investigate on IT applications, technologies, and best practices in the advancements of the security of organisation's information
3.4 Contribute to the advancement of the profession through participation in research or inquiry into areas of practice and professional practice	3.4.1 Exercise critical research skills and competencies gained to identify opportunities for growth and market development. 3.4.2 Participate in IT Security educational activities to enhance knowledge and skills of professional practice and competencies
3.5 Demonstrate competency in cryptography and authentication techniques and digital forensics	3.5.1 Formulate cryptography solutions in business and other contexts 3.5.2 Analyse and solve problems that require forensics intervention. 3.5.3 Demonstrate understanding of the various user authentication techniques. 3.5.4 Design and construct user authentication modules
3.6 Provide leadership and technical support in the professional development of peers and other practitioners to promote quality delivery of products and services	3.6.1 Work efficiently as an individual or in teams. 3.6.2 Assess and appraise team-members and team task progress.
3.7 Demonstrate competence in the Cyber Security Field	3.7.1 Communicate with clients, colleagues and others using appropriate methods and techniques.

	3.7.2 Carry out measurement and calculations using appropriate equipment and formulae as required. 3.7.3 Demonstrate requisite skills and attitudes for teamwork and a sense of collective responsibility for achievement of team goals and objectives. 3.7.4 Identify the problems and take remedial Actions and / or appropriate decisions for resolving problems. 3.7.5 Identify opportunities and initiate or suggest ideas and actions to improve the field as a whole 3.7.6 Demonstrate knowledge and understanding of Health and Safety requirements and related personal obligations. 3.7.7 Plan and organize activities and tasks to achieve efficiency. 3.7.8 Evaluate own actions or performance and make judgements about what to do to improve. 3.7.9 Use of ICT for information retrieval and processing as well as communication and collaboration with others.

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	***Credit Value***
5	***72***
6	***84***
7	***324***
TOTAL CREDITS	***480***
Rules of Combination: ***(Please Indicate combinations for the different constituent components of the qualification)***	
Fundamental component = 96 credits. Core component = 372 credits Elective component = 12 credits. **Total = 480 credits.**	

ASSESSMENT ARRANGEMENTS

Learners shall be assessed through formative assessment and summative assessment. The contribution of each type of assessment towards the qualification shall be 75% formative assessment and 25% summative assessment.

MODERATION ARRANGEMENTS

There shall be internal and external moderation of assessments as a quality assurance measure. The moderation will be done in accordance with the ETP and national policies on moderation.

All assessments and moderation processes shall be carried out by assessors and moderators who are registered and accredited by Botswana Qualifications Authority or any recognised and relevant international body.

RECOGNITION OF PRIOR LEARNING

Candidates may submit evidence of prior learning and current competence and/or undergo appropriate forms of Recognition of Prior Learning (RPL) assessment for the award of credits towards the qualification in accordance with applicable policies and relevant national-level policy and legislative framework. Implementation of RPL shall also be consistent with requirements, if any, prescribed for the field or sub-field of study by relevant national, regional, or international professional bodies.

CREDIT ACCUMULATION AND TRANSFER

There shall be provision for the award of credits leading to the award of the qualification through Credit Accumulation and Transfer (CAT) in accordance with national and ETP's policies on CAT.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

LEARNING PATHWAYS

1. Horizontal Pathways

Learners can pursue related NCQF Level 7 qualifications, including, but not limited to:

- Bachelor of Science Computer Science.
- Bachelor of Science Software Engineering.
- Bachelor of Software Engineering.
- Bachelor of Science Forensic Computing

2. Vertical Pathways

a) ***NCQF Level 7 qualifications, including, but not limited to:***

- Master of Science in Cyber Security.
- Master of Science in Computer Science.
- Master of Science in Business Technology.

2. EMPLOYMENT

After completion of this program the candidate should be able to work as, among others:

- Application Security Specialist.
- Cloud Security Manager.
- Computer Programmer.
- Forensics Analyst.
- Information Security Analyst/Officer.
- Information Systems Manager.
- IT Auditor.
- Network Administrator.
- Network Security Administrator.

QUALIFICATION AWARD AND CERTIFICATION

The Bachelor of Science in Cyber Security qualification shall be awarded to learners who accumulate a minimum of 480 credits as per the rules of combination. A certificate and transcript shall be issued to learners who meet the requirements for award of the qualification.

REGIONAL AND INTERNATIONAL COMPARABILITY

The qualification was benchmarked against similar qualifications in Kenyatta University(Kenya) and University of Potomac, United States of America.

Kenyatta University Bachelor of Science in Cyber Security and Forensics, at NQF Level 7, is worth 420 Credits and produces graduates with competencies in applying the general theory of Information Technology and Cyber security, providing software solution from the knowledge of the sub-fields of computer science, managing, organising, and retrieving information based on the concepts of information systems Security.

University of Potomac Bachelor of Science in Cyber Security and Policy, worth 120 credits, is comparable with Bachelor of Science in Cyber Security. The two qualifications are comparable in terms of learning outcomes and articulation pathways.

Although the qualifications examined generally follow similar structures and standards, there are differences, though not significant, in NQF level and Credit value, Assessment strategies and Qualification rules and minimum Standards.
This qualification generally compares well with all the qualifications studied since the exit outcomes cover similar scope and depth and are aligned to exit-level descriptors typical of this level and type of qualification as done within the region and beyond.

REVIEW PERIOD
The qualification shall be reviewed every after 5 years.