Program Specification

(Postgraduate)

Program Name:	**Master of Science in Cybersecurity (MS in Cybersecurity)**
Program Code (as per the Saudi Standard Classification of Educational Levels and Specializations):	**061203**
Qualification Level:	Master
Department:	Computer Science
College:	Science
Institution:	Northern Border University
Program Specification:	New ☒ updated* ☐
Last Review Date:	write here

*Attach the previous version of the Program Specification.

Table of Contents

A. Program Identification and General Information:

1. Program's Main Location:

The program offers in the main campus only (Arar)

2. Branches Offering the Program (if any):

NA

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:

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

6. Professions/jobs for which students are qualified:

The Master of Science in Cybersecurity (MS in Cybersecurity) is meticulously designed to equip students with an arsenal of skills essential for defining and executing organization-wide strategies, programs, and policies. Beyond the technical intricacies of cybersecurity, this program instills a profound awareness of technology's pivotal role in securing competitive strategic advantages and enhancing productivity. Graduates emerge not only with a robust understanding of cybersecurity's technical foundations but also with a keen focus on information risk management, trusted computing, legal ramifications of incidents, and the evaluation and implementation of cutting-edge solutions .

Some examples of Professions/jobs for which students are qualified:

المهنة	Job Code	Job Name
رئيس أمن سيبراني	112010	Head of Cyber Security
مدير موارد بشرية أمن سيبراني	121216	Human Resources Manager Cyber Security
مدير أمن سيبراني	133012	Cyber Security Manager
مدرب أمن سيبراني	235604	Cyber Security Trainer
أخصائي استشارات أمن سيبراني	242126	Cyber Security Consulting Specialist
أخصائي مخاطر أمن سيبراني	242127	Cyber Security Risk Specialist
أخصائي التزام في الأمن سيبراني	242128	Cyber Security Compliance Specialist
مُقيّم ضوابط أمن سيبراني	242129	Cybersecurity Controls Evaluator
مدقق أمن سيبراني	242130	Cyber Security Auditor
أخصائي حوكمة الأمن سيبراني	242207	Cyber Security Governance Specialist
أخصائي أمن سيبراني	251106	Cyber Security Specialist
مطور أمن سيبراني	251206	Cyber Security Developer

مقيم أمن سيبراني للبرمجيات	251901	Software Cyber Security Evaluator
باحث أمن سيبراني	251904	Cyber Security Researcher
أخصائي بنية تحتية للأمن السيبراني	252207	Cybersecurity Infrastructure Specialist
أخصائي استجابة للحوادث السيبرانية	252903	Cyber Incident Response Specialist
محلل دفاع الأمن السيبراني	252904	Cybersecurity Defense Analyst
محلل معلومات التهديدات السيبرانية	252915	Cyber Threat Intelligence Analyst
أخصائي اكتشاف التهديدات السيبرانية	252916	Cyber Threat Detection Specialist
أخصائي تحقيقات جرائم سيبرانية	252922	Cybercrime Investigation Specialist
أخصائي قانوني أمن سيبراني	261107	Cybersecurity Legal Specialist
مساعد أمن سيبراني	351305	Cyber Security Assistant

7. Relevant occupational/ Professional sectors:

The relevance of cybersecurity extends across a wide array of occupational and professional sectors, reflecting its critical role in safeguarding digital assets, ensuring data privacy, and fortifying organizational resilience against cyber threats. Some of the key sectors where cybersecurity professionals play a pivotal role include:

- Government and Defense
  - Ministry of defense
  - Army
  - Intelligence Agency
  - All the ministries.
- Financial Services
  - Ministry of Finance
  - Banks
  - Insurance company
  - Stock market
- Healthcare
  - Ministry of health
  - hospitals
- Technology and Software Development
  - Private companies
  - Development software company
- Critical Infrastructure
  - Ministry of Communication
  - Communication company like STC, Zain, Salam etc..
- Retail and E-commerce
  - Ministry of Commerce
  - E-commerce and E-shopping company
- Education
  - Ministry of education

- Universities

8. Major Tracks/Pathways (if any): NA		
Major track/pathway	**Credit hours** (For each track)	**Professions/jobs** (For each track)

9. Exit Points/Awarded Degree (if any): NA	
Exit points/Awarded degree	Credit hours

10. Total credit hours: (36)

B. Mission, Goals, and Program Learning Outcomes

1. Program Mission:

Empowering cybersecurity leaders through advanced education, enhancing digital security and supporting innovation in the Kingdom.

1. Consistency of the program mission with the mission of the college and the university

Domains of consistency	Teaching and Learning	Research and Innovation	Community Engagement	Other		Number of words
University mission	We are a regionally serving, comprehensive university committed to educational excellence. Guided by our core values, heritage, and place, We deliver innovative educational programs characterized by outcomes that leverage the human, economic, cultural, and natural resources for the Northern Borders Region and beyond.					
Consistency of the university's mission with consistency areas	✓	✓	✓			43
College mission	Providing academic programs in basic sciences and its applications, outstanding research that meet the region's needs, and contributing to the development of community.					
Keywords from the college mission through which consistency is achieved	Teaching and Learning	Research and Innovation	Community Engagement			Number of words
Academic program	✓					**23**
Scientific research		✓				
Developing the community			✓			
Program Mission	Empowering cybersecurity leaders through advanced education, enhancing digital security and supporting innovation in the Kingdom.					
Keywords from program mission through which consistency is achieved	Teaching and Learning	Research and Innovation	Community Engagement			Number of words
advanced education	✓					**15**
supporting innovation		✓				
Enhancing digital security in the Kingdom.			✓			

2. Program Goals:

1. **Developing Practical Expertise**: To equip students with the practical and technical skills needed to tackle contemporary digital security challenges.
2. **Focus on Innovation**: To encourage innovation and research in the field of cybersecurity, keeping pace with technological developments.
3. **Enhancing Digital Security**: To contribute to the improvement of information and data security at both national and global levels.
4. **Building Leadership**: To prepare students to be leaders in cybersecurity, capable of making effective strategic decisions.

5. **Integration with job Market**: To develop strong relationships with the job Market to ensure the alignment of education with market needs.

2.1 Consistency of the goals of the developed program with the mission of the program

Developed program goals	Domains of consistency with the mission of the program			
	Research and innovation	Community engagement	Teaching and learning	
PG1	✓		✓	
PG2	✓		✓	
PG3		✓		
PG4		✓		
PG5		✓		

2.2 Consistency of the goals of the program with the goals of the college and the goals of the university

University goals		Goals numbers
UG1	Providing excellent education that sharpens intellect and professionalism.	4
UG2	Stimulating research and innovation following the university's research priorities.	
UG3	Developing community partnership.	
UG4	Developing an administrative and financial system that enhances management efficiency and diversifies sources of income.	

College objectives		Objectives numbers
CO1	Providing academic programs in basic sciences and their applications that meet labour market requirements	4
CO2	Increasing research productivity	
CO3	Enhancing community partnerships.	
CO4	Attaining academic accreditation	

College objectives	Matrix of consistency of College objectives with the objectives of the university			
	UO1	UO2	UO3	UO4
CO1	✓			
CO2		✓		
CO3			✓	
CO4				✓

	Matrix of consistency of program goals with the goals of the college			
Program goals	CG1	CG2	CG3	CG4
PG1	✓	✓		
PG2		✓		

PG3			✓	
PG4	✓		✓	
PG5	✓			

2.3 Consistency of the goals of the developed program with NBU Graduate Attributes

Northern Border University Graduates Attributes		
GA1	**National identity**	Demonstrate high standards of ethical and socially responsible behavior, as well as academic and professional honesty and integrity; contribute to finding solutions to social problems; and commit to being a responsible citizen.
GA2	**Self-management**	Demonstrate self-management skills, self-learning and critical thinking, the ability to take initiative to self-develop according to specific standards, and ability to present evidence and arguments to make a decision unbiasedly.
	Critical thinking	
GA3	**Digital culture**	Effectively use information technology, analytical, mathematical, and statistical tools to perform data analysis, suggest solutions, and solve problems using critical thinking.
GA4	**Teamwork**	Have the ability to lead a team, assume responsibility for performing tasks and developing work, achieve goals effectively, and promote health, psychological and social aspects.
GA5	**Entrepreneurship**	Identify the function of entrepreneurship and its requirements in the successful, commercial application.
GA6	**Communication skills**	Effectively communicate both verbally and in writing, using appropriate presentation forms, scholarly language, adequate reasoning for various issues and dealing with beneficiaries.

Program goals	Consistency Matrix of the goals of the program with NBU Graduates Attributes						
	GA1	GA2		GA3	GA4	GA5	GA6
	National identity	Self-management	Critical thinking	Digital culture	Teamwork	Entrepreneurship	Communication skills
PG1	✓			✓			
PG2				✓		✓	
PG3	✓			✓			✓
PG4		✓			✓		✓
PG5						✓	

3. Program Learning Outcomes: *

Knowledge and Understanding:	
K1	Ability to understand advanced concepts and principles in cybersecurity, including cryptography, network security, and secure software development, with a focus on critical analysis and practical application of these principles in complex environments.
K2	Proficiency in understanding the technological underpinnings of cybersecurity threats and defenses, including malware analysis, penetration testing, and intrusion detection.
Skills:	
S1	Ability to apply cybersecurity tools and techniques to assess, mitigate, and manage security risks across diverse digital environments.

S2	Implementing security controls to protect data, systems, and networks from cyber threats, vulnerabilities, and exploits.
Values, Autonomy, and Responsibility:	
V1	Commitment to upholding ethical principles and professional standards in cybersecurity practice, including honesty, integrity, and respect for user privacy and confidentiality.
V2	Develop the ability for independent and critical thinking to identify emerging cybersecurity threats, and recognize the importance of lifelong learning and continuous professional development in the field of cybersecurity

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

C. Curriculum:

1. Curriculum Structure:

Program Structure	Required/ Elective	No. of courses	Credit Hours	Percentage
Course	Required	4	12	33.3
	Elective	4	12	33.3
Graduation Project (if any)				
Thesis (if any)		1	12	33.3
Field Experience (if any)				
Others (Thesis)				
Total		9	36	100

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

2. Program Courses:

Level	Course Code	Course Title	Required or Elective	Pre-Requisite Courses	Credit Hours	Type of requirements (Institution, College, or Program)
Level 1	MCY601	Introduction To Cybersecurity	Required	None	3	Program
	MCY602	Network Security	Required	None	3	Program
	MCY603	Cryptography	Required	None	3	Program
	MCYxxx	xxx	Elective		3	Program
Level 2	MCY604	Software Secure Assurance	Required	MCY601	3	Program
	MCY605	xxx	Elective		3	Program
	MCYxxx	xxx	Elective		3	Program
	MCYxxx	xxx	Elective		3	Program
Level 3	MCY621	Thesis	Required	Complete 24 Cr.H	12	Program
Elective	MCY611	Cloud security	Elective	MCY601, MCY602	3	Program
	MCY612	Operating systems security	Elective	MCY601, MCY602	3	Program
	MCY613	Penetration testing and ethical hacking	Elective	MCY601, MCY602	3	Program
	MCY614	Malware Analysis and Defense	Elective	MCY601, MCY602	3	Program
	MCY615	Risk Management in Cybersecurity	Elective		3	Program
	MCY616	Digital forensics and incident Response	Elective		3	Program
	MCY617	Artificial Intelligence for Cyber Security	Elective		3	Program
	MCY618	IoT and Blockchain Security	Elective	MCY601, MCY602	3	Program

* Include additional levels (for three semesters option or if needed).
** Add a table for the courses of each track (if any)

3. Course Specifications:

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

All course specifications using NCAAA template (T-104)

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	S1	S2	V1	V2
Introduction To Cybersecurity	I	I	I	I	I	
Network Security	I	I	I	I	I	
Cryptography	I	I	I	I	I	
Risk Management in Cybersecurity	I	I	I	I	I	
Digital forensics and incident Response	I		I	I		I
Artificial Intelligence for Cyber Security	I	I	I	I		I
Software Secure Assurance	P	P	P	P		P
Cloud security	P	P	P	P	P	
IoT and Blockchain Security	P	P		P	P	
Penetration testing and ethical hacking	M	M	M	M	M	M
Malware Analysis and Defense	M		M	M	M	
Operating systems security	M	M		M	M	
Thesis	M	M	M	M	M	M

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

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.

The MS in Cybersecurity Program is committed to fostering a dynamic learning environment where students cultivate expertise in cybersecurity through a blend of theory, industry best practices, and hands-on application. With an emphasis on student-centered learning, our approach empowers students as active participants in their educational journey, equipping them with the skills and knowledge necessary for success in the field.

To achieve the program learning outcomes in all areas of a cybersecurity degree program, various teaching and learning strategies can be implemented. Here's a description of some effective strategies:

1. Lectures and Presentations: Traditional lectures and presentations delivered by faculty members provide students with foundational knowledge and understanding of cybersecurity concepts, principles, and theories. These sessions may include multimedia materials, case studies, and real-world examples to illustrate key concepts and foster engagement.

2. Hands-On Labs and Practical Exercises: Hands-On labs and practical exercises allow students to apply theoretical knowledge to real-world scenarios in a controlled environment. Through lab sessions, students gain practical skills in cybersecurity tools, techniques, and technologies, such as penetration testing, network analysis, and cryptography.

3. Group Projects and Collaborative Learning: Group projects and collaborative learning activities encourage teamwork, communication, and problem-solving skills among students. By working together on cybersecurity projects, such as developing security policies, conducting risk assessments, or designing secure software applications, students learn to collaborate effectively and leverage each other's strengths.

4. Case Studies and Simulations: Case studies and simulations immerse students in realistic cybersecurity scenarios, enabling them to analyze complex problems, make informed decisions, and develop strategies to mitigate security risks. These interactive learning experiences help students develop critical thinking skills and apply theoretical knowledge to practical situations.

5. Guest Lectures and Industry Speakers: Inviting guest lecturers and industry speakers from cybersecurity professionals, practitioners, and researchers enriches students' learning experiences by providing insights into current trends, emerging technologies, and real-world applications of cybersecurity concepts. Guest speakers may share their experiences, expertise, and career advice with students, inspiring them to pursue careers in cybersecurity.

6. **Research Thesis and Independent Study:** Research thesis and independent study opportunities allow students to delve deeper into specific areas of cybersecurity that align with their interests and career goals. Under the guidance of faculty mentors, students conduct original research, explore advanced topics, and contribute to the body of knowledge in cybersecurity through scholarly inquiry and investigation.

It can be summarize in the following table:

Program Learning Outcomes: *		Teaching Strategies
Knowledge and Understanding:		
K1	Ability to understand advanced concepts and principles in cybersecurity, including cryptography, network security, and secure software development, with a focus on critical analysis and practical application of these principles in complex environments.	- Lectures and readings on core concepts - Flipped classroom, - self-reflection, - pros-cons grid - Interactive discussions and Q&A sessions - Case studies on real-world applications

		- Tutorials on fundamental principles - Online modules and resources
K2	Proficiency in understanding the technological underpinnings of cybersecurity threats and defenses, including malware analysis, penetration testing, and intrusion detection.	- Hands-on labs and simulations - Demonstrations of tools and techniques - Guest lectures from industry experts - Workshops and seminars - Collaborative group projects
Skills:		
S1	Ability to apply cybersecurity tools and techniques to assess, mitigate, and manage security risks across diverse digital environments.	- Lab sessions with cybersecurity tools - Real-world scenario simulations - Team-based projects and role-playing exercises - Case study analysis - Use of virtual environments and sandboxes
S2	Implementing security controls to protect data, systems, and networks from cyber threats, vulnerabilities, and exploits.	- Design and implementation projects - Role-playing in incident response simulations - Peer-to-peer teaching and presentations - Use of software development platforms - Collaboration with industry partners for real-world projects
Values, Autonomy, and Responsibility:		
V1	Commitment to upholding ethical principles and professional standards in cybersecurity practice, including honesty, integrity, and respect for user privacy and confidentiality.	- Discussions on ethics and professional standards - Case studies on ethical dilemmas - Role-playing ethical decision-making
V2	Develop the ability for independent and critical thinking to identify emerging cybersecurity threats, and recognize the importance of lifelong learning and continuous professional development in the field of cybersecurity	- Independent research projects - Critical analysis of current events in cybersecurity - Encouragement of continuous learning through online courses - Discussion forums on emerging trends - Mentorship and guidance from faculty

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).

Assessing the achievement of program learning outcomes in all areas of a cybersecurity program requires a combination of direct and indirect assessment methods tailored to each outcome. Here's how different assessment methods can be used:

1. Direct Assessment Methods:

- **Examinations:** Written exams, quizzes, and practical assessments can directly measure students' knowledge and understanding of cybersecurity concepts, principles, and theories. Examinations may

include multiple-choice questions, short-answer questions, and hands-on tasks that assess students' ability to apply theoretical knowledge to practical scenarios.

- **Lab Assignments and Projects:** Hands-on lab assignments and projects provide direct evidence of students' skills in applying cybersecurity tools, techniques, and technologies to real-world scenarios. Assessments may include analyzing network traffic, conducting vulnerability assessments, and implementing security controls to mitigate risks.
- **Thesis Evaluation:** For programs with a thesis component, evaluating the quality of students' thesis research and writing directly assesses their ability to conduct independent research, analyze data, and make original contributions to the field of cybersecurity. Thesis evaluations may consider factors such as research methodology, data analysis, and scholarly writing.

2. Indirect Assessment Methods:

- **Surveys and Questionnaires:** Surveys and questionnaires can gather indirect feedback from students, alumni, employers, and other stakeholders to assess program learning outcomes related to skills, values, autonomy, and responsibility. Surveys may include Likert-scale questions, open-ended responses, and qualitative feedback on students' perceptions of their learning experiences and preparedness for cybersecurity careers.
- **Course Evaluations:** Course evaluations allow students to provide feedback on individual courses, instructors, and instructional methods, which can indirectly assess the effectiveness of teaching and learning strategies in achieving program learning outcomes. Course evaluations may include ratings of course objectives, instructional materials, and instructor effectiveness in facilitating learning.
- **Portfolio Review:** Reviewing student portfolios of coursework, projects, and research artifacts provides indirect evidence of students' attainment of program learning outcomes across multiple courses and learning experiences. Portfolios may include written assignments, presentations, code samples, and other artifacts that demonstrate students' growth and achievement over time.

It can be summarize in the following table:

Program Learning Outcomes: *		Teaching Strategies
Knowledge and Understanding:		
K1	Ability to understand advanced concepts and principles in cybersecurity, including cryptography, network security, and secure software development, with a focus on critical analysis and practical application of these principles in complex environments.	- Written exams - Quizzes - Class participation and engagement in discussions - Assignment-based assessments - Group projects on case studies
K2	Proficiency in understanding the technological underpinnings of cybersecurity threats and defenses, including malware analysis, penetration testing, and intrusion detection.	- Practical lab assessments - Problem-based assignments - Project reports and presentations - Peer reviews and feedback sessions
Skills:		
S1	Ability to apply cybersecurity tools and techniques to assess, mitigate, and manage security risks across diverse digital environments.	- Practical lab assessments - Problem-based assignments - Project reports and presentations - Peer reviews and feedback sessions

S2	Implementing security controls to protect data, systems, and networks from cyber threats, vulnerabilities, and exploits.	- Project presentations and demonstrations - Design and implementation reports - Peer reviews and feedback - Practical exams - Assessment of communication skills through written and oral presentations
Values, Autonomy, and Responsibility:		
V1	Commitment to upholding ethical principles and professional standards in cybersecurity practice, including honesty, integrity, and respect for user privacy and confidentiality.	- Participation in ethics discussions - Case study analyses - Assessment of role-playing exercises - Evaluation of adherence to ethical guidelines in projects
V2	Develop the ability for independent and critical thinking to identify emerging cybersecurity threats, and recognize the importance of lifelong learning and continuous professional development in the field of cybersecurity	- Research project reports - Presentations on emerging threats - Participation in continuous learning activities - Critical analysis papers - Feedback from mentors and faculty

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)

The process of registering a thesis involves several requirements, conditions, and procedures to ensure that students are adequately prepared and supported throughout their thesis research. Here's an outline of the requirements and procedures for registering a thesis, along with the controls, responsibilities, and procedures of scientific guidance:

1. Eligibility Requirements:

- Students must meet specific eligibility criteria to register for a thesis, which include: completing all the coursework, maintaining a minimum of 80% GPA, and obtaining approval from their academic advisor or program coordinator.

2. Topic Selection:

- Students select a thesis topic in consultation with their academic advisor or a faculty member with expertise in their area of interest. The topic should align with the student's academic and career goals and contribute to the body of knowledge in cybersecurity.

3. Thesis Proposal:

- Students are required to prepare a thesis proposal outlining the research questions, objectives, methodology, and expected contributions of their thesis project. The proposal should be reviewed and approved by a thesis committee composed of faculty members with relevant expertise.

4. Registration Process:

- Once the thesis proposal is approved, students complete the registration process according to the guidelines and procedures established by the academic department or program. This may involve submitting the thesis proposal, completing registration forms, and paying any associated fees.

5. Scientific Guidance:

- Upon registration, students are assigned a scientific advisor or thesis supervisor who provides guidance and support throughout the thesis research process. The scientific advisor helps students refine their research objectives, develop a research plan, and navigate challenges encountered during the research.

6. Progress Monitoring:

- Throughout the thesis research period, students are required to meet regularly with their scientific advisor to discuss progress, address any issues or concerns, and receive feedback on their work. The scientific advisor monitors the student's progress and provides guidance to ensure that the thesis meets academic standards and objectives.

7. Thesis Defense Preparation:

- As the thesis nears completion, students prepare for a thesis defense, where they present their research findings, methodology, and conclusions to a thesis committee. The scientific advisor assists students in preparing for the defense, including rehearsal presentations, addressing potential questions, and ensuring that the thesis meets all requirements.

8. Thesis Submission:

- After successfully defending the thesis, students make any necessary revisions or corrections based on feedback from the thesis committee. Once the thesis is finalized, students submit the completed thesis document according to the submission guidelines and deadlines established by the academic department or program.

9. Evaluation and Grading:

- The thesis is evaluated and graded by the thesis committee based on the quality of the research, analysis, writing, and presentation. Evaluation criteria may include originality, rigor, clarity, and contribution to the field of cybersecurity. Students may receive feedback and a final grade for their thesis.

10. Compliance with Regulations:

- Throughout the thesis process, students are expected to comply with all relevant regulations, policies, and ethical standards governing academic research and scholarship. This includes adhering to guidelines for data collection, analysis, and reporting, as well as obtaining necessary approvals for human subjects research or other ethical considerations.

11. Documentation and Record-Keeping:

- Records of thesis registration, progress reports, committee meetings, and evaluations are maintained by the academic department or program to ensure accountability and transparency in the thesis process.

By establishing clear requirements, procedures, and responsibilities for thesis registration and supervision, department ensure that students receive the necessary support and guidance to successfully complete their thesis projects and contribute to the advancement of knowledge in cybersecurity.

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)

The scientific supervisor starts to comply with the tasks affiliated to supervising the research thesis after finalizing all the formal procedures to register the research thesis .

2.1 Regulations to Select a Scientific Supervisor:

The program follows the applied procedures for scientific supervision published by the NBU website and are made accessible in CS Postgraduate Programs Handbook, introduced in the presentation of the New Students Orientation. The CS department requires the following conditions to select scientific supervisor for MCyb research thesis:

- Major research area in cybersecurity field.
- Supervised cybersecurity related project/thesis in a regular program.
- Supervisors cannot be assigned to more than five students where these students can be formed into a maximum of three groups.

2.2 Responsibilities of Scientific Supervisors:

The supervision of research thesis in the MCYB program is responsible for:

1. Discuss with the student the ideas for the research thesis and announce the selected ideas among the other students to avoid duplication.
2. Fill out and submit the Supervisor Consent Form.
3. Assist the students to prepare and submit their research project proposals.

The responsibilities of the research projects supervisors (During 2nd year) can be summarized as follows:

1. To meet the students weekly to discuss the thesis.
2. To follow up on the project's completing stages.
3. To advise and guide the students during all thesis phases and milestones.
4. To ensure thesis completion within one year.

2.3 Procedures of the Scientific Supervision and Follow-up:

Based on the Graduate Studies Unified Regulations by the Ministry of Education, the rules and regulations published by the NBU, and the CS regulations for master programs, several evaluations were approved for the research project in the MSCyb program. Throughout the second-year students work closely with their supervisors to undertake the research project as per the following milestones, at the

end of each milestone, students must submit a progress report that will be evaluated by the students' supervisors, evaluators, and program coordinators:

- **Research Foundation**. During this initial phase the student(s) must submit the Progress Report 1 in the third week of the third semester. The report will be reviewed and evaluated by the supervisor and approved by the program coordinator. Students use the same template for the progress reports in the different stages of their research project.

- **Research Initiation**. In this stage, students are expected to have enough knowledge about their research thesis and the thesis environment and have started the thesis implementation. Hence, students have a solid ground and clear direction to continue to the next stage of their research projects. By the end of this stage, students must submit the second progress report which covers the Thesis Foundation and Initiation in Week 8 of third semester. The report will be reviewed and evaluated by the selected evaluator. The coordinator of the MCYB program posts the titles of all the research projects and the faculty members in the program select the projects they can/will evaluate. The evaluators must be supervisors for other research projects. Evaluators are responsible for evaluating a maximum of the same number of projects they supervised.

- **Research Core**. Approaching the end of the semester, students in this stage must construct and evaluate their research projects. As they expected to complete required experiments, build a prototype, framework, or simulations, apply related algorithms, conduct the necessary analysis for the identified research problem. A cumulative progress report is submitted via Blackboard in Week 19 of second year. This report is reviewed and approved by the students' supervisors and the coordinator of the MCYB program.

- **Research Handover**. The complete comprehensive thesis documentation is submitted by the Final Exams week (Week 19 of second year). The final complete report should demonstrate the applied learning, work undertaken, feature direction, and challenges. The report should be written using the Research Thesis Template. The complete report is reviewed and approved by the students' supervisors and the coordinator of the MCYB program. The students' supervisors ensure that all submitted reports are original using plagiarism detection tool.

- **Research Arbitration**. At the end of the semester students will present and discuss their research projects in a final presentation to the examination committee that includes the project supervisor and another faculty member who must be a supervisor for another research thesis. Faculty members volunteer to direct the sessions of the final presentation according to schedule published by the program coordinators and shared via emails. The examination committee and the session director are provided with guidelines to ensure that proper procedures are followed. Also, the program coordinator meets with the research supervisors, evaluators, and the sessions directors to explain all the aspects related to the research projects arbitration. Directors of the final presentation sessions can be faculty members from the program, who are not research thesis supervisors, or invited faculty members from the different departments who voluntarily assist in monitoring and directing final presentations of the research projects. The examination committee uses the Research Thesis Evaluation Form to document their comments and scores for the different parts of the research project. The session director collects the completed forms and submits them to the program coordinator along with a report about the session.

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)

Thesis Committee Selection and Responsibilities:

The responsibility for selecting the thesis committee lies with the Graduate Studies Committee. The committee is responsible for ensuring that the thesis evaluation is thorough and impartial.

- **Selection Process:**
  - The Graduate Studies Committee selects the thesis committee members based on their expertise and relevance to the thesis topic.
  - The committee must include at least one external examiner to provide an unbiased perspective and ensure the quality and integrity of the thesis evaluation process.
- **Committee Composition:**
  - The committee will typically consist of the student's scientific supervisor, other faculty members with relevant expertise, and the external examiner.
  - The external examiner should be a recognized expert in the field and should not be affiliated with the institution.

3.1 Regulations for selection of the examination committee

The complete report of the research thesis is evaluated by the examination committee that includes the thesis supervisor and another faculty member who must be a supervisor for another research thesis. Examination committees are provided with evaluation rubric.

3.2 Requirements to proceed for research thesis examination:

The MCYB research thesis is assessed primarily on the final report written by the students. The research thesis must fulfill the following requirements:

1. Technical artifact:
   The thesis deliverable can be in the form of a prototype, a software, an algorithm, a solution design for a particular problem, a documented architecture, technology evaluation report, adoptability measures of technology or framework, analytical report, framework/policy implementation or improvement.

2. Documentation:
   Students must follow a provided template and provide a minimum of 12000 words thesis document which represents the insight on the knowledge learned in the related thesis form, the related literature, demonstration of work conducted, work validation, feature direction and challenges.

3.3 Procedures for approval of the research thesis

Students upload the final documentation and presentation of their research thesis on Blackboard. Program coordinators approve the submissions after making sure that they fulfill the requirements. Then, the examination committee evaluates the complete reports of the research thesis s.

3.4 Criteria for evaluation of the research thesis

The examination committee evaluate the different aspects of the research thesis according to the following criteria:

- **Cognitive/ intellectual skills:**
  - Displays exceptional mastery of a complex and specialized area of knowledge and skills, with an exceptional critical awareness of current problems and/or new insights at the forefront of the field. Shows outstanding ability to evaluate methodologies critically and, where appropriate, to propose new hypotheses.
  - Deal with a range of complex issues both systematically and creatively, making excellent judgements in the absence of complete data.
- **Technical Skills:**
  - Employs advanced skills to conduct research and, where appropriate, advanced technical or professional activity, accepting accountability for related decision making.
  - Displays an exceptional grasp of techniques applicable to the thesis objectives.
  - Shows originality in application of knowledge, and excellent understanding of how established the used techniques are to create and interpret knowledge.
- **Use of research-informed literature:**
  - Evaluate critically, with exceptional insight, a range of literature relating to current research and advanced scholarship in the discipline.
  - Make consistently excellent use of appropriate academic conventions and academic honesty.
  - Communicate very high-level arguments, evidence and conclusions to specialist and non-specialist audiences.
- **Skills for life and professional employment.**
  - Shows a very high level of employability skills, including team working/leadership, thesis management, IT/computer literacy, creativity, and flexibility.
  - Demonstrates very high-level communication skills in a range of complex contexts, and ability to write at publishable standards.
  - Demonstrates autonomy and notable originality in tackling and solving demanding problems.
  - Shows a high level of consistency and autonomy in planning and implementing tasks at a professional or equivalent level.
  - Demonstrates the skills and attitudes needed to advance own knowledge and understanding, and to develop new skills to a high level.
  - Demonstrates the independent learning ability required for continuing professional development.

- **Report**:
  - In addition to meeting the other requirements, for the writing is essentially error-free; the style and format is appropriate; writing flows smoothly from one idea to another; expressed ideas can be easily followed.

The student must publish at least one research paper indexed by WOS or Scopus as an essential requirement to award the degree.

H. Student Admission and Support:

1. Student Admission Requirements:

1- The applicant must have a bachelor's degree in the field of computer science or related disciplines such as information systems, information technology, software engineering, cyber security, or computer engineering from a university recognized by the Ministry of Education in Saudi Arabia.
2- The applicant must have Good or a GPA of at least 70% (equivalent to 3 out of 5 or higher).
3- The applicant must have obtained at least 50% marks in the aptitude test for university graduates.
4- The applicant must have a score of 4.5 in the ILETS English language test or its equivalent in any other English language test.
5- The applicant must pass the interview conducted by the department.

The weight of selection criteria is summarized as follow:

- The GPA is 50%.
- Aptitude test for university graduates is 20%
- English language test is 20%.
- The interview is 10%.

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 new students will be invited to an academic guidance meeting, in the first week, aimed at shedding some light on the regulations and the registration process at the faculty of science, computer science department.
- An agenda will be introduced to the new students that introduces students' rights and responsibilities. In addition, some information about university life through campus; visits, meetings, lectures, and other activities. This could be done via the cooperation with different academic & support departments in the faculty.

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)

1. The academic services are provided through the academic guidance committee. The student has an academic guide who introduces academic & career advice, and general counseling. The student meets his academic guide at least three times a semester, one at the beginning of his registration and the other one after the first mid-term and the last one towards the end of the semester. The teaching staff are asked to post their guidance hours. Academic advising files include the following documents:
    - Student advising file.
    - Academic advisor profile

- Basic data of the student

2. The head of the department council meets the students and listens to their academic problems and concerns.

3. There are some helpful programs in the deanship of community service and continuing education that help the students in choosing and preparing for their future career.

4. For psychological and social counseling, there is a unit of guidance and counseling in the Deanship of Student Affairs to provide preventive and therapeutic counseling services that meet the needs of the student in all aspects of personal, social, educational, and professional aspects.

4. Special Support:

(Low achievers, disabled, and talented students).

1. The teaching staff members should consider the individual differences between the students who are low achievers and talented ones during their lectures.
2. The low achievers' students can take advantage of the office hours of the teaching staff member which have been defined since the beginning of the semester.
3. The talented students have the chance to finish their studies in a short time compared to their peers.
4. The unit of guidance and counseling in the Deanship of Student Affairs helps students to overcome educational obstacles during their academic career, by preparing specialized programs and services for people with special needs through the Center for Special Needs at the Deanship of Student Affairs, which takes care of students with special needs at NBU
5. Honorary list of Dean for outstanding 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		1		1	1	2
Associate Professor		4	Cybersecurity	2	2	4
Assistant Professor		2	Cybersecurity	1	1	4
Technicians and Laboratory Assistant		4	Cybersecurity	2	2	4
Administrative and Supportive Staff						
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.)

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

- Required Textbook
- Essential Reference Material
- Electronic Resources- Websites, Blackboard

2. Facilities and Equipment:

(Library, laboratories, classrooms, etc.)

1. Learning Resources.

- Different processes are followed by faculty and teaching staff for planning and acquisition of different learning resources such as textbooks, references and any needed resources including electronic and web-based resources. Course instructors specify the needed resource according to the program plan. The specified resources should be approved by the program council. Each semester, the faculty members specify a list of books to be provided by the library as well as the software and tools needed for the department labs. The adequacy of the resources is evaluated by the program council through continuous revision of these resources and by capturing the student feedback on a periodic basis. The following link illustrates the steps of building and developing acquisitions (supplying) the libraries of Northern Border University.
  https://www.nbu.edu.sa/AR/Deanships/Library_Issues/Pages/default.aspx.
- The textbooks and references included in the faculty of science library are updated annually. Finally, the Saudi Digital Library (SDL) contains millions of books and papers which updated continuously. The teaching staff announce and train the students to access the library's website and retrieve the information they need.

2. Facilities and Equipment

The computer science department is enriched with many facilities such as well-equipped laboratories and classrooms. There are 14 labs in both the boys' and girls' sections. These labs are suitable for teaching almost all subjects of computer science program such as:

- Computer Programming
- Computer Networking
- Database Systems
- Digital Logic Systems

The classrooms are spacious, well-ventilated, Wi-Fi enabled, and provided with smart boards and data shows. Many libraries introduce their services such as the faculty of science library, the central library of the university and the Saudi Digital Library (SDL). Finally, the faculty cafeteria is a popular meeting place for students.

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

(According to the nature of the program)

1. There is "Security and Safety Division" in both sections which is staffed 24 hours a day all year round, providing a focal point for the reporting of serious incidents and implementation of emergency procedures.
2. There is a "Camera Surveillance System" that includes monitoring the alarms besides a 24-hour a day uniformed patrol and response service.
3. All buildings are provided with an emergency exit, fire alarms and advanced sensors for volatile gases.
4. All labs are provided with first aid kits, fire extinguishers, suitable glasses made of special materials in for certain experiments, and water sources.
5. The student is directed, with his first entry into the laboratory, to the following.

a. Don't take your food or water to the lab.
b. Don't mess around with the experiment components.
c. Don't conduct the experiment without the teaching staff member guiding.
d. Leave the components as they were before after carrying out the experiment.

G. Program Quality Assurance:

1. Program Quality Assurance System:

Provide a link to the quality assurance manual.

- The program has a quality assurance manual, and has procedure to monitor the quality of the program; these procedures will be described in the next section.

2. Program Quality Monitoring Procedures:

Course monitoring is a continuous process by which a program is kept under review, via Course Reports and Field Experience Reports. Course monitoring is a continuous process by which a program is kept under review, via Course Reports and Field Experience Reports. Combined, these reporting processes make up an overall course monitoring reporting process which underpins the effective operation of the program. The Procedure is illustrated as follows:

- At the end of each semester, each course coordinator will prepare a course report in consultation with the course teaching team. The course report should be reflective of the learning and teaching

during the semester, and of the assessment, approach taken, recommending any amendments to the course definition that should be considered by the program team.

- A program team through the Quality Committee is constantly seeking to gather evidence and feedback, by evaluating that evidence and by making subsequent changes to enhance outcomes, delivery, and operation. Student feedback is particularly important, and the University uses the NCAAA Course Evaluation Survey and Student Experience Survey to inform the Monitoring Quality processes.
- The process is reflective by collecting evidence and looking at course reports, analyzing the issues and evidence and comparing the program performance against the key performance indicators or benchmarks for the subject area. This should lead to program improvements. Hence annual monitoring of programs and courses is the cornerstone of the quality processes, and leads to a review of every program's currency, ensuring the continuing relevance, appropriateness, and success of the award and student experience.
- **The aims of the Monitoring process are:**
  - To evaluate the statistical information on student recruitment, grades, progression, and completion.
  - To reflect on the learning, teaching and assessment strategies deployed and consider any recommendations for change.
  - To review the appropriateness and effectiveness of the learning outcomes in securing the program's aims and objectives.
  - To recommend changes for improving the student learning experience or curriculum content.

To complete the annual monitoring forms at both courses and program level, using the NCAAA templates.

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

1. Courses are reviewed periodically to ensure their continuity of their relevance to the needs of computer sciences students.
2. The department is coordinating with all departments concerned, both within the College of Computer Science and with departments outside the College.
3. The quality committee ensures that the course outcomes of other department courses are compatible with the mission, goals, and objectives of the program.
4. The course specifications of other department courses are collected and verified by the quality committee at the beginning of the semester. The CLOs of other courses are mapped to the PLOs of program in program specification.
5. The teaching & learning activities and assessment of students are done by the course coordinators / HOD of other departments.

The course reports of other department courses are collected and verified by the quality committee at the end of the semester, and these are duly considered in the preparation of the annual program report.

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

(including male and female sections).

1. The syllabus of all courses is available online to all instructors and students.
2. Checking the course outlines for both male and female sections for all university branches to ensure consistency.
3. Identify a coordinator for each course to maintain quality and consistency for all sections across all branches.
4. For all sections open to a given course, it's mandatory to follow the same assessment plan.

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

1. Assessment plan for Program Learning Outcomes (PLOs):
    - The department council has approved a three-year cycle where each domain is assessed in a year (PLOs Assessment plan attached).

Mechanisms for using Results in the Development Processes

- The CLO-PLO based assessment provides summary of PLOs attainments during a semester. This summary is used by Assessment and Evaluation Committee to identify possible following corrective course of actions:
    - Revision in pre-requisite as inadequate pre-requisite knowledge.
    - Revision in course or course material or providing more helping material, modification in text or reference material.
    - Modifications in course assessment methods.
    - Revision of the learning accomplishments of a course.
    - The graduation thesis addresses most of the Program Learning Outcomes and is noted as missing in the presented evaluation. It is a terminal comprehensive activity and provides students with the opportunity to exhibit the acquired skills and knowledge during the program.
- The Quality and Academic Accreditation Unit (QAAU) has implemented the required forms for direct and indirect assessment with the help of the Assessment and Evaluation Committee.
    - The assessment committee is looking into the CLO based assessment method for the student outcomes and determines the reasons for non-achievements. The trigger is initiated with the non-achievement of PLO in a particular course.
    - Later, detailed analysis of course files to assess the achievement of CLO is performed. Then, the Assessment and Evaluation Committee requires the instructor to provide a Continuous Improvement Plan and Strategies.
- Tracking program graduates and taking their feedback and suggestions and use these suggestions for making decision regarding any plan modification.
- Holding regular surveys for current and graduated students to evaluate the program, and to focus on problems that they faced during studying and after graduation.

2. Consulting organizations in the field of this program to understand their requirements and expectations of our graduates.

6. Program Evaluation Matrix:

Evaluation Areas/Aspects	Evaluation Sources/References	Evaluation Methods	Evaluation Time
Effectiveness of teaching & assessment (course evaluation)	Students	Surveys	Five weeks prior to the final exam each semester

Evaluation Areas/Aspects	Evaluation Sources/References	Evaluation Methods	Evaluation Time
Effectiveness of teaching & assessment (program evaluation)	Students	Surveys	Five weeks prior to the final exam each semester
Effectiveness of teaching & assessment (program evaluation)	Students focus group	Meeting/Feedback form	End of academic each year
Effectiveness of supervision & assessment	Students	Surveys	Five weeks prior to the final exam each semester
Learning resources	Faculty/ students	Surveys	After the midterm of each first semester
Professional skills and employability rate	Alumni	Surveys	At the end of the second semester
Program graduates' competency	employers	Surveys	At the end of the second semester
Overall Program Quality	Independent Reviewers	Reviewing Report on Annual Program Report	End of academic each year
Overall Program Quality	Quality and Development Committee	Comprehensive Report on overall. Program Quality	Each five years

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 (__2__) year(s).

No.	KPIs Code	KPIs	Targeted Level	Measurement Methods	Measurement Time
1	KPI-PG-1	Students' Evaluation of Quality of learning experience in the Program	80%	Average of overall rating of final year students for the quality of learning experience in the program.	End of second Year.
2	KPI- PG-2	Students' evaluation of the quality of the courses	80%	Average students' overall rating of the quality of courses in an annual survey.	End of each semester.
3	KPI-PG-3	Students' evaluation of the quality of academic supervision	80%	Average students' overall rating of the quality of scientific supervision in an annual survey.	After completing the program
4	KPI-PG-4	Average time for students' graduation	2 years	Average time (in semesters) spent by students to graduate from the program.	After the batch complete the program
5	KPI-PG-5	Rate of students dropping out of the program	20%	Percentage of students who did not complete the program to the total number of students in the same cohort.	End of each semester.
6	KPI-PG-6	Employers' evaluation of the program graduates' competency	75%	Average of the overall rating of employers for the competency of the program graduates in an annual survey.	After the batch complete the program and get a job.
7	KPI-PG-7	Students' satisfaction with services provided	80%	Average of students' satisfaction rate with the various services provided by the program (food, transportation, sports facilities, academic advising, ...) on a five- point scale in an annual survey.	End of each year.
8	KPI-PG-8	Ratio of students to faculty members	5:1	The ratio of the total number of students to the total number of full-time and full- time equivalent faculty members participating in the program.	Every year

No.	KPIs Code	KPIs	Targeted Level	Measurement Methods	Measurement Time
9	KPI-PG-9	Percentage of publications of faculty members	100%	Percentage of faculty members participating in the program with at least one research publication during the year to total faculty members in the program.	End of each year.
10	KPI-PG-10	Rate of published research per faculty member	1 paper] year	The average number of refereed and/or published research per faculty member participating in the program during the year. (Total number of refereed and/or published research to the total number of faculty members during the year)	End of each year.
11	KPI-PG-11	Citations rate in refereed journals per faculty member	5	The average number of citations in refereed journals from published research (total number of citations in refereed journals from published research for faculty members to the total published research).	End of each year.
12	KPI-PG-12	Percentage of students' publication	100%	Percentage of students who: a. published their research in refereed journals. b. presented papers at conferences. to the total number of students in the program during the year.	End of graduation year.
13	KPI-PG-13	Number of patents, innovative products, and awards of excellence	1 / program	Number of: a. Patents and innovative products b. National and international excellence awards obtained annually by the students and staff of the program.	Every 4 years

*including KPIs required by NCAAA

H. Specification Approval Data:

Council / Committee	**COMPUTER SCIENCE DEPARTMENT COUNCIL**
Reference No.	**NINTH COUNCIL MEETING - 2023-2024 ACADEMIC YEAR/ FIRST TOPIC**
Date	**20-04-2023**