

**Faculty of Computer and
Information Technology (FCIT)**

كلية: الحاسوب وتكنولوجيا المعلومات

Program: Master of Cybersecurity

برنامج: ماجستير الأمن السيبراني

قالب وثيقة مواصفات برنامج ماجستير
Template for Program Specification

**Faculty of Computer and Information
Technology (FCIT)**

Sana'a University

كلية الحاسوب وتكنولوجيا المعلومات

جامعة صنعاء

Prepared by:

- 1. Prof.Abdoulwase M. AL.Azzani**
- 2. Dr.Mohammad Algawda**
- 3. Eng. Bakeel Azman**

وثيقة مواصفات برنامج ماجستير الأمن السيبراني

مقدمة Introduction

مع هذا التطور المتسارع في مجال الحوسبة وتكنولوجيا المعلومات والاتصالات برزت حاجة المجتمع إلى متخصصين في هذا المجال الرقمي المتسارع. وعليه فإن كلية الحاسوب وتكنولوجيا المعلومات – جامعة صنعاء منذ نشأتها الأولى في عام 2007م تمكنت من تحقيق رسالتها من خلال إعداد كوادر مؤهلة لرفد المجتمع محليا وإقليميا بالمتخصصين في مجالات الحاسوب وتكنولوجيا المعلومات. واستشرقا للمستقبل من قبل قيادة الكلية بأهمية الحفاظ على أمن المعلومات فقد استحدثت الكلية قسم/برنامج "تكنولوجيا الشبكات وأمن الحاسوب" عند إنشائها والبدء في استقبال الطلاب الراغبين في هذا التخصص بدءا من العام الجامعي 2007 – 2008م.

ونتيجة لهذا التطور الرقمي المتسارع تداخلت كافة الأنشطة في حياتنا بشكل متزايد مع الفضاء الرقمي. فقد برز الأمن السيبراني كتخصص محوري في حماية الأصول الرقمية ومكافحة الجرائم الإلكترونية المتنامية. ويمثل تخصص الأمن السيبراني خط الدفاع الأول لمواجهة التهديدات والحد من الجرائم السيبرانية المتطورة.

حيث يهدف برنامج ماجستير الأمن السيبراني إلى إعداد كادرا مؤهلا مهنيا وباحثيا وأكاديميا على مستوى عالٍ من الكفاءة المهنية والأخلاقية قادرا على تأمين الأنظمة القائمة على الحاسوب والشبكات والمعلومات، بالإضافة إلى امتلاكه الأدوات والمهارات اللازمة للكشف عن الجرائم الرقمية باحترافية ومهنية. حيث يتمكن خريجو البرنامج من المساهمة بفاعلية في التنمية المستدامة والتحول الرقمي للأمن، ورفع مستوى الوعي المجتمعي لمواجهة المخاطر الأمنية الرقمية المحتملة في مجال الأمن السيبراني، وتلبية احتياجات المجتمع لحماية المعلومات وأصول الحوسبة على المستوى الشخصي والتنظيمي.

معلومات عامة عن البرنامج Program Identification and General Information

1	اسم البرنامج والدرجة العلمية:	برنامج ماجستير الأمن السيبراني درجة ماجستير علوم في الأمن السيبراني
2	الجهة المسؤولة عن منح الدرجة العلمية (الكلية/المركز/المعهد):	جامعة صنعاء – كلية الحاسوب وتكنولوجيا المعلومات
3	الجهة المسؤولة عن تنفيذ البرنامج (القسم العلمي):	قسم الأمن السيبراني – كلية الحاسوب وتكنولوجيا المعلومات
4	الأقسام العلمية المشاركة في تنفيذ البرنامج:	قسم الأمن السيبراني والتحقيق الجنائي
5	لغة الدراسة في البرنامج:	إنجليزي / عربي
6	عام البدء بالدراسة (للبرامج الجديدة):	2026- 2025
7	أسلوب الدراسة في البرنامج (انتظام/ عن بعد..الخ):	انتظام
8	نوع برنامج الماجستير (مقررات دراسية ورسالة/ مقررات دراسية ومشاريع/ رسالة):	مقررات دراسية ورسالة
9	مكان تنفيذ البرنامج (في الجامعة أم خارجها):	كلية الحاسوب وتكنولوجيا المعلومات
10	نظام الدراسة في البرنامج (نظام ساعات معتمدة، فصلي، سنوي...):	فصلي
11	الزمن الكلي للبرنامج (إجمالي السنوات والساعات المعتمدة لمنح المؤهل):	عامين – 36 ساعة معتمدة
12	المهنة/ المهن التي يعد البرنامج الخريج للالتحاق بها:	1. مدير الأمن السيبراني: Cybersecurity Manager

2. مدير أمن المعلومات: Chief Information Security Officer (CISO).		
3. مستشار الأمن السيبراني: Cyber security consultant.		
4. مدير أمن الشبكات: Network Security Manager.		
5. خبير في الأدلة الجنائية الرقمية: Digital Forensics Expert.		
6. الهاكر الأخلاقي/مختبر الاختراق: Ethical Hacker/Penetration Tester.		
7. خبير في عمليات الدفاع السيبراني: Expert of Cyber Defense Operations.		
8. مهندس الأمن السيبراني: Cybersecurity Architect.		
9. مطور البرمجيات الآمنة: Secure Software Developer.		
10. مدير الحوكمة والمخاطر والامتثال: Manager of Governance, Risk and Compliance.		
11. محلل أنظمة أمن المعلومات: Information Security Systems Analyst.		
12. باحث أكاديمي/علمي في مجال الأمن السيبراني: Academic/Scientific Cybersecurity Researcher.		
(مثلاً: الطالب الملتحق المتعثر - الذي لا يستطيع إكمال البرنامج يمكن أن يوفر له البرنامج نقاط خروج مبكرة بمستوى تأهيل دبلوم متوسط) بكالوريوس حاسوب	13	مستوى / مستويات التأهيل المستهدفة في البرنامج (نوع الشهادة التي تمنح للطلاب في حال التعثر):
	14	المؤهل المطلوب للالتحاق بالبرنامج:
	15	المعدل/ التقدير المطلوب للالتحاق بالبرنامج:
	16	شروط أخرى:
	17	اسم منسق البرنامج:
	18	تاريخ آخر اعتماد لمواصفات البرنامج:

رؤية الجامعة ورسالتها وأهدافها University Vision, Mission and Aims	
رؤية الجامعة University Vision Sana'a University aspires to achieve a national leading role in teaching, learning, scientific research and community service; and to be among the best regional universities and the foremost house of expertise and think tank in Yemen.	
رسالة الجامعة University Mission To contribute to the sustainable development efforts by providing an accredited higher education environment and excellent research services within a fruitful national partnership based on transparency, professionalism and creativity.	
أهداف الجامعة Aims of the University 1. To provide specialized and in-depth academic opportunities for students in different fields of knowledge to meet the country's needs of specialists, technicians, and experts. 2. To cherish the Arabic language, its teaching and development, and mainstream its use as the language of science and education in various arenas of knowledge as a vehicle for the cultural meanings, values, and ethics of the Arab-Islamic civilization. 3. To develop knowledge through engaging in multidisciplinary research, both individually and collectively, and directing them towards serving community needs and development plans. 4. To nurture the development of technology and its utilization in community development. 5. To promote the activities of authorship, translation, and publishing in various fields of knowledge, with special emphasis on the Yemeni heritage.	

6. To contribute to the promotion of arts, literature, and the advancement of sciences.
7. To offer technical and specialized studies and consultations for various public and mixed-sector institutions.
8. To strengthen relations with universities and public and private institutions in the country to ensure a mutual and constructive interaction of knowledge, expertise, resources, and participation that will guarantee an effective contribution to the comprehensive development of the country.

رؤية الكلية ورسالتة وأهدافه Faculty Vision, Mission and Aims

رؤية الكلية Faculty Vision

الريادة وطنياً والتميز إقليمياً في التعليم والبحث والابتكار والأثر المجتمعي في مجالات الحوسبة والتكنولوجيا.

To achieve a leading position locally and excellence regionally in education, research, innovation, and community impact in the fields of computing and technology.

رسالة الكلية Faculty Mission

تقديم تعليم نوعي في مجالات الحوسبة والتكنولوجيا لإعداد كوادر مؤهلة ملتزمة بأخلاقيات المهنة، وإنتاج بحوث مبتكرة، ضمن بيئة مُحفزة وشراكات مجتمعية فاعلة، تلبي متطلبات سوق العمل وتسهم في تحقيق التنمية المستدامة والتحول الرقمي.

Providing distinguished education in the fields of computing and technology to prepare qualified graduates committed to professional ethics and produce innovative research, within a stimulating learning environment and effective community partnerships, addressing labor-market needs and contributing to the achievement of sustainable development and digital transformation.

أهداف الكلية Aims of the Faculty

1. تقديم تعليم نوعي في مجالات الحوسبة والتكنولوجيا لرفد المجتمع بكوادر مؤهلة ملتزمة بأخلاقيات المهنة قادرة على المنافسة والإبداع في سوق العمل تسهم في تحقيق التنمية المستدامة والتحول الرقمي.
 2. تصميم وتطوير برامج أكاديمية وبحثية نوعية، متوافقة مع معايير الجودة والاعتماد، وتواكب التحديات والتطورات واحتياجات سوق العمل.
 3. توفير وتطوير بيئة أكاديمية مُحفزة تُنمّي التعلّم النشط، والتعليم، والبحث، والابتكار، والإبداع، وريادة الأعمال.
 4. إنتاج بحوث مبتكرة وحلول تقنية في الحوسبة والتكنولوجيا تسهم في تحقيق التنمية المستدامة.
 5. تطوير واستقطاب الكفاءات المتميزة بما يعزّز التعليم والبحث العلمي وخدمة المجتمع.
 6. بناء وإدامة شراكة أكاديمية ومجتمعية فاعلة تعزز التعليم والتعلم والبحث العلمي.
 7. تقديم الاستشارات التقنية والتدريب المتخصص، ونشر الثقافة الرقمية لتمكين القطاعات المختلفة ودعم التحول الرقمي.
1. Providing distinguished education in the fields of computing and technology to graduate qualified professionals committed to professional ethics, capable of competing and innovating in the labor market, and contributing to sustainable development and digital transformation.
 2. Designing and developing distinguished academic and research programs, aligned with quality and accreditation standards, and responsive to evolving challenges and labor-market needs.

3. Offering and improving a stimulating academic environment that fosters active learning, teaching, research, innovation, creativity, and entrepreneurship.
4. Producing innovative research and technological solutions in computing and technology that contribute to sustainable development.
5. Developing and attracting distinguished cadres to enhance education, scientific research, and community service.
6. Building and sustaining effective academic and community partnerships that enhance education, learning, and scientific research.
7. Providing technical consultations, specialized training, and spreading digital culture to empower various sectors and support digital transformation.

رؤية ورسالة القسم العلمي وأهدافه Department Mission and Aims

رؤية القسم Department Vision

الريادة محليا والتميز إقليميا في التعليم والبحث العلمي والابتكار وخدمة المجتمع في مجالات الأمن السيبراني.

To achieve a leading position locally and excellence regionally in education, scientific research, innovation, and community service in the field of Cybersecurity.

رسالة القسم Department Mission

تقديم تعليم نوعي لإعداد كوادر مؤهلة ملتزمة بأخلاقيات المهنة، وإنتاج بحوث مبتكرة في مجال الأمن السيبراني من خلال بيئة محفزة وشراكة مجتمعية فاعلة بما يلبي متطلبات سوق العمل ويسهم في تحقيق التنمية المستدامة والتحول الرقمي الآمن.

Providing high-quality education to prepare qualified professionals committed to professional ethics, and producing innovative research in the field of cybersecurity—through a stimulating environment and effective community partnerships—to meet labor-market needs and contribute to achieving sustainable development and secure digital transformation.

أهداف القسم Department Aims

يهدف القسم الى:

1. تقديم تعليم نوعي في مجال الأمن السيبراني لرفد المجتمع بكوادر مؤهلة ملتزمة بأخلاقيات المهنة، قادرة على المنافسة والإبداع في سوق العمل، وتسهم في تحقيق التنمية المستدامة والتحول الرقمي الآمن.
2. تقديم وتطوير برامج أكاديمية وبحثية نوعية في مجال الأمن السيبراني تواكب التحديات والتطورات المستمرة ومتطلبات سوق العمل المتزايدة لحماية الفضاء الرقمي ومكافحة الجرائم الإلكترونية.
3. الاسهام في توفير بيئة تعليمية وأكاديمية محفزة لتعزيز التعليم والتعلم والإبداع والابتكار في مواجهة التحديات المتزايدة في الأمن السيبراني.

4. إنتاج بحوث علمية مبتكرة في مجالات الأمن السيبراني تسهم في تحقيق التنمية المستدامة والتحول الرقمي الآمن.
5. تطوير واستقطاب الكوادر المتميزة في مجالات الأمن السيبراني لتسهم في تعزيز التعليم والبحث العلمي وخدمة المجتمع.
6. بناء شراكة فاعلة مع المؤسسات الأكاديمية والبحثية والصناعية تعزز التعليم والتعلم والبحث العلمي في مجالات الأمن السيبراني.
7. تقديم خدمات استشارية وتدريبية ونشر المعرفة المتخصصة والوعي في مجالات الأمن السيبراني.

1. Providing high-quality education in cybersecurity to supply society with qualified professionals committed to professional ethics, capable of competing innovatively in the labor market, and contributing to sustainable development and secure digital transformation.
2. Providing and developing high-quality academic and research programs in cybersecurity that keep pace with ongoing challenges and developments and with growing labor-market demands, in order to protect cyberspace and combat cybercrime.
3. Providing a stimulating educational and academic environment that strengthens teaching and learning, fosters creativity and innovation, and helps confront the escalating challenges in cybersecurity.
4. Producing innovative scientific research in cybersecurity that contributes to sustainable development and secure digital transformation.
5. Developing and attracting distinguished cybersecurity talents, thereby enhancing education, scientific research, and community service.
6. Building effective partnerships with academic, research, and industry institutions that bolster education, learning, and scientific research in cybersecurity.
7. Providing consultation and training services, disseminating specialized knowledge, and raising awareness in the field of cybersecurity.

رسالة البرنامج وأهدافه Program Mission and Aims

■ رسالة البرنامج Program Mission

إعداد كادر مؤهل ومتميز مهنياً وبحثياً ملتزماً بأخلاقيات المهنة ومزوداً بأحدث المعارف والمهارات التخصصية والشخصية قادراً على إنتاج بحوث علمية وتقديم حلول أمنية متقدمة في مجال الأمن السيبراني تلبي احتياجات سوق العمل محلياً وإقليمياً من خلال بيئة محفزة وخدمة مجتمعية فاعلة.

Preparing a well-qualified cadre distinguished professionally and in research committed to professional ethics and equipped with the latest specialized

knowledge and personal skills; capable of producing scientific research and delivering advanced cybersecurity solutions that meet labor-market needs locally and regionally, through a stimulating environment and active community engagement.

■ أهداف البرنامج Program Aims

يهدف برنامج ماجستير الأمن السيبراني إلى:

1. إعداد كادر مؤهل ومتميز مهنياً وبحثياً ملتزم بأخلاقيات المهنة قادراً على المنافسة والإبداع ويسهم في تقديم حلول متقدمة في مجال الأمن السيبراني تلبي احتياجات سوق العمل الوطني والإقليمي.
 2. تزويد الطلبة بأحدث المعارف والمهارات التخصصية والشخصية في مجالات الأمن السيبراني.
 3. إنتاج بحوث علمية تسهم في تحقيق التنمية المستدامة والتحول الرقمي للأمن.
 4. المساهمة في خدمة المجتمع ونشر الوعي في مجال الأمن السيبراني.
1. Preparing a qualified workforce, distinguished professionally and in research, committed to professional ethics, and capable of competing and innovating, and contributing to the delivery of advanced cybersecurity solutions that meet national and regional labor-market needs.
 2. Equipping students with the latest specialized and personal competencies in the field of cybersecurity.
 3. Producing scientific research that contributes to achieving sustainable development and secure digital transformation.
 4. Contributing to community service and raising awareness in the field of cybersecurity.

مرجعيات البرنامج Program Benchmarks

إلى ماذا استند القسم العلمي في تطوير البرنامج مثلاً:
اللوائح والأنظمة الصادرة عن وزارة التعليم العالي.
معايير التخصص الوطنية (نارس).
المعايير المرجعية لهيئات الاعتماد الإقليمية والعالمية.
البرامج المماثلة في الجامعات الأخرى (مسمى الدرجة/ عدد الساعات المعتمدة/ عدد الساعات طبيعة البرنامج/ عدد وأسماء المقررات) ... الخ

أسماء البرامج المرجعية المماثلة:

1. King Fahd University of Petroleum & Minerals (KFUPM), College of Computing and Mathematics, Information & Computer Science Department, Master of Cybersecurity;
https://bulletin.kfupm.edu.sa/main/program?program_id=145&title=master-of-science-in-security-and-information-assurance
2. University of London, MSc Cyber Security;
<https://www.london.ac.uk/study/courses/postgraduate/msc-cyber-security>.
3. Princess Sumaya University for Technology, Master's Degree in Cyber Security;
<https://www.psut.edu.jo/en/program/master-of-science-program-in-Cyber-security>
4. SANS Technology Institute, Cybersecurity Master's Degree; <https://www.sans.edu/cyber-security-programs/masters-degree/?msc=main-nav>.
5. University of Twente, ; Master's in Computer Science with a specialization in Cyber Security; <https://www.utwente.nl/en/education/master/programmes/computer-science/specialisation/cyber-security/courses-research/>.

6. Universiti Teknologi Malaysia (UTM), Master of Cyber Security - Course Offered;
<https://comp.utm.my/master-csy/>.

ملحق (1) المعايير الأكاديمية للمحتوى لهيئة الاعتماد.
ملحق (2) مسح أسماء البرامج المماثلة للبرنامج الحالي.
ملحق (3) مسح مخرجات التعلم في البرامج المماثلة للبرنامج الحالي.
ملحق (4) مسح الساعات المعتمدة للبرامج المماثلة للبرنامج الحالي.
ملحق (5) مسح المقررات الدراسية في البرامج المماثلة للبرنامج الحالي.

ملخص مسح البرامج المرجعية المماثلة للبرنامج الحالي

البرنامج الحالي	البرامج المرجعية المماثلة						البيانات المطلوبة
	البرنامج السادس	البرنامج الخامس	البرنامج الرابع	البرنامج الثالث	البرنامج الثاني	البرنامج الأول	
Master of Cybersecurity	Cyber Security (Course Offered)	Master of Cyber Security	Master's Degree in Cybersecurity	Master of Cyber Security	Master of Science in Cyber Security	M.S. in Security & Information Assurance	اسم البرنامج:
Faculty of Computer and Information Technology (FCIT)	Faculty of Computing	Electrical Engineering Mathematics and Computer Science (EEMCS)	SANS Technology Institute	King Hussein School of Computing Sciences	Group	College of Computing and Mathematics	اسم الكلية/المركز/المعهد:
Sana'a University	Universiti Teknologi Malaysia (UTM)	University of Twente	SANS Technology Institute	Princess Sumaya University for Technology	University of London	King Fahd University of Petroleum & Minerals	اسم الجامعة:
Yemen	Malaysia	Dutch	USA	Jordan	UK	King of Saudi Arabia	اسم الدولة:
Courses & Thesis	Courses & Thesis	Courses & Thesis	Courses	Courses & Thesis	Courses & Thesis	Courses & Thesis	طبيعة الدراسة في البرنامج (مقررات/ أطروحة/ مقررات فقط/ أطروحة فقط)
On-campus	On-campus	On-campus	On-campus	On-campus	Distance-learning	On-campus	سلوب الدراسة في البرنامج (انتظام/ عن بعد)
2 years	1.5 years	2 Years	3-5 Years	2 Years	2-5 years	2 Years	عدد الفصول الدراسية (إن وجدت)
30 CHs	33 CHs	90 Units ⁴	28 CHs	25 CHs	150 Units ³	24 CHs + 1 CH ¹	إجمالي عدد الساعات المعتمدة لمقررات البرنامج
18	24	55 Units ⁴	19	18	150 Units ³	9 + 1	عدد الساعات المعتمدة للمقررات الإلزامية
12	9	35 Units ⁴	9	7	0 Units ³	15 (9 + 6) ²	عدد الساعات المعتمدة للمقررات الاختيارية
6	8	10	11	6	10	3 + 1 ¹	عدد المقررات الإلزامية

البرنامج الحالي	البرامج المرجعية المماثلة						البيانات المطلوبة
	البرنامج السادس	البرنامج الخامس	البرنامج الرابع	البرنامج الثالث	البرنامج الثاني	البرنامج الاول	
4	3	7 or Least	3	3	0	5 (3 of SEC & 2 of ICS) ²	عدد المقررات الاختيارية
It is based on the applicant's transcript for study in the program	2 ⁵	---	---	---	---	---	وجود مقررات إضافية تكميلية للالتحاق بالبرنامج وعددها
6 CHs	12 CHs	30 Units ⁴	0 CHs (Courses)	9 CHs	30 Units ³	6 CHs	عدد الساعات المعتمدة للأطروحة
36 CHs	45 CHs	180 ² Units ⁴	36 CHs	34 CHs	180 ¹ Units ³	30 CHs	عدد الساعات المعتمدة (مقررات + أطروحة)
2 Years	1.5 Years	2 Years	3 -5 Years	2 Years	2 – 5 Years	2 Years	المدة المحددة لإنجاز الأطروحة
2 Years	1.5 Years	2 Years	2 Years	2 Years	2 Years	2 Years	الحد الأدنى لإنهاء البرنامج
3 Years	2-... Years	3-... Years	3.5 Years	3-... Years	5 Years	3-... Years	الحد الأعلى لإنهاء البرنامج

¹ The program degree plan in the program website: there is a course " Graduate Seminar – 0 CH" not computed in the total of the program credit hours.

² An Elective Courses are five Courses (15 CHs). The elective courses distributed into: Tree elective courses (9 CHs) are elective from SEC Elective Courses, and tow elective courses (6 CHs) are to be taken according to the approved degree plan.

³ In UK, Ten Core Modules: Each core module is worth 15 UK credits. This means each module is designed to require approximately 150 hours of student work (15 credits * 10 hours/credit). In the UK, the Credit Accumulation and Transfer Scheme (CATS) is a system where one credit represents approximately 10 hours of "notional learning time". This includes lectures, seminars, practical work, and independent study.

⁴ Master 120 EC: In the Netherlands, each credit represents 28 hours of work. including: • Attending lectures and tutorials, Reading course materials, Preparing for tests and exams, Writing papers and assignments, Participating in group work, • Self-study.

⁵ For Non CS Background.

مخرجات التعلم المقصودة للبرنامج (ILOs) Intended Learning Outcomes	
أولاً: مجال المعرفة والفهم (A) Knowledge and Understanding	
بعد الانتهاء من البرنامج بنجاح سوف يكون المتخرج قادراً على ان:	
Demonstrate deep understanding of advanced security concepts, theories, facts, practices, research methodology, tools and techniques related to cybersecurity field.	- A1

ثانياً: مجال المهارات الذهنية (B) Intellectual Skills	
بعد الانتهاء من البرنامج بنجاح سوف يكون المتخرج قادراً على ان:	
Analyze the computing effects on society, and evaluate and troubleshoot complex security vulnerabilities, malware, threats, risks and digital crimes to elaborate security solutions.	- B1

Develop and choose suitable tools, techniques and technology resources to design and implement a complex computing system and creative security solutions to defend individual and organization's computing assets

- B2

ثالثاً: مجال المهارات العملية والمهنية (C) Professional and Practical Skills

بعد الانتهاء من البرنامج بنجاح سوف يكون المتخرج قادراً على ان:

Apply advanced cybersecurity concepts, theories, facts, tools, techniques and the best practices to detect, prevent, response and recover from cyber-incidents efficiently.

-C1

Conduct advanced research using cybersecurity research and inquiry methodologies.

-C2

Manage, troubleshoot complex and advance security vulnerabilities and investigate in the digital crimes in cybersecurity practices

-C3

رابعاً: مجال المهارات العامة (D) General Skills

بعد الانتهاء من البرنامج بنجاح سوف يكون المتخرج قادراً على ان:

Communicate effectively and perform tasks proficiently in various roles to disseminate and achieve project and research outcomes.

-D1

Demonstrate a strong commitment to academic and professional responsibilities and ethical conduct, and regulatory compliance with the best practices, while actively engaging in continuous professional development.

-D2

ملحق (6) موازنة اهداف البرنامج مع مخرجات التعلم.

ملحق (7) موازنة مخرجات التعلم المقصودة للبرنامج مع المعايير الوطنية.

ملحق (8) موازنة مخرجات التعلم للبرنامج مع المعايير المرجعية للمحتوى العلمي.

هيكل البرنامج:

- الحد الأدنى لعدد الساعات المعتمدة أو الوحدات الدراسية لنيل درجة الماجستير في تخصص معين (30) ساعة معتمدة / وحدة دراسية، ويخصص إضافة لذلك (6) ساعات معتمدة للرسالة العلمية.
- يتكون هيكل البرنامج من المتطلبات التالية:

الوزن النسبي %	الساعات المعتمدة	عدد المقررات	المتطلبات
0%	يعتمد على سجل درجات المتقدم للدراسة في البرنامج	يعتمد على سجل درجات المتقدم للدراسة في البرنامج	مقررات استدرائية
50%	18	6	مقررات إجبارية
33.33%	12	4	مقررات اختيارية
16.67%	6	1	الرسالة
100%			الإجمالي

وفيما يلي تفصيل بمتطلبات هيكل البرنامج:

أولاً: المقررات الاستدرائية للبرنامج:

Admissions to the program according to admission laws, regulations and rules issued by the Ministry of Higher Education and Scientific Research, University admission laws and regulations, and any decisions making by specialist councils in the faculty and university.

Additionally, applicant to the program must successfully complete a maximum of 30 credit hours of pre-requisite courses if not study it previously. The department council identify the required pre-requisite courses by the applicant from the following courses:

المتطلبات القبليّة Pre- Requisites	الساعات المعتمدة Credit Hours				اسم المقرر (Course Title)		
	الإجمالي Total C.H	تمارين / Tut.	عملية Pr.	نظرية Th.	عربي (Arabic)	English	
	6	4	---	4	رياضيات الحوسبة	Mathematics in Computing	1
	3	2	---	2	رياضيات متقطعة	Discrete Mathematics.	2
	3	2	---	2	جبر خطي	Linear Algebra.	3
	3	2	---	2	إحصاء واحتمالات	Probability and Statistics.	4
	6	---	4	4	لغة برمجة	Programming Languages	5
	3	---	2	2	هياكل بيانات وخوارزميات	Data Structures and Algorithms.	6
	3	---	2	2	نظم تشغيل	Operating Systems.	7
	3	---	2	2	شبكات الحاسوب	Computer Networks.	8
	3	---	2	2	معمارية حاسوب	Computer Organization and Architecture	9
	33	10	12	22	إجمالي الساعات المعتمدة		

ثانياً: المقررات الإلزامية:

المتطلبات القبليّة Pre- Requisites	إجمالي الساعات المعتمدة للمقرر	عدد الأيام الدراسية للمقرر	توزيع الساعات المعتمدة (CHs Distribution)			الساعات المعتمدة (CHS)	رمز المقرر Code/ NO.	اسم المقرر Course Title	
			تمارين/ سمنار Tut.	عملية Pr.	نظرية Th.				
					3	3		Research Methodology	1
			2		3	3		Advanced Information Security	2
			2		3	3		Network and Infrastructure Security	3
			2		3	3		Secure Software Development	4
			2		3	3		Cryptography and Data Security	5
			2		3	3		Hacker Tools, Techniques & Exploits	6
					18	18	إجمالي الساعات المعتمدة		

ثالثاً: المقررات الاختيارية

المتطلبات القبليّة Pre-Requisites	إجمالي الساعات المعتمدة للمقرر	عدد الأيام الدراسية للمقرر	الساعات المعتمدة Credit Hours				رمز المقرر Code/ NO.	اسم المقرر Course Title	
			الإجمالي Total C.H	تمارين/ سمنار Tut.	عملية Pr.	نظرية Th.			
			3					Elective I	1
			3					Elective II	2
			3					Elective III	3
			3					Elective III	4
		-	12				إجمالي الساعات المعتمدة		

رابعاً: رسالة الماجستير

تعد رسالة الماجستير جزءاً من متطلبات نيل درجة الماجستير في برنامج ماجستير الأمن السيبراني بواقع 6 ساعات معتمدة. ويسمح للطلاب تسجيل رسالة الماجستير بعد أن يجتاز المقررات الدراسية للبرنامج بنجاح (بمعدل عام 75% على الأقل). حيث يقوم الطالب بتقديم طلب التسجيل على الرسالة وعنوان موضوع الرسالة المقترح إلى رئيس القسم وفقاً للقوالب المقررة من الدراسات العليا في الكلية. يتولى رئيس القسم عرض طلبات الطلاب لتسجيل رسائل الماجستير لهم على مجلس القسم لمناقشة طلباتهم وإقرار توزيع الطلاب على أعضاء هيئة التدريس الذين سيتولون الإشراف على رسائلهم.

خارطة المنهج (تسكين/ موازنة مخرجات التعلم مع مقررات البرنامج):

Intended Learning Outcomes Mapping (Curriculum Map)

تكتب مخرجات تعلم البرنامج الفرعية، وترفق مع وثيقة مواصفات البرنامج. ويتم بعد ذلك اعتمادها كأساس لكتابة خارطة المنهج. ويتم رسم خارطة المنهج من خلال جدول يضم المقررات الدراسية لمنهج البرنامج، وتوضيح علاقة أو إسهام كل منها، في تحقيق مخرجات تعلم البرنامج الأكاديمي.

ملحق () مصفوفة تسكين مخرجات التعلم للبرنامج في مقررات دراسية (خارطة المنهج).

مصفوفة خارطة المنهج للبرنامج - Intended Learning Outcomes Mapping (Curriculum Map)

م	المقررات Courses	مخرجات البرنامج Program ILOs							
		D2	D1	C3	C2	C1	B2	B1	A1
1	Advanced Information Security					✓		✓	✓
2	Network and Infrastructure Security					✓	✓		✓
3	Hacker Tools, Techniques & Exploits	✓	✓	✓				✓	✓
4	Research Methodology		✓		✓				✓
5	Secure Software Development		✓			✓	✓		✓
6	Cryptography and Data Security					✓	✓	✓	✓
7	Thesis		✓	✓	✓	✓	✓	✓	✓

Teaching Strategies for Current Program:

Teaching Strategies		استراتيجيات التدريس (التعليم والتعلم):
No	Teaching Strategy	Describe How to Use it
1	Lectures/Interactive Lectures,	These are interactive lectures weekly conducted in the class and supported with variety of teaching formats including, lectures and multimedia presentations, use of whiteboard and solved examples, and class discussions, in which concepts, approaches, and case studies are presented, explored, and shown students what they need to know.
2	Practical Lab Sessions (Hands-On Labs and Cyber Ranges)	Practical Applications using a variety of software's before the real design and implementation. A variety of web-based searches students will be assigned to learn how they can search for solutions using the Web. This is arguably the most crucial strategy. Cybersecurity is a practical discipline, and students need to go beyond theory to develop muscle memory for defending and attacking systems. Cyber Ranges: Use virtual environments that simulate real-world IT infrastructure. This allows students to perform offensive (e.g., penetration testing, ethical hacking) and defensive (e.g., incident response, network defense) exercises in a safe, controlled space. Simulations: Implement simulations for specific attacks, like phishing, ransomware, or Denial-of-Service (DoS) attacks. This helps students learn to identify and respond to threats in a timely manner.

Teaching Strategies		استراتيجيات التدريس (التعليم والتعلم):
No	Teaching Strategy	Describe How to Use it
		This strategy focuses on providing students with practical experience in a simulated environment. Cybersecurity Labs and Simulations: This is paramount. Students should be able to configure firewalls, analyze network traffic, conduct vulnerability assessments, perform penetration testing, and respond to simulated cyberattacks in a controlled environment. Virtual labs are particularly useful for providing scalable and accessible hands-on experiences.
3	Homework Assignments	Students are given special tasks, exercises, puzzles, and activities during the class or at homes.
4	Group Discussions	Discussions are carried out about some aspects. related to the subject. It involves a large or small group activity that encourages students to focus on a topic and contribute to the free flow of ideas. The teacher may begin a brainstorming session by posing a question or a problem, or by introducing a topic. Students then express possible answers, relevant words and ideas.
5	Case Studies and Real-World Scenarios	Connect theoretical knowledge to current events. Analyzing past cyberattacks and breaches provides valuable insights into vulnerabilities, attacker methodologies, and effective incident response strategies. This approach connects theoretical knowledge to actual events, allowing students to learn from past incidents.
6	Problem-Based Learning	Present students with complex, open-ended cybersecurity problems (e.g., a data breach scenario, a new malware threat) and have them collaboratively research, analyze, and devise solutions. This encourages self-directed learning and the development of practical problem-solving skills. Capture the Flag (CTF) games are cybersecurity competitions that challenge participants to find "flags"—hidden pieces of text or files—by exploiting vulnerabilities in a system. They are a popular and effective way to practice and develop cybersecurity skills. Examples of CTF Games and Platforms include: GoogleCTF , DEF CON CTF, PicoCTF, TryHackMe & Hack The Box.
7	Project-Based	A master's thesis or capstone project can be an excellent way for students to apply their cumulative knowledge to a real-world security problem, such as developing a secure application or creating a comprehensive security policy for a fictional company.
8	Collaborative and Interdisciplinary Work	Cybersecurity is a team effort. Effective teaching strategies should encourage collaboration and communication skills. Examples: Group Projects: Assign group projects that require students to work together to design and implement security solutions, mirroring a Security Operations Center (SOC) team, and Interdisciplinary Courses: Incorporate topics like law, ethics, and policy into the curriculum, as cybersecurity professionals must understand the legal and ethical implications of their actions. This approach emphasizes teamwork and the integration of diverse fields into the cybersecurity curriculum.
9	Flipped Classroom and Active Learning	This pedagogical model moves traditional lecture content outside of the classroom and uses in-class time for interactive, hands-on activities. • Pre-Class Readings/Videos: Students can watch lectures or read materials on a topic before class. • In-Class Activities: Class time is then dedicated to lab exercises, group discussions, and problem-solving, with the instructor acting as a

Teaching Strategies		استراتيجيات التدريس (التعليم والتعلم):
No	Teaching Strategy	Describe How to Use it
		facilitator. This approach has been shown to improve student learning outcomes and engagement. This model uses class time for interactive, hands-on activities rather than traditional lectures.
10	Presentations. Report Assignments.	

Assessment Strategies for Current Program:

Assessment Strategies		استراتيجيات التقييم
No	Assessment Strategy	Describe how to use it
1	Quizzes, Written Exam (Midterm and Final Exams)	Quizzes assess student ability to follow the lecturer during the study course. Mid. term & Final exams for each course is required for all courses except Graduation Projects. These exams will evaluate the extent in which the student understanding of theoretical and applied subjects.
2	Home Assignments, (Weekly Assignments OR Bi-Weekly Assignments)	Home works and assignments will evaluate students according to their ability to explain and illustrate the assignments they are given.
3	Reviews of Research Papers	
4	Individual/Group Reports	
5	Individual/Group Presentations	
6	Lab Reports	
7	Case Studies	
8	Discussion Boards	
9	Cyber Defense Exercises	

نظام وأسلوب الدراسة في البرنامج:	
نظام الدراسة: انتظام	
أسلوب الدراسة: مقررات + رسالة	
مدة البرنامج: عامان	
عدد الساعات لإكمال البرنامج: 36 ساعة معتمدة	

الخطة الدراسية للبرنامج Study Plan:

First Semester					العام الجامعي الأول: الفصل الدراسي الأول		
المتطلبات القبلية Pre- Requested	الساعات المعتمدة Credit Hours				رمز المقرر Code / No	اسم المقرر Course Title	
	Total C.H.	تمارين / سمنار Tut.	عملي Pr.	نظري Th.			
	3			3		Advanced Information Security	1 أمن معلومات متقدم

العام الجامعي الأول: الفصل الدراسي الأول					
المتطلبات القبلية Pre- Requested	الساعات المعتمدة Credit Hours				اسم المقرر Course Title
	Total C.H.	تمارين / سمنار Tut.	عملي Pr.	نظري Th.	
	3			3	Network and Infrastructure Security
	3			3	Research Methodology
	3			3	Elective I
	3			3	Elective II
	15			15	اجمالي الساعات المعتمدة Total Credit Hours
العام الجامعي الأول: الفصل الدراسي الثاني					
المتطلبات القبلية Pre- Requested	الساعات المعتمدة Credit Hours				اسم المقرر (Course Title)
	Total C.H.	تمارين / سمنار Tut.	عملي Pr.	نظري Th.	
	3			3	Secure Software Development
	3			3	Cryptography and Data Security
	3			3	Hacker Tools, Techniques & Exploits
	3			3	Elective III
	3			3	Elective IV
	15			15	اجمالي الساعات المعتمدة Total Credit Hours

العام الجامعي الثاني:		
المتطلبات القبلية Pre- Requested	اسم المقرر (Course Title)	رمز المقرر (Code/No)
6	رسالة الماجستير	—

Elective Courses (12 Credit Hours):

Choose four Courses from only one of the following Competence Areas:

Elective Course of the Master of Cybersecurity Program								
No.	Course Code	Course Name	اسم المقرر	CHs	L	T	P	Prerequisites, Co-requisites
A. Penetration Testing								
1		Penetration Testing & Ethical Hacking		3	3	-	-	Inf. Sec., Network and Infrastructure Security
2		Scripting & Automation for Red Team Operations		3	3	-	-	Penetration Testing & Ethical Hacking
3		Web Application Penetration Testing		3	3	-	-	Penetration Testing & Ethical Hacking
4		Cloud Penetration Testing		3	3	-	-	1 & 2

Elective Course of the Master of Cybersecurity Program

No.	Course Code	Course Name	اسم المقرر	CHs	L	T	P	Prerequisites, Co-requisites
5		Advanced Penetration Testing & Exploit Development		3	3	-	-	1 & 2
6		Enterprise Penetration Testing		3	3	-	-	
7		Red Team Operations and Adversary Emulation		3	3	-	-	3-5
B. Cyber Defense Operations								
1		Defensible Security Architecture & Engineering		3	3	-	-	Adv. Info. Security, Network and Infrastructure Security
2		Security Operations Center (SOC) Operations		3	3	-	-	1
3		Cyber Threat Intelligence (CTI) Operations ≈ Threat Intelligence & Analysis)		3	3	-	-	1 & 2
4		Cloud Defense Strategies		3	3	-	-	
5		Advanced Network and Infrastructure Security		3	3	-	-	
6		Advanced Threat Detection & Monitoring		3	3	-	-	2 & 3
7		AI for Cyber Defense		3	3	-	-	6
Digital Forensics and Incident Response (DFIR)								
1		Storage, Filesystems and Host Forensics		3	3	-	-	Network & Infrastructure Security
2		Incident Response Planning & Operations		3	3	-	-	1
3		Network Forensics		3	3	-	-	Network & Infra. structure Security
4		Cloud/Mobile Forensics		3	3	-	-	1-3
5		Advanced Digital Forensics and Incident Response (DFIR)		3	3	-	-	3-5
6		IoT & Embedded Systems Forensics		3	3	-	-	
C. Security Management								
1		Information Security Governance, Risk, and Compliance (GRC)		3	3	-	-	Adv. Info. Security
2		Cybersecurity Risk Management		3	3	-	-	1
3		Business Continuity and Disaster Recovery (BCDR)		3	3	-	-	1 & 2
4		Security Architecture		3	3	-	-	1 & 2
5		Security Strategy & Policy Design		3	3	-	-	1 & 2

Elective Course of the Master of Cybersecurity Program

No.	Course Code	Course Name	اسم المقرر	CHs	L	T	P	Prerequisites, Co-requisites
6		Information Security Auditing & Assessment		3	3	-	-	1 & 2
7		Third-Party & Supply Chain Risk Management		3	3	-	-	5
8		Building and Leading Security Operations Centers		3	3	-	-	4 & 5

متطلبات/ شروط القبول في البرنامج Admission Requirements for the Program

Admission Requirements:

- Applicants must satisfy the General Requirements and admission rules set of the Ministry of Pedagogical & Education and Scientific Research, and Sana'a University.
- A Bachelor Degree in Computing Science or equivalent degree in any computing fields from a recognized university.
- The priority for the enrollment in the program is for applicants who hold a BSc degree in Computer Science, Software Engineering.
- Official certificates and transcripts of the applicant from all college studies must be submitted. He may submit a detailed résumé if he would like here academic and professional background to be considered.
- Applicants who hold BSc in other related disciplines should have a satisfactory background in core areas of computer/computing science which may include:
 - Mathematics in Computing (2 Semesters – at least 6 CHs)
 - Discrete Mathematics.
 - Linear Algebra.
 - Probability and Statistics.
 - Programming Languages (2 Semesters – at least 6 CHs).
 - Data Structures and Algorithms.
 - Operating Systems.
 - Computer Networks.
 - Computer Organization and Architecture.
- If the applicant's prior education does not include the courses listed above, the applicant may still enroll under provisional status, followed by full admission have completed the missing courses.
- The department council identify the required pre-requisite courses based on applicant's transcript before a change of status to regular graduate student.

شروط القبول
&
التخصصات المطلوبة :

درجة اللغة المطلوبة
TOEFL / IBT

مهارات الحاسوب
(ICDL)

شروط أخرى:
مثل (اختبار القبول/
المقابلة الشخصية)

- Pass the aptitude test and personal interview (if available).
- Any other conditions approved by the relevant committees and councils at the faculty and university.

متطلبات التخرج من البرنامج :Graduation Requirements

- بالإضافة إلى المتطلبات الواردة في لائحة الدراسات العليا والبحث العلمي بالجامعة والتي يجب تحقيقها، يحصل الطالب على درجة الماجستير إذا أكمل 36 ساعة معتمدة بنجاح وفقاً للشروط والمتطلبات التالية:
1. أن يكمل الطالب بنجاح 24 ساعة معتمدة بواقع ثمانية مقررات دراسية.
 2. يعتبر الطالب ناجحاً في المقرر إذا حصل على 65% على الأقل من إجمالي درجة المقرر.
 3. أن يحصل الطالب على معدل تراكمي 75% على الأقل لكي يتمكن من تسجيل الرسالة البحثية.
 4. إتمام أطروحة الماجستير والدفاع عنها بنجاح بواقع 6 ساعات معتمدة.
 5. نشر ورقة بحثية على الأقل في مجلة محكمة كجزء من رسالة الماجستير.

In addition to the requirements stipulated in the university's Graduate Studies and Scientific Research Regulations, which must be met, a student is awarded a master's degree if they successfully complete 36 credit hours according to the following conditions and requirements:

1. The student must successfully complete 24 credit hours, consisting of eight courses.
2. The student is considered to have passed the course if they obtain at least 65% of the total course grade.
3. The student must obtain a cumulative GPA of at least 75% to be able to register for the research thesis.
4. The master's thesis must be successfully completed and defended, with a total of 6 credit hours.
5. At least one research paper must be published in a peer-reviewed journal as part of the master's thesis.

المصادر والتجهيزات والامكانيات اللازمة لتنفيذ البرنامج:

Resource and equipment's needed for Program Implementations

مثل: مصادر التعلم/ التجهيزات والأدوات والمواد التعليمية/ المعامل والمختبرات وغيرها...

الكادر التدريسي:

أستاذ مساعد	أستاذ مشارك	أستاذ	
2	2	1	الكادر المطلوب
2	2	1	الكادر المتوفر
يتوفر في الكلية كادر كافي – 26 عضو هيئة تدريس (7 أستاذ، 9 أستاذ مشارك، و 10 أستاذ مساعد)			ملاحظة

تقويم البرنامج وتحسينه Program evaluation and improvement

العينة Sample	طريقة التقويم Assessment method	الفئة المستهدفة Targeted
All candidates	Interviews Questionnaires	Final Year Students
All candidates	Interviews Questionnaires Meetings	Graduates

As many as possible	Survey	Employers
	Questionnaires	
Experts from CAQA, Ministry of Higher Education.	Reports	Council of Accreditation and Quality Assurance

وصف مقررات البرنامج:

Appendix 1: Program Standards & Benchmarks:

Program Standards & Benchmarks:

1. Program Standards

2. Graduate studies system at Yemeni universities, Prime Ministerial Decision No. (40) of 2008 regarding the postgraduate studies system at Yemeni universities.
3. Systems and Regulations issued by the Ministry of Higher Education.
4. Council of Accreditation & Quality Assurance, National Academic Reference Standard (NARS) for Computing Programs, January 2023.
5. ABET: Computing Accreditation Commission; Criteria for Accrediting Computing Programs; Effective for Reviews during the **2025-2026** Accreditation Cycle; GENERAL CRITERIA FOR MASTER'S LEVEL PROGRAMS: General Criteria for Stand-Alone Master's Programs, **2025**.

2. Program Benchmarks; Similar Programs:

1. King Fahd University of Petroleum & Minerals (KFUPM), College of Computing and Mathematics, Information & Computer Science Department, Master of Cybersecurity; https://bulletin.kfupm.edu.sa/main/program?program_id=145&title=master-of-science-in-security-and-information-assurance.
2. University of London, MSc Cyber Security; <https://www.london.ac.uk/study/courses/postgraduate/msc-cyber-security>.
3. Princess Sumaya University for Technology, Master's Degree in Cyber Security; <https://www.psut.edu.jo/en/program/master-of-science-program-in-Cyber-security>.
4. SANS Technology Institute, Cybersecurity Master's Degree; <https://www.sans.edu/cyber-security-programs/masters-degree/?msc=main-nav>.
5. University of Twente, ; Master's in Computer Science with a specialisation in Cyber Security; <https://www.utwente.nl/en/education/master/programmes/computer-science/specialisation/cyber-security/courses-research/>.
6. Universiti Teknologi Malaysia (UTM), Master of Cyber Security - Course Offered; <https://comp.utm.my/master-csy/>.

Appendix 2: Survey of Similar Accredited Programs at National and International Universities (Benchmarks)

Program No.	The Academic Program	The University	Website	The Faculty	The Department	The Country	Degree Award at Program Completion	Program Accrediting Body	Year of Accreditation	Study Duration
Current Program	Master of Cybersecurity	Sana'a University	https://su.edu.ye	Faculty of Computer and Information Technology (FCIT)	Cybersecurity	Yemen	Master of Cybersecurity	New	New	2 Years
The 1 st Program	M.S. in Security & Information Assurance	King Fahd University of Petroleum & Minerals	https://bulletin.kfupm.edu.sa/main/program?program_id=145&title=master-of-science-in-security-and-information-assurance	College of Computing and Mathematics	Information & Computer Science	King of Saudi Arabia	Master of Cybersecurity	---	---	2 Years
The 2 nd Program	Master of Science in Cyber Security	University of London	https://www.london.ac.uk/study/courses/postgraduate/msc-cyber-security	---	---	UK	MSc Cyber Security	---	---	2-5 years
The 3 rd Program	Master of Cyber Security	Princess Sumaya University for Technology	https://www.psut.edu.jo/en/program/master-of-science-program-in-Cyber-security	King Hussein School of Computing Sciences	Cyber Security Department	Jordan	MSc Cyber Security	---	---	2 Years
The 4 th Program	Master's Degree in Cybersecurity	SANS Technology Institute	https://www.sans.edu/cyber-security-programs/masters-degree/?msc=main-nav	SANS Technology Institute	Master of Science in Information Security Engineering	USA	Master of Cybersecurity	---	---	3-5 Years
The 5 th Program	Master of Cyber Security	University of Twente	https://www.utwente.nl/en/education/master/programmes/computer-science/specialisation/cyber-security/	Electrical Engineering Mathematics and Computer Science (EEMCS)	Computer Science	Dutch	Master's in Computer Science with a specialization in Cyber Security	---	---	2 Years

Program No.	The Academic Program	The University	Website	The Faculty	The Department	The Country	Degree Award at Program Completion	Program Accrediting Body	Year of Accreditation	Study Duration
The 6 th Program	Cyber Security (Course Offered)	Universiti Teknologi Malaysia (UTM)	https://comp.utm.my/master-csy/	Faculty of Computing	Computer Science	Malaysia	Master of Cyber Security	---	---	1.5 years

Appendix 3: Survey of PILOs for Similar Accredited Programs at National and International Universities

Current Program PILOs	Similar Accredited Programs						Accreditation Bodies
	The 1 st Program	The 2 nd Program	The 3 rd Program	The 4 th Program	The 5 th Program	The 6 th Program	ABET
A1	PILO1	GPILO 1, 2; A1,2,5,7-11; B10,11	PILO4	PILO1,4	Know 1,2,3	A1	SO 4
B1	PILO2	A6,12,13; B8	PILO1, 7	PILO1,2	Value1	C3	SO 1
B2	PILO2	A8; B9; C3,10,11,13	PILO2	PILO1,2,5	Skill1; Value1	B1	SO 2
C1	PILO4	B2,3; C2	PILO6	PILO2	Skill2	C1	SO 1
C2	PILO1	GPILO 3, 4; B4; C4,5,6	PILO6	PILO4	Skill3	C2	SO 2
C3	PILO1	A4; B7; B12,14; C1	PILO7	PILO3,5	Skill 1	C3	SO 4
D1	PILO3	B1,5,6; C8,9	PILO3, 5	PILO3	Skill 3	D1,2,3	SO 3, SO 5
D2	PILO1	GPILO 5; A3; B13; C7,12	PILO4	PILO4,5	Value2; Skill3	D4,5,6	SO 4

Appendix 3: Survey of Number of Courses and Credit Hours of Similar Programs

University		Sana'a University		KFUPM: King Fahd University of Petroleum & Minerals		University of London		Princess Sumaya University for Technology		SANS Technology Institute		University of Twente		Universiti Teknologi Malaysia		Average	
		CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses
Program Name		Master of Cybersecurity		Master of Cybersecurity		MSc Cyber Security		Master's Degree in Cyber Security		Master's Degree in Cyber Security		Master's in CS with Cyber Security special.		Master of Cyber Security			
Total CHs and Courses		36	10	30	8 + 1 ¹	180 ²	11	34	10	36	16	120	18	45	15		
Requirement	Type	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses
University Requirements	Compulsory	0	0	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Electives	0	0	--	--	--	--	--	--	--	--	--	--	3	1	--	--
	Percentage	0%	0%	--%	--%	--%	--%	--%	--%	--%	--%	--%	--%	6.67%	7.69%	--%	--%
Faculty Requirements	Compulsory	3	1	--	--	--	--	--	--	--	--	--	--	3	1	--	--
	Electives	0	0	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Percentage	8.3%	9.09%	--%	--%	--%	--%	--%	--%	--%	--%	--%	--%	6.67%	7.69%	--%	--%
Department Requirements	Compulsory	0	0	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Electives	0	0	6 ²	2	--	--	--	--	--	--	--	--	--	--	--	--
	Percentage	0%	0%	20%	20%	--%	--%	--%	--%	--%	--%	--%	--%	--%	--%	--%	--%

University		Sana'a University		KFUPM: King Fahd University of Petroleum & Minerals		University of London		Princess Sumaya University for Technology		SANS Technology Institute		University of Twente		Universiti Teknologi Malaysia		Average	
		CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses	CHs	No. of Courses
Program Requirements	Compulsory	18	6	9 + 1 ¹	3 + 1 ¹	150	10	16	6	19	11	55	10	18	6	--	--
	Percentage	50%	54.55%	30%	40%	83%	91%	47.06%	60%	52.78%	68.75%	45.83%	55.56%	40%	46.16%	--%	--%
	Electives	9	3	9	3	0%	0%	9	3	9	3	35	7	9	3	--	--
	Percentage	25%	27.27%	30%	30%	0%	0%	26.47%	30%	25%	18.75%	29.17%	38.88%	20%	23.08%	--%	--%
	Graduation Project/Thesis	6	1	6	1	30	1	9	1	8	2	30	1	12	2	--	--
	Percentage	16.7%	9.09%	20%	10%	17%	9%	26.47%	10%	22.22%	12.5%	25%	5.56%	26.66%	15.38%	--%	--%
	Summer Training	--	--	--	--	--	--	--	--	--	--					--	--
	Percentage	---	--%	--%	--%	--%	--%	--%	--%	--%	--%					--%	--%
	Industrial Training	--	--	--	--			--	--	--	--					--	--
	Percentage	---	--%	--%	--%	%	%	--%	--%	--%	--%					--%	--%
	Practical Skills	--	--	--	--	--	--	--	--	--	--					--	--
	Percentage	---	--%	--%	--%	--%	--%	--%	--%	--%	--%					--%	--%
Total	CHs/Courses	36	11	30	10	180 ³	11	34	10	36	16	120 ⁴	18	45	13		
	Percentage	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%		
Other Courses		0	0	0	0	0	0	0	0	0	0	0	0	6 ⁵	2	--	--
Total		36	11	31	10	36	11	36	11	36	11	36	11	45	15		
		100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%		

¹ The program degree plan in the program website: there is a course " Graduate Seminar – 0 CH" not computed in the total of the program credit hours.

² An Elective Courses are five Courses (15 CHs). The elective courses distributed into: Tree elective courses (9 CHs) are elective from SEC Elective Courses, and tow elective courses (6 CHs) are to be taken according to the approved degree plan.

- ³ In UK, Ten Core Modules: Each core module is worth 15 UK credits. This means each module is designed to require approximately 150 hours of student work (15 credits * 10 hours/credit). In the UK, the Credit Accumulation and Transfer Scheme (CATS) is a system where one credit represents approximately 10 hours of "notional learning time". This includes lectures, seminars, practical work, and independent study.
- ⁴ Master 120 EC: In the Netherlands, each credit represents 28 hours of work. including: • Attending lectures and tutorials, Reading course materials, Preparing for tests and exams, Writing papers and assignments, Participating in group work, • Self-study.
- ⁵ For Non CS Background.

Appendix 4: Comparison of Program Courses and Similar Programs Courses

#	Current Program					1 st Program					2 nd Program					3 rd Program					4 th Program					5 th Program					6 th Program				
	Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours			
		C	H	L	T		P	C	H	L		T	P	C	H		L	T	P	C		H	L	T	P		C	H	L	T		P	C	H	L
1	Research Methodology(FR)	3	3			-----	--	--	--	--	Research Method or Cyber Security	15				Cyber Threat Intelligence	3				Research Methods (0.5 CHs) + Advanced Technical Research & Communication Practicum (3 CHs)	3.5				Research Topics (10 Unit)	10				Research Methodology	3			
2	Advanced Information Security	3	3			Principles of Information Assurance and Security	3				Cyber security foundations	15				Digital Forensics Investigation	3				Security Essentials	3				Computer Ethics	5				Secure Software Engineering	3			
3	Secure Software Development	3	3			Elective I	3				Software and Application Security	15				Seminar (1 CH)	3				Defensible Security Architecture & Engineering	3				Software Security	5				Cloud Computing Security	3			
4	Network and Infrastructure Security	3	3			Network Security	3				Network and Infrastructure Security	15				Advances Network Security	3				Intrusion Detection In-Depth	3				Internet Security	5				Information Security Governance and Risk Management	3			
5		3	3			Elective II	3				Security Management and Governance	15				Legal governance and Compliance	3				IT Security Planning, Policy & Leadership	3				Cyber Risk Management	5				Cryptographic Engineering	3			
6	Cryptography and Data Security	3	3			Cryptography and Data Security	3				Applied Cryptography	15				Advanced Cryptography	3				Situational Response Practicum	1				Security and Cryptography	5				Digital Forensics	3			
7	Hacker Tools, Techniques & Exploits	3	3			SEC/SIA Elective I	3				Computer Systems Security	15				Elective I	1				Hacker Tools, Techniques, Exploits, &	3				Blockchain and Distributed Ledger	5				Penetration Testing	3			



#	Current Program				1 st Program				2 nd Program				3 rd Program				4 th Program				5 th Program				6 th Program																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									
	Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours				Course Name	Course Hours																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																							
		C	H	L	T		P	C	H	L		T	P	C	H		L	T	P	C		H	L	T	P		C	H	L	T	P	C	H	L	T	P																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														

Note:

C H: Credit Hours; L: Lecture; T: Tutorial; P: Lab Session.

Appendix 6: Program Intended Learning Outcomes (PILOs)

I = Introduced; P=Practiced; M/A=Mastered/Advanced

No.	Course Code	Course Title	Program Intended Learning Outcomes (PILOs)							
			A1	B1	B2	C1	C2	C3	D1	D2
1		Advanced Information Security	✓	✓		✓				
2		Network and Infrastructure Security	✓		✓	✓				
3		Hacker Tools, Techniques & Exploits	✓	✓				✓	✓	✓
4		Research Methodology	✓				✓		✓	
5		Secure Software Development	✓		✓	✓			✓	
6		Cryptography and Data Security	✓	✓	✓	✓				
7		Thesis	✓	✓	✓	✓	✓	✓	✓	

Program Intended Learning Outcomes (PILOs)

Upon successful completion of the graduate Cybersecurity Program, the graduates will be able to:

- A1.** Demonstrate deep understanding of advanced security concepts, theories, facts, practices, research methodology, tools and techniques related to cybersecurity field.
- B1.** Analyze the computing effects on society, and evaluate and troubleshoot complex security vulnerabilities, malware, threats, risks and digital crimes to elaborate security solutions.
- B2.** Develop and choose suitable tools, techniques and technology resources to design and implement a complex computing system and creative security solutions to defend individual and organization's computing assets.
- C1.** Apply advanced cybersecurity concepts, theories, facts, tools, techniques and the best practices to detect, prevent, response and recover from cyber-incidents efficiently.
- C2.** Conduct advanced research using cybersecurity research and inquiry methodologies.
- C3.** Manage, troubleshoot complex and advance security vulnerabilities and investigate in the digital crimes in cybersecurity practices.
- D1.** Communicate effectively and perform tasks proficiently in various roles to disseminate and achieve project and research outcomes.
- D2.** Demonstrate a strong commitment to academic and professional responsibilities and ethical conduct, and regulatory compliance with the best practices, while actively engaging in continuous professional development.

Appendix 7: Alignment of Department Mission and Program Mission

Department Program	تقديم تعليم متميز	إنتاج بحوث مبتكرة في مجال الأمن السيبراني	من خلال بيئة محفزة وشراكة مجتمعية فاعلة	إعداد كوادر مؤهلة مهنية وأكاديمية	ملتزمة بأخلاقيات المهنة	تتبع متطلبات سوق العمل	وتساهم في تحقيق التنمية المستدامة والتحول الرقمي الأمن.
إعداد كادر مؤهل ومتميز مهنيًا وبحثيًا	✓			✓			✓
ملتزمًا بأخلاقيات المهنة					✓		
ومزودًا بأحدث المعارف والمهارات التخصصية والشخصية	✓	✓					✓
قادرا على إنتاج بحوث علمية وتقديم حلول أمنية متقدمة في مجال الأمن السيبراني		✓					✓
تتبع احتياجات سوق العمل محليا وإقليميا						✓	
من خلال بيئة محفزة وشراكة مجتمعية فاعلة.			✓				

Appendix 8: Alignment of Program Graduate Attributes and Program Objectives

Attribute Objective	Attrib1	Attrib2	Attrib3	Attrib4	Attrib5	Attrib6	Attrib7	Attrib8
PO1	✓		✓		✓	✓		
PO2	✓	✓	✓	✓	✓	✓	✓	✓
PO3		✓	✓				✓	✓
PO4				✓	✓	✓		

Appendix 8: Alignment of Program Graduate Attributes and Program Intended Learning Outcomes

Attribute Program ILOs	Attrib1	Attrib2	Attrib3	Attrib4	Attrib5	Attrib6	Attrib7	Attrib8
A1	✓			✓	✓	✓	✓	
B1		✓					✓	
B2	✓	✓	✓				✓	
C1	✓	✓	✓		✓	✓	✓	
C2	✓			✓	✓		✓	✓
C3		✓	✓		✓	✓		
D1				✓	✓	✓	✓	
D2		✓	✓			✓	✓	✓

Appendix 9: Graduate Attributes:

Graduate Attributes:

Upon successful completion of Master of Cybersecurity Program, graduates will be able to:

Attrib1. Deep and comprehensive knowledgeable:

- Graduates have deep knowledge and comprehensive understanding of cybersecurity principles, theories, facts, tools, techniques, methodologies, and the threat landscape.

Attrib2. Creative and critical thinker:

- Graduates will be able to creative thinking, analyze and evaluate the effectiveness of security strategies and solutions from various perspectives.
- Graduates will be able to develop creative defenses to face an expect attacker tactics.

Attrib3. Complex system Developer and advanced problem Solver:

- Graduates have capabilities to develop complex security systems.

- Graduates have advanced skills to identify and resolve complicated security issues, troubleshoot incidents, and choose effective countermeasures.

Attrib4. Communicator:

- Graduates will be able to effectively communicate clearly and concisely to transport their ideas and research results professionally to both technical and non-technical audiences.

Attrib5. Project Manager and Collaborator:

- Graduates have the project management principles and methodologies skills within the context of cybersecurity, and can initiate, plan, execute, monitor, and accomplish security projects effectively.
- Graduates can able to work effectively individually or within a team work to achieve shared tasks.

Attrib6. Professional and Responsible:

- Graduates will adhere to professional responsibilities and ethical conduct, act with integrity, and take of their actions and decisions in protection computing assets and regarding user privacy.

Attrib7. Researcher:

- Graduates will possess research skills to explore cybersecurity emerging trends, analyze vulnerabilities and evaluate new security tools through independent study or research.

Attrib8. Self-learner:

- Graduates will be adhering to develop their knowledge and skills through self-study, professional development, and engagement with the cybersecurity community.

Appendix 10: Program Intended Learning Outcomes (PILOs)

1. Program Intended Learning Outcomes (PILOs):

A. Knowledge and Understanding:

Upon successful completion of the graduate Cybersecurity Program, the graduates will be able to:

- A1. Demonstrate deep understanding of advanced security concepts, theories, facts, practices, research methodology, tools and techniques related to cybersecurity field.

B. Cognitive/ Intellectual Skills:

Upon successful completion of the graduate Cybersecurity Program, the graduates will be able to:

- B1. Analyze the computing effects on society, and evaluate and troubleshoot complex security vulnerabilities, malware, threats, risks and digital crimes to elaborate security solutions.
- B2. Develop and choose suitable tools, techniques and technology resources to design and implement a complex computing system and creative security solutions to defend individual and organization's computing assets.

C. Practical and Professional Skills:

Upon successful completion of the graduate Cybersecurity Program, the graduates will be able to:

- C1. Apply advanced cybersecurity concepts, theories, facts, tools, techniques and the best practices to detect, prevent, response and recover from cyber-incidents efficiently.
- C2. Conduct advanced research using cybersecurity research and inquiry methodologies.
- C3. Manage, troubleshoot complex and advance security vulnerabilities and investigate in the digital crimes in cybersecurity practices.

D. General and Transferable Skills:

Upon successful completion of the graduate Cybersecurity Program, the graduates will be able to:

- D1. Communicate effectively and perform tasks proficiently in various roles to disseminate and achieve project and research outcomes.
- D2. Demonstrate a strong commitment to academic and professional responsibilities and ethical conduct, and regulatory compliance with the best practices, while actively engaging in continuous professional development.

Appendix 11: Alignment of Program Objectives and Program Intended Learning Outcomes

Program PILOs \ Program Objectives	PObj1	PObj2	PObj3	PObj4
A1		✓	✓	
B1	✓	✓		✓
B2	✓	✓		✓
C1	✓	✓		✓
C2	✓	✓	✓	
C3	✓	✓		✓
D1		✓	✓	✓
D2	✓	✓		✓

Appendix 12: Program Structure

No	Requirements		No. of Courses	Credit Hours	Rational Weight %
1	University Requirements	Compulsory	--	--	0%
		Elective	--	--	
2	Faculty Requirements	Compulsory	1	3	0.08%
		Elective	--	--	
3	Department Requirements	Compulsory	--	--	0%
		Elective	--	--	
4	Program Requirements	Compulsory	5	15	0.75%
		Elective	4	12	
5	Field Training (if any)	Compulsory	--	--	---%
6	Thesis	Compulsory	1	6	0.17%
	Total:		11 (10 Courses + Thesis)	36	100%



The END
