هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2023
TPG-151

Program Specification

(Postgraduate)

Program Name:	**M.Sc. in Cybersecurity**
Program Code (as per the Saudi Standard Classification of Educational Levels and Specializations):	*Enter Program Code*.
Qualification Level:	Master Degree (Level 7)
Department:	Computer Science
College:	Faculty of Computing and Information
Institution:	Al-Baha University
Program Specification:	New ☑ updated* □
Last Review Date:	25-12-2023

*Attach the previous version of the Program Specification.

Table of Contents

A. Program Identification and General Information:

1. Program's Main Location:

Alaqiq Main Campus (Male Section)

Shahbah Main Campus (Female Section)

2. Branches Offering the Program (if any): None

None

3. System of Study:

✓ Coursework & Thesis	□ Coursework

4. Mode of Study:

✓ On Campus	□ Distance Education	□ Other ....(specify)

5. Partnerships with other parties (if any) and the nature of each: None

- Partnership Arrangement:
- Type of Partnership:
- Duration of Partnership:

6. Professions/jobs for which students are qualified:

- **Cybersecurity Specialist**
- **Cybersecurity Manager**
- **Cybersecurity Architect**
- **Cybersecurity Consultant**

7. Relevant occupational/ Professional sectors:

- **IT**
- **Security**
- **Banking**
- **Transports**
- **Education**
- **Power Grid**
- **Medication**
- **Marketing**

8. Major Tracks/Pathways (if any):

Major track/pathway	Credit hours (For each track)	Professions/jobs (For each track)
1. M.Sc. in Cybersecurity-Thesis Track	33	1. Cybersecurity Consultant

		2. Information Security Analyst 3. Cybersecurity Researcher 4. Security Operations Center (SOC) Analyst 5. Penetration Tester (Ethical Hacker) 6. Security Architect 7. Cybersecurity Manager 8. Incident Responder 9. Cryptographer 10. Security Software Developer
2. M.Sc. in Cybersecurity-Research Project Track	36	1. Cybersecurity Consultant 2. Information Security Analyst 3. Cybersecurity Researcher 4. Security Operations Center (SOC) Analyst 5. Penetration Tester (Ethical Hacker) 6. Security Architect 7. Cybersecurity Manager 8. Incident Responder 9. Cryptographer 10. Security Software Developer
9. Exit Points/Awarded Degree (if any): None		
Exit points/Awarded degree		Credit hours
1.		
8. Total credit hours: (Thesis Track: 33 CHs and Research Project Track: 36 CHs))		

B. Mission, Goals, and Program Learning Outcomes

1. Program Mission:

The Master of Science in Cybersecurity program is dedicated to the rigorous advancement of research and development in the field of cybersecurity. Our mission is to cultivate highly skilled national professionals, thereby bridging the existing gap in the Saudi labor market. This program aims to foster excellence and innovation, contributing significantly to the national cybersecurity landscape.

2. Program Goals:

- To keep pace with academic advances in international universities in the field of cybersecurity.
- To increase learners' experience by enabling them to solve academic and practical problems in cybersecurity area.
- To enable graduates to compete in the fields of cybersecurity.
- To support continuous development through partnerships with local and international companies.
- To connect programs through integrated courses designed and taught through advanced cybersecurity technology.
- To integrate academic programs by bridging the gap between theoretical advances and practical applications in cybersecurity.

3. Program Learning Outcomes:*

Knowledge and Understanding:	
K1	Describe methods and analytical approaches to research that contributes to extending knowledge in cybersecurity field.
K2	Theoretical deep understanding of cybersecurity concepts and practices to protect and defend cyber systems and respond to and recover from advanced cyber-attacks.
K3	Interpret and deeply comprehend knowledge in modern and advanced findings along with theories in cybersecurity.
Skills:	
S1	Employ and critically assess a diverse array of advanced techniques, methods, and practices, alongside specialized tools informed by the latest developments in cybersecurity.
S2	Implement advanced cyber research and innovative projects for cybersecurity product and service development, using quantitative and qualitative methods to handle data in complex contexts.
S3	Utilize and critically assess a variety of techniques and methods in advanced cybersecurity scenarios, while effectively communicating specialized knowledge and skills to diverse beneficiaries.

Values, Autonomy, and Responsibility:	
V1	Demonstrate ethical conduct, integrity, and responsible member in the cybersecurity community, managing tasks autonomously and taking a leadership role in professional projects and community service.
V2	Engage in proactive professional planning and decision-making with high autonomy, contributing effectively to the advancement of cybersecurity.

* * Add a table for each track (if any)

** Same PLOs for both tracks as they both focus on research, with more emphasize on research for Thesis Track (on S2)

C. Curriculum:

1. Curriculum Structure:

(Thesis Track)

Program Structure	Required/ Elective	No. of courses	Credit Hours	Percentage
Course	Required	7	21	63.8%
	Elective	2	6	18.%
Graduation Project (if any)				
Thesis (if any)	Required	1	6	18.1%
Field Experience(if any)				
Others (.....)				
Total		10	33	100%

(Research Project Track)

Program Structure	Required/ Elective	No. of courses	Credit Hours	Percentage
Course	Required	7	21	58.33%
	Elective	4	12	33.33%
Graduation Project (if any)				
Thesis (if any)				
Field Experience(if any)				
Research Project	Required	1	3	8.33%
Total		12	36	100%

2. Program Courses:

(Thesis Track)

Level	Course Code	Course Title	Required or Elective	Pre-Requisite Courses	Credit Hours	Type of requirements (Institution, College, or Program)
Level 1	CYBS60101	Fundamental of Cybersecurity	Required	None	3	
	CYBS60102	Intro to Cryptography	Required	None	3	
Level 2	CYBS60103	Advanced Analysis and Design of Algorithms	Required	None	3	
	CYBS60201	Advanced. Programming in Cybersecurity	Required	Advanced Analysis & Design of Algorithms	3	
Level	CYBS60202	Operating System Security	Required	None	3	

Level	Course Code	Course Title	Required or Elective	Pre-Requisite Courses	Credit Hours	Type of requirements (Institution, College, or Program)
3	CYBS60203	Network Security	Required	None	3	
Level 4	CYBS 60301	Research Methods in Computer Science	Required	None	3	
		Elective I from Group A	Elective		3	
Level 5		Elective II from Group B	Elective		3	
	CYBS6999	Thesis	Required	Passed all core courses & Research Methods in CS	6	
Level 6						

(Research Project Track)

Level	Course Code	Course Title	Required or Elective	Pre-Requisite Courses	Credit Hours	Type of requirements (Institution, College, or Program)
Level 1	CYBS60101	Fundamental of Cybersecurity	Required	None	3	
	CYBS60102	Intro to Cryptography	Required	None	3	
Level 2	CYBS 60103	Advanced Analysis and Design of Algorithms	Required	None	3	
	CYBS60201	Advanced. Programming in Cybersecurity	Required	Advanced Analysis & Design of Algorithms	3	
Level 3	CYBS60202	Operating System Security	Required	None	3	
	CYBS60203	Network Security	Required	None	3	
Level 4	CYBS60301	Research Methods in Computer Science	Required	None	3	
		Elective I from Group A	Elective		3	
Level 5		Elective II from Group A	Elective		3	
		Elective III from Group B	Elective		3	
Level 6		Elective IV from Group C	Elective		3	
	CYBS6555	Research Project	Required	Passed all core courses	3	

3. Course Specifications:

Insert hyperlink for all course specifications using NCAAA template (T-104)

https://drive.google.com/drive/folders/1KKeRGJ4Fs7wbfJ2D7iT0z7LmO_wE3Kf8?usp=drive_link

4. Program learning Outcomes Mapping Matrix:

Align the program learning outcomes with program courses, according to the following desired levels of performance *(I = Introduced   P = Practiced   M = Mastered).*

Course code & No.	Program Learning Outcomes										
	Knowledge and understanding				Skills				Values, Autonomy, and Responsibility		
	K1	K2	K3	---	S1	S2	S3	---	V1	V2	V3
1. CYBS60101	P	P	M		I						
2. CYBS60102	I	P				P					
3. CSIC60103	I	P			P						
4. CYBS60201	I	M	M			M	P				
5. CYBS60202	I	P	P			P	P				
6. CYBS60203		M	M			M					
7. CYBS6999		M	M			M	M		M		M
8.CYBS6555		M	M			M	M		M	M	M
9. CSIC60301		P	M		M	P			M		
10. CYBS60302		M	P		P		P				M
11. CYBS60303		M	P		P		P				M
12. CYBS60304		I	P			P	P				M
13. CYBS60305	I	P			P	P			M		
14. CYBS60306	I	P			P	P			M		M
15. CYBS60307	I	P			P	P			M		
16. CYBS60308	I	P	M		P	M	I			M	I
17. CYBS60309	I	P	M		P						
18. CYBS60310	I	P	M		P						
19. CYBS60311	I	P	M		P						
20. CYBS60312	I	P				P					
21. CYBS60313		I	P		P				M	M	
22. CYBS60314	I	P				P	P		M	M	

Course code & No.	Program Learning Outcomes										
	Knowledge and understanding				Skills				Values, Autonomy, and Responsibility		
	K1	K2	K3	---	S1	S2	S3	---	V1	V2	V3
23. CYBS60315		M	M			M					

* Add a separated table for each track (if any).

* Course-PLO matrix are the same for both track; however, CLO-PLO weight matrix might be different for each cohort based on track and the set of selected elective courses.

5. Teaching and learning strategies applied to achieve program learning outcomes:

Describe teaching and learning strategies, to achieve the program learning outcomes in all areas.

1. Traditional and flipped classroom teaching strategies and blended learning: Encouraging instructors to use wide variations of teaching strategies for full student involvement and knowledge gain.

2. Case Studies and Simulations: Engage students in real-world cybersecurity case studies and simulations to develop practical problem-solving skills and critical thinking abilities.

3. Hands-On Online tools and Projects: Offer hands-on experiential learning opportunities through online tools sessions and projects that involve working with cybersecurity tools, techniques, and technologies.

4. Collaborative Learning: Encourage group projects and collaborative assignments to foster teamwork, communication, and peer learning among students.

5. Cybersecurity Competitions: Participate in or organize cybersecurity competitions and challenges to promote a competitive yet cooperative environment for honing skills and knowledge.

6. Research and Analysis: Emphasize research-oriented assignments and analysis of cybersecurity threats, vulnerabilities, and countermeasures to enhance analytical and investigative skills.

7. Ethical Hacking and Penetration Testing: Provide opportunities for students to engage in ethical hacking exercises and penetration testing to understand offensive security techniques and reinforce defensive strategies.

6. Assessment Methods for program learning outcomes:

Describe assessment methods (Direct and Indirect) that can be used to measure the achievement of program learning outcomes in all areas.

The program should devise a plan for assessing Program Learning Outcomes (all learning outcomes should be assessed at least once in the program's cycle).

The program should devise a plan for assessing Program Learning Outcomes (all learning outcomes should be assessed at least twice in the bachelor program's cycle and once in other degrees).

Course Learning Outcomes	Assessment Methods
• K1	• Assignments, quizzes, examinations and discussion
• K2	• Assignments, quizzes, examinations and discussion
• K3	• Assignments, quizzes, examinations and discussion
• S1	• Assignments, projects, examinations and discussion
• S2	• Assignments, projects, examinations and research evaluation
• S3	• Assignments, projects, examinations and research evaluation
• V1	• Student extra activities, discussion, reports and assignments evaluation
• V2	• Student extra activities, discussion, reports and assignments evaluation

D. Thesis and Its Requirements (if any):

1. Registration of the thesis:

(Requirements/conditions and procedures for registration of the thesis as well as controls, responsibilities and procedures of scientific guidance)

Requirements:

- A successful completion of all core courses
- A successful completion of Research Methods in Computer Science course
- Registration for the thesis is anticipated at higher academic levels

Procedure:

- A list of allegeable supervisors is distributed to allegeable students along with their research interest, list of publications, and contact information
- Students, with anticipated supervisor, or supervisor committee, submit a short proposal to the program management
- Proposal and supervisor eligibility is evaluated by the program management (or postgraduate studies committee) and initial acceptance is issued

- A certificate from King Fahad Library is requested for the originality of the title
- Thesis Title and Supervisor/Supervision Committee are approved by department council, then college council.
- Student is enrolled in the thesis course (register) the next semester

2. Scientific Supervision:

(The regulations of the selection of the scientific supervisor and his/her responsibilities, as well as the procedures/ mechanisms of the scientific supervision and follow-up)

Each student is required to collaborate in selecting an academic advisor for their thesis. The Duties of the academic advisor include the following:

- Assisting the student in selecting an appropriate topic for the thesis.
- Offering guidance in the preparation of a research proposal, ensuring it aligns with the standards set by the Deanship of Graduate Studies, or the alternative University Committee
- Submitting regular progress reports on the student's work to the department chair at the end of each semester.
- Providing a comprehensive final report upon the student's successful completion of the thesis.

3.Thesis Defense/Examination:

(The regulations for selection of the defense/examination committee and the requirements to proceed for thesis defense, the procedures for defense and approval of the thesis, and criteria for evaluation of the thesis)

- All thesis topics must be approved by the department council
- The composition of the thesis committee, including the chair and members, requires approval by the department council.
- The committee must consist of an odd number of members, with a minimum of three members.
- At least one member of the committee should hold the rank of Professor or Associate Professor.
- Approval of the thesis necessitates the agreement of at least two-thirds of the committee members.
- Committee members are obligated to complete the thesis approval form, documenting their decision and providing recommendations, if any.

H. Student Admission and Support:

1. Student Admission Requirements:

Requirements of admission to the program:

- English proficiency test (minimum of 3.5 IELTS scores in all parts or equivalent proficiency test such as TOEFL and STEP)
- Applicant should have a bachelor's degree in one of the specializations of computer, including: Computer Science, Information Systems, Information Technology, and Computer Engineering.
- Applicant should be nominated as follows:

GPA	Postgraduate General Aptitude Test	English Score	Specialization Relevance
50%	30%	10%	10%

- Meet any additional conditions stipulated by the admissions deanship of higher education and/or faculty of computer science and information technology.

Note: Transferred requirement and courses equivalency will be considered as case by case basis.

2. Guidance and Orientation Programs for New Students:

(Include only the exceptional needs offered to the students of the program that differ from those provided at the institutional level).

The process for preparation of new faculty and teaching staff includes:

- Meeting with program-coordinator, department head and dean
- Providing faculty handbook
- Attending of new faculty orientation
- Attending of workshop/s of deanship of development

3. Student Counseling Services:

(Academic, professional, psychological and social)

(Include only the exceptional needs offered to the students of the program that differ from those provided at the institutional level)

Academic advisors will be assigned to groups of students to provide counseling services.

4. Special Support:

(Low achievers, disabled, , and talented students).

As provided by the university, all facilities in campus have already considered support for special need students.

E. Faculty and Administrative Staff:

1. Needed Teaching and Administrative Staff:

Academic Rank	Specialty		Special Requirements / Skills (if any)	Required Numbers		
	General	Specific		M	F	T
Professor	2	2	CS, Cybersecurity	2	2	
Associate Professor	2	2	Computer Science	3	1	
Assistant Professor	7	4	CS, Cybersecurity	7	4	
Lecturer						
Teaching Assistant						
Technicians and Laboratory Assistant	1	1		1	1	
Administrative and Supportive Staff	2			1	1	
Others (specify)						

F. Learning Resources, Facilities, and Equipment:

1. Learning Resources:

Learning resources required by the Program (textbooks, references, and e-learning resources and web-based resources, etc.)

The required textbooks, references, and other resources for teaching are identified by the instructor teaching the course. The instructor's suggestions are submitted to the Department Council. All suggestions are collected and are reviewed by Library Committee. The Department council approves the Library Committee Decision. The Deanship of Computers and Information Technology will send list of textbooks and the references to the Library Deanship. According to the University regulation, the Library deanship is responsible to provide the requirements.

By the end of each academic year, each department should submit a list of required textbook or other related resources to the Dean of the college. The Dean is then submitting the request to Deanship of Libraries Affair or Deanship of Information Technology to process.

The curriculum development and assessment committee advices and monitors acquisition of textbook

2. Facilities and Equipment:

(Library, laboratories, classrooms, etc.)

The required software, hardware and other resources for teaching are identified by the instructor teaching the course. The instructor's suggestions are submitted to the Department Council. All suggestions are collected and are reviewed by Technical Committee. The Department council approves the Technical Committee Decision. The Deanship of Computers and Information Technology will send the list to the Deanship of e-Learning and Information Technology. According to the University regulation, the e-Learning and Information Technology deanship is responsible to provide the requirements.

By the end of each academic year, each department should submit a list of required software and hardware for teaching to the Dean of the college. The Dean is then submitting the request to Deanship of e-Learning and Information Technology to process.

3. Procedures to ensure a healthy and safe learning environment:

(According to the nature of the program)

E-learning and IT Deanship is responsible for providing a healthy and safe environment of laboratories and other IT and communications equipment/environment according to the safety standard from the university.

G. Program Quality Assurance:

1. Program Quality Assurance System:

Provide a link to quality assurance manual.

1. Program's quality system manual - Google Drive

2. Program Quality Monitoring Procedures:

- Program quality is monitored by the quality assurance system of the university, which include a program management headed by the department head, then a college level committee headed by the dean of the college, and a Review unit under the deanship of Development and Quality, which is associated directly with H.E University President
- By law and policies, many of the program procedures are supervised and followed up by the Deanship of research, especially procedure related to course registration, thesis, program progress and completion, and final graduation.

- Program quality is governed by the same committees of the CS Department, and its related procedures and decisions are discussed at the Department council

3. Procedures to Monitor Quality of Courses Taught by other Departments:

- All program courses belong to the same department, CS Department. Each course has a course coordinator from the department
- Specialized professors and experts from other departments are enabled to teach some students groups, however, course coordinators from the department monitor the quality of course delivery and assessment. All final exams for the same course are unified.
- Co-supervisors are allowed from other departments, if needed, however, main supervisors are always from the CS department

4. Procedures Used to Ensure the Consistency between within the main campus:

(including male and female sections).

Male and female sections have the most possible coordination to assure consistency, the practices include:

A coordinator assigned for each course to coordinate topics covered, assessments, CLOs compliance,

5. Assessment Plan for Program Learning Outcomes (PLOs):

The program will use the following for the assessment for the PLOs:

- Grade-Based
- Course-Exit Survey
- Rubrics

At the end of each academic year, the coordinator of the program will summarize all the PLOs assessment results and recommendations for improvements from the course reports. Then a report on the PLO assessment will be submitted to the head of the department for further actions.

6. Program Evaluation Matrix:

Evaluation Areas/Aspects	Evaluation Sources/References	Evaluation Methods	Evaluation Time
Leadership	Faculty, Program Leaders	Survey, interview	End of academic year

Evaluation Areas/Aspects	Evaluation Sources/References	Evaluation Methods	Evaluation Time
Effectiveness of teaching and assessment	Faculty, Program Leaders, Peer Reviewer	Survey, interview, visit	End of academic year
Learning resources	Students, Program Leaders, Peer Reviewer	Survey	End of academic year
Extent of achievement of course learning outcomes	Faculty, Program Leaders	Survey	End of academic year

Evaluation Areas/Aspects (e.g., leadership, effectiveness of teaching & assessment, learning resources, services, partnerships, etc.)
Evaluation Sources (students, graduates, alumni, faculty, program leaders, administrative staff, employers, independent reviewers, and others.
Evaluation Methods (e.g., Surveys, interviews, visits, etc.)
Evaluation Time (e.g., beginning of semesters, end of the academic year, etc.)

7. Program KPIs:*

The period to achieve the target (____) year(s).

No.	KPIs Code	KPIs	Targeted Level	Measurement Methods	Measurement Time
1	CYB-PLO-K1	Knowledge	75%	Grading	Each end of semester
2	CYB-PLO-K2	Knowledge	75%	Grading	Each end of semester
3	CYB-PLO-K3	Knowledge	75%	Grading	Each end of semester
4	CYB-PLO-S1	Skill	75%	Grading	Each end of semester
5	CYB-PLO-S2	Skill	75%	Grading	Each end of semester
6	CYB-PLO-S3	Skill	75%	Grading	Each end of semester
7	CYB-PLO-C1	Competence	75%	Grading	Each end of semester
8	CYB-PLO-C2	Competence	75%	Grading	Each end of semester
9	CYB-PLO-C3	Competence	75%	Grading	Each end of semester

*including KPIs required by NCAAA

H. Specification Approval Data:

Council / Committee	
Reference No.	
Date	