QUALIFICATION SPECIFICATION			**SECTION A**
QUALIFICATION DEVELOPER	Botswana International University of Science and Technology		
TITLE	Bachelor of Science (Honors) in Cyber Security and Digital Forensics	**LEVEL**	8
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 Honors	✓	Master		Doctor	
CREDIT VALUE	120					

1. RATIONALE AND PURPOSE OF THE QUALIFICATION

RATIONALE:

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 expertises to safeguard the nations against cyber-attacks. Students will also study digital forensics, which is concerned with the investigation of criminal activities.

PURPOSE:

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

The graduates will be able to do the following:

- Apply information security management systems to protect information assets of large organizations.
- Monitor network infrastructure for advanced cyber-attacks.
- Perform digital investigation of advanced cyber- attack.
- Conduct advanced digital data extraction and analysis.

Upon completion, graduates will work as:

- Digital Forensics Specialist
- Cyber security Specialist
- Information Security Implementer
- Information Security Auditor
- Cyber Threat Specialist
- Cryptographer

2. ENTRY REQUIREMENTS (including access and inclusion)

1. Applicants with relevant qualification of Bachelor's Degree (NCQF level 7) can be admitted into this qualification.
2. Candidates who do not meet the minimum entry requirements will be considered through RPL and CAT. Assessment will be done in line with Institutional and National Policies.

3. QUALIFICATION SPECIFICATION SECTION B

GRADUATE PROFILE (LEARNING OUTCOMES)	ASSESSMENT CRITERIA
LO1. Conduct cyber security highly specialised risk assessment according to international professional board in large scale organizations	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 specialised knowledge of different information security management systems. AC2. Apply technical controls (cryptography, access management, firewalls, anti-virus

	software and intrusion prevention systems) and describe their purpose in the cyber architecture. AC3. Incorporate cyber investigations readiness framework. AC4. Incorporate incident response and management procedures AC5. Systematic define components and steps of a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP)
LO3. Design and implement operational and strategic cyber security strategies and policies according to international standards in large scale organizations	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.
LO4. Carry out cyber security investigation using the national law enforcement guidelines in large scale organizations.	AC1. Respond to advanced cyber incident. AC2. Application of specialised digital forensic tools and theories AC3. Analyze the evidence to discover patterns of suspicious activities. AC4. Present results at the level of an expert

	AC5. Report the forensic findings.
LO5. Conduct advanced digital data extraction and analysis	AC1. Acquire the raw data from corrupt media or memory chips. AC2. Analyze raw data using industry standard and custom tools. AC3. Verify the results and produce a forensic report
LO6. 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 highly specialized knowledge of different cyber security legislations
LO7. 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
1. 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. Produce a final project as a team

4. QUALIFICATION STRUCTURE

SECTION C

	CORE COMPONENT		
CORE COMPONENT Subjects / Units / Modules /Courses	Individual Research Project in Cyber Security and Digital Forensics	8	24
	Group Project in Cyber Security and Digital Forensics	8	24
	Advanced Cyber Security I	8	12
	Advanced Cloud Forensics	8	12
	Ethical Hacking and Investigation Techniques	8	12
	ELECTIVE COMPONENT		
ELECTIVE COMPONENT Subjects / Units / Modules /Courses	Network Forensics	8	18
	Internet of Things Forensics	8	9
	Advanced Cyber Security II	8	9
	Wireless and Mobile Security	8	9
	Data Visualization Analytics	8	9
	Malware Forensics	8	9
	Cryptocurrencies, Blockchains and Applications	8	18
	Big Data Technologies	8	9
	Compliance and Legal Issues	8	9
	Risk Management	8	9
	Human and Organizational Aspects of Information Security	8	9

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

The qualification consists of a total of **120 credits** for Bachelor of Science (Honours) with **84 credits** Core Components and **36 credits** made from choosing several Elective Components.

Table 1 Credit Distribution

Level	**Credit**
8	120
Total	**120**

Rule

The qualification in Bachelor of Science (Honours) in Cyber Security and Digital Forensics is 120 credits Qualification and students will be awarded the Qualification after attaining a minimum of 120 credits.

Candidates are required to select a total of 36 credits of electives throughout the qualification all from level 8. The electives allow students to focus on an area of their interest within the Cyber Security and Digital Forensics discipline.

5. ASSESSMENT AND MODERATION ARRANGEMENTS

ASSESSMENT

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

Formative Assessment

Formative assessment or continuous assessment contributing towards the award of credits will 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 60%.

Summative Assessment

Candidates may undergo assessment including written and practical and simulated projects. The final examination contributes 40% 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 Honors in Cyber Security
- Bachelor of Science Honors in Digital Forensics
- Bachelor of Science Honors in Information Security Management
- Bachelor of Science Honors in Computer Science

Vertical Articulation:

- Master of Science in Cyber Security
- Master of Science in Digital Forensics
- Master of Science in Information Security Management
- Master of Science in Computer Science

Employment Pathways

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

- Information Security Specialist
- Computer Systems Security Specialist
- Threat Intelligence Expert
- Insider Threat Specialist
- Security Incident Responder
- Business Process and Security Specialist
- Risk Manager Expert
- Security Operations (SOC) Expert
- Healthcare Information Systems Security Specialist
- Web Mobile Application Security Specialist
- Malware Expert
- Disaster Recovery Expert
- Digital Forensics Investigator Specialist
- Industrial Cyber Security Specialist

- Network Security Expert
- Cyber Security Specialist
- 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 (Hons) in Cyber Security and Digital Forensics degree, a candidate is required to achieve a minimum of **120** credits inclusive of **84** credits for Core courses, and **36** credits for Optional/ Elective Courses.

Certification

Candidates meeting prescribed requirements will be awarded the qualification and will be issued a certificate together with a transcript.

9. REGIONAL AND INTERNATIONAL COMPARABILITY

Benchmarking

Regional

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

International

The following universities have qualifications in Bachelor of Science Honours in Cyber Security and Digital Forensics.

1. **Kingston University, London, Bachelor of Science Honours in Cyber Security & Computer Forensics**
2. **University of Portsmouth, Bachelor of Science Honours Cyber Security and Forensic**

Computing

3. **University of Sunderland, Bachelor of Science Honours Cyber Security and Digital Forensic**

Kingston University, University of Portsmouth and University of Sunderland are considered with high ranks in the world for offering the similar course to the proposed Bachelor of Science Honours in Cyber Security and Digital Forensics. Benchmarking is done to identify the common features as well as need for improvement or advancement in comparison with Kingston University (KU), University of Portsmouth (UP) and University of Sunderland (US). This helps the proposed qualification to enhance their curriculum to match the requirements of the world universities. An overview summary of the qualifications is presented in Table 5.

Table 5: Cyber Security and Digital Forensic Qualification Comparison

Category	**Proposed Qualification**	**Kingston University**	**University of Portsmouth**	**University of Sunderland**
Course Name	Bachelor of Science Honours in Cyber Security and Digital Forensics	Bachelor of Science Honours in Cyber Security & Computer Forensics	Bachelor of Science Honours in Cyber Security and Forensic Computing	Bachelor of Science Honours in Cyber Security & Digital Forensics
Course Duration	1-year progression from Bachelor of Science in Cyber Security and Digital Forensics	3-year full time 4-year sandwich with work placement	3-year full-time, 4-year sandwich with work placement or foundation year	3-year full-time, 4-year sandwich with work placement
Internship	No placement	Placement with Extra one-year Training	Placement with Extra one-year Training	Placement with Extra one-year Training

Project work	Available	Available	Available	Available

Course Structure Analysis

The course structure of core courses for the proposed qualification, Kingston University, University of Portsmouth and University of Sunderland are discussed and further outlined in Table 6.

Similarities with the proposed program

The proposed qualification and benchmarking institutions are both offering an individual research. Ethical hacking is proposed and is offered by Kingston University and University of Portsmouth while University of Sunderland does not offer it. The proposed course structure include Advanced Cyber Security module, which is also offered by Kingston University and University of Sunderland while University of Portsmouth offer it as Cyber Security and Forensic Computing. The proposed qualification include Advanced Cloud Forensics and similar courses from benchmarking institutes include Cyber crime and Digital Forensics from Kingston University, Cyber Security and Forensic Computing from University of Portsmouth and Advanced Computer Forensics from University of Sunderland. Both the benchmarking institution and the proposed institutions have a number of electives that allow a student to specialise in an area of interest in Cyber Security and Digital Forensics.

Difference with the proposed program

One major difference between the proposed qualification to the three institutions is that the proposed qualification is only one year. This is because the proposed qualification is a progression from the Bachelor of Science in Cyber Security and Digital Forensics. The institutions used for benchmarking offer foundation courses in Cyber Security from year 1 and 2 which are almost similar to the Bachelor of Science in Cyber Security and Digital Forensics qualification. Year three of the benchmarking institutions offer advanced courses that align with the proposed qualification. The final year of both the proposed and institutions used for benchmarking have final year projects that have the research element. The proposed qualification has an additional group project that gives students the platform to work in advanced research topics in Cyber Security and Digital Forensics and also gain teamwork skills which are crucial industry. The curriculum provided in the proposed qualification covers all the knowledge area and additional modules that would satisfy the future needs of the students as well.

Table 6: Cyber Security and Digital Forensic Qualification Syllabi Comparison

S/N	Proposed Qualification	Kingston University	University of Portsmouth	University of Sunderland
1.	Individual Research Project in Cyber Security and Digital Forensics (Core)	Individual Project (Core)	Individual Project (Option)	Computing Project (Core)
2.	Group Project in Cyber Security and Digital Forensics (Core)	-	-	-
3.	Ethical Hacking and Investigation Techniques (core)	Ethical Hacking (Core)	Ethical Hacking (core) Forensic Investigations (core)	-
4.	Advanced Cyber Security I	Cyber Security (Core)	Cyber Security and Forensic Computing (Core)	Advanced Cyber Security (Core)
5.	Advanced Cloud Forensics (Core)	Cyber crime and Digital Forensics (Core)	Cyber Security and Forensic Computing (Core)	Advanced Computer Forensics (Core)

6.	Network Forensics (Elective)	Network and Mobile Security (Core)	-	Advanced Computer Forensics (Core)
7.	Human and Organizational Aspects of Information Security (core)	-	Cyber Law Governance and Human Rights (Option)	-
8.	Internet of Things Forensics (Elective)	Cyber crime and Digital Forensics (Core)	-	Advanced Computer Forensics (Core)
9.	Advanced Cyber Security II (Elective)	Cyber Security (Core)	-	Advanced Cyber Security (Core)
10.	Wireless and Mobile Security (Elective)	Network and Mobile Security (Core)	-	Advanced Cyber Security (Core)
11.	Data Visualization Analytics (Elective)	-	-	
12.	Malware Forensics (Elective)	-	Malware Forensics (Core)	Advanced Computer Forensics (Core)
13.	Cryptocurrencies, Blockchains and Applications (Elective)	-	-	-
14.	Big Data Technologies (Elective)	-	Virtualisation and Cloud Computing (Core)	-

15.	Compliance and Legal Issues (Elective)	-	Cyber Law Governance and Human Rights (Option)	Professional Issues in Cybersecurity and Digital Forensics (Core)
16.	Risk Management	-	-	-

10. REVIEW PERIOD

This qualification shall be reviewed every five years