الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)

The Saudi Cybersecurity Higher Education Framework

(SCyber-Edu – 1: 2020)

إشارة المشاركة: أبيض، تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تـم إنشـاء نظـام بروتوكـول الإشـارة الضوئيـة لمشـاركة أكـبر قـدر مـن المعلومـات الحساسـة ويسـتخدم عـلى نطـاق واسـع في العـالم وهنـاك أربعـة ألـوان (إشـارات ضوئيـة):

أحمر – شخصي وسري للمستلم فقط

المسـتلم لا يحـق لـه مشـاركة المصنـف بالإشـارة الحمـراء مـع أي فـرد سـواء مـن داخـل أو خـارج المنشـأة خـارج النطـاق المحـدد للاسـتلام.

برتقالي – مشاركة محدودة

المسـتلم بالإشـارة البرتقاليـة يمكنـه مشـاركة المعلومـات في نفـس المنشـأة مـع الأشـخاص المعنيـين فقـط، ومـن يتطلـب الأمـر منـه اتخـاذ إجـراء يخـص المعلومـة.

أخضر – مشاركة في نفس المجتمع

حيـث يمكنـك مشـاركتها مـع آخريـن مـن منشـأتك أو منشـأة أخـرى عـلى علاقـة معكـم أو بنفـس القطـاع، ولا يسـمح بتبادلهـا أو نشرهـا مـن خـلال القنـوات العامـة.

أبيض – غير محدود

التحديثات على الوثيقة

النسخة

١,٠

التاريخ

أكتوبر ٢٠٢٠

التغييرات

النسخة الأولى

قائمة المحتويات

١	**المقدمة**	**١٢**
١-١	نطاق الإطار السعودي للتعليم العالي في الأمن السيبراني	١٢
١-٢	المنهجية	١٣
١-٣	المتطلبات السابقة ومتطلبات الرياضيات	١٥
١-٤	هيكل الوثيقة	١٥
٢	**البرامج**	**١٦**
٢-١	الدبلوم المتوسط	١٦
٢-٢	البكالوريوس (مسار في الأمن السيبراني)	١٨
٢-٣	البكالوريوس (برنامج في الأمن السيبراني)	٢٠
٢-٤	الدبلوم العالي (للمختصين في تقنية المعلومات)	٢٢
٢-٥	الدبلوم العالي (لغير المختصين في تقنية المعلومات)	٢٤
٢-٦	الماجستير	٢٦
٢-٧	الدكتوراه	٢٨
٣	**الوحدات المعرفية**	**٣١**
	أساسيات الأمن السيبراني Cybersecurity Foundations (CSF)	**٣١**
	مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)	٣٢
	مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)	٣٣
	أساسيات التشفير Basic Cryptography (BCY)	٣٤
	أساسيات الشبكات Basic Networking (BNW)	٣٥
	أساسيات البرمجة Basic Scripting and Programming (BSP)	٣٦
	الدفاع عن الشبكات Network Defense (NDF)	٣٧

مفاهيم نظم التشغيل Operating Systems Concepts (OSC)	٣٨
التهديدات السيبرانية Cyber Threats (CTH)	٣٩
تخطيط وإدارة الأمن السيبراني Cybersecurity Planning and Management (CPM)	٤٠
السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics and Compliance (PLE)	٤١
إدارة البرامج الأمنية Security Program Management (SPM)	٤٢
تحليل المخاطر السيبرانية Security Risk Analysis (SRA)	٤٣
الخوارزميات المتقدمة Advanced Algorithms (AAL)	٤٤
ضبط الوصول Access Control (ACC)	٤٥
التشفير المتقدم Advanced Cryptography (ACR)	٤٦
الخوارزميات Algorithms (ALG)	٤٧
تقنية وبروتوكولات الشبكات المتقدمة Advanced Network Technology and Protocols (ANT)	٤٨
الاتصالات التناظرية Analog Telecommunications (ATC)	٤٩
الأدوات التحليلية Analytical Tools (ATT)	٥٠
الوعي والفهم Awareness and Understanding (AUU)	٥١
استمرارية الأعمال، والتعافي من الكوارث، وإدارة الحوادث السيبرانية Business Continuity, Disaster Recovery and Incident Management (BDR)	٥٢
الحوسبة السحابية Cloud Computing (CCO)	٥٣
الجريمة السيبرانية Cyber Crime (CCR)	٥٤
مشتريات المكونات Component Procurement (CPP)	٥٥
أخلاقيات الأمن السيبراني Cybersecurity Ethics (CSE)	٥٦
قواعد البيانات Databases (DAT)	٥٧
إدارة البيانات Data Administration (DBA)	٥٨
الاتصالات الرقمية Digital Communications (DCO)	٥٩

التحقيق الجنائي الرقمي Digital Forensics (DFS)	٦٠
سلامة البيانات وتوثيقها Data Integrity and Authentication (DIA)	٦١
التعلّم العميق Deep Learning (DLL)	٦٢
أنظمة إدارة قواعد البيانات Database Management Systems (DMS)	٦٣
بنية الأنظمة الموزعة Distributed Systems Architecture (DSA)	٦٤
تراكيب البيانات(Data Structures (DST	٦٥
التحقيق الجنائي الرقمي في الأجهزة Device Forensics (DVF)	٦٦
الأنظمة المدمجة وإنترنت الأشياء Embedded Systems and Internet of Things (ESI)	٦٧
المحاسبة الجنائية الرقمية Forensic Accounting (FAC)	٦٨
الأساليب المنهجية Formal Methods (FMD)	٦٩
منع الاحتيال وإدارة الحد منه Fraud Prevention and Management (FPM)	٧٠
بنية الأجهزة والعتاد Hardware Architecture (HAA)	٧١
أمن الأجهزة والعتاد والبرمجيات الثابتة Hardware/Firmware Security (HFS)	٧٢
التحقيق الجنائي الرقمي للمضيف Host Forensics (HOF)	٧٣
الهندسة العكسية للأجهزة والعتاد Hardware Reverse Engineering (HRE)	٧٤
بنى توكيد المعلومات Information Assurance Architectures (IAA)	٧٥
الالتزام بتوكيد المعلومات Information Assurance Compliance (IAC)	٧٦
معايير توكيد المعلومات Information Assurance Standards (IAS)	٧٧
أنظمة التحكم الصناعية Industrial Control Systems (ICS)	٧٨
بحث موجه/ دراسة مستقلة Independent/Directed Study/Research (IDR)	٧٩
أنظمة كشف/منع التسلل Intrusion Detection/Prevention Systems (IDS)	٨٠
إدارة الهوية Identity Management (IMM)	٨١
أمن تخزين المعلومات Information Storage Security (ISS)	٨٢

مقدمة في نظرية الحوسبة Introduction to the Theory of Computation (ITC)	٨٣
أمن دورة حياة الأنظمة والمنتجات Life-Cycle Security (LCS)	٨٤
البرمجة منخفضة المستوى Low Level Programming (LLP)	٨٥
إدارة نظام تشغيل لينكس Linux System Administration (LSA)	٨٦
التحقيقات الجنائية الرقمية في الوسائط Media Forensics (MEF)	٨٧
تعلم الآلة Machine Learning (MLL)	٨٨
تقنيات الهاتف الجوال Mobile Technologies (MOT)	٨٩
إدارة أمن الشبكات Network Security Administration (NSA)	٩٠
تقنية وبروتوكولات الشبكات Network Technology and Protocols (NTP)	٩١
التحقيق الجنائي الرقمي في الشبكات Network Forensics (NWF)	٩٢
إدارة نظم التشغيل Operating Systems Administration (OSA)	٩٣
تأمين نظم التشغيل Operating Systems Hardening (OSH)	٩٤
نظرية نظم التشغيل Operating Systems Theory (OST)	٩٥
الخصوصية Privacy (PRI)	٩٦
اختبار الاختراق Penetration Testing (PTT)	٩٧
فحص ضمان الجودة / الوظيفة QA/Functional Testing (QAT)	٩٨
مبادئ الترددات الراديوية Radio Frequency Principles (RFP)	٩٩
توكيد البرمجيات Software Assurance (SAS)	١٠٠
التحكم بالأنظمة System Control (SCC)	١٠١
بروتوكولات الاتصالات الآمنة Secure Communication Protocols (SCP)	١٠٢
أمن سلاسل الإمداد Supply Chain Security (SCS)	١٠٣
برمجة النظم Systems Programming (SPG)	١٠٤
ممارسات البرمجة الآمنة Secure Programming Practices (SPP)	١٠٥

الهندسة العكسية للبرمجيات Software Reverse Engineering (SRE)	١٠٦
التحليل الأمني للبرمجيات Software Security Analysis (SSA)	١٠٧
هندسة أمن الأنظمة Systems Security Engineering (SSE)	١٠٨
تحليل الثغرات الأمنية Vulnerability Analysis (VLA)	١٠٩
تقنيات البيئة الافتراضية Virtualization Technologies (VTT)	١١٠
أمن تطبيقات الويب Web Application Security (WAS)	١١١
إدارة نظام ويندوز Windows System Administration (WSA)	١١٢
شبكات الاستشعار اللاسلكية Wireless Sensor Networks (WSN)	١١٣

١ المقدمة

استناداً إلى تنظيم الهيئة الوطنية للأمن السيبراني الصادر بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٠٢/١١هـ والذي تضمن اختصاصات ومهمات الهيئة ومنها: "بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر، وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة"، وانطلاقاً من حرص الهيئة على بناء وتطوير برامج أكاديمية وطنية عالية الجودة في مجال الأمن السيبراني، فقد عملت الهيئة على إعداد "الإطار السعودي للتعليم العالي في الأمن السيبراني" ليكون دليلاً إرشادياً يمكن الاستفادة منه في تطوير وتقييم واعتماد برامج التعليم العالي في الأمن السيبراني. وقد تم تطوير هذا الإطار من قبل الهيئة بالتنسيق والتعاون مع وزارة التعليم وهيئة تقويم التعليم والتدريب.

يهدف هذا الإطار إلى المساهمة في وضع الحد الأدنى من متطلبات الخطط الدراسية لبرامج التعليم العالي في الأمن السيبراني، وذلك لضمان الجودة الأكاديمية لتلك البرامج، وضمان قدرتها على تخريج كوادر مؤهلة تأهيلاً عاليًا في مجال الأمن السيبراني بحيث ينضمون إلى الكوادر الوطنية العاملة في مجال الأمن السيبراني، ويثرونها بمعرفتهم وخبراتهم، ويسهمون في الجهود الوطنية الرامية للوصول إلى"فضاء سيبراني سعودي آمن وموثوق يُمَكِّن النمو والازدهار".

وقد تم إعداد الإطار السعودي للتعليم العالي في الأمن السيبراني ليكون متوافقًا مع التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات، وإرشادات المركز الوطني للتقويم والاعتماد الأكاديمي.

١-١ نطاق الإطار السعودي للتعليم العالي في الأمن السيبراني

يغطي هذا الإطار برامج الدرجات العلمية بعد المرحلة الثانوية في تخصصات الأمن السيبراني التالية:

١. الدبلوم المتوسط
٢. البكالوريوس
٣. الدبلوم العالي
٤. الماجستير
٥. الدكتوراه

ويمكن الاستفادة من هذا الإطار وتطبيقه على البرامج التعليمية والدرجات العلمية في تخصصات الأمن السيبراني التي يتم تدريسها في المؤسسات التعليمية العامة والخاصة للتعليم بعد المرحلة الثانوية في المملكة العربية السعودية.

في الإصدار الأول من هذا الإطار، تم التركيز على البرامج التعليمية في الأمن السيبراني بشكل عام دون التطرق للبرامج المتخصصة في مجالات فرعية في الأمن السيبراني، على أن تتم في الإصدارات القادمة لهذا الإطار تغطية العديد من برامج التخصصات الفرعية في الأمن السيبراني. وستتم

مراجعة متطلبات الخطط الدراسية الواردة في هذا الإطار وتحديثها بصورة دورية لتواكب التطورات السريعة التي يشهدها مجال الأمن السيبراني.

٢-١ المنهجية

رغم أن مجال الأمن السيبراني يعد من المجالات الحديثة نسبياً مقارنة بالمجالات الأخرى ذات العلاقة التي مضى وقت طويل على ظهورها مثل علوم الحاسب وهندسته ، إلا أن العديد من الدول والمنظمات الأكاديمية الدولية بادرت مؤخراً بوضع أطرٍ خاصة بالتعليم العالي في مجال الأمن السيبراني بهدف ضمان جودة مخرجات برامج التعليم في هذا المجال.

ومن الأمثلة على تلك الأطر: إطار برنامج المراكز الوطنية للتميّز الأكاديمي في الدفاع السيبراني (CAE-CD)[١] في الولايات المتحدة الأمريكية؛ ومعايير مجلس الاعتماد الأكاديمي للهندسة والتكنولوجيا (ABET) لبرامج الحوسبة؛ وإرشادات مناهج الأمن السيبراني من معهد مهندسي الكهرباء والإلكترونيات (IEEE) وجمعية آلات الحوسبة (ACM) في عام ٢٠١٧؛ بالإضافة إلى إطار برامج التعليم العالي المعتمدة من المركز الوطني للأمن السيبراني (NCSC) في المملكة المتحدة. وتتشارك هذه الأطر في عدد من السمات المشتركة. وقد تمت الاستفادة من تلك الأطر الدولية في تحديد منهجية إعداد الإطار السعودي للتعليم العالي في الأمن السيبراني وذلك بوضع الحد الأدنى من متطلبات الخطط الدراسية في الأمن السيبراني لكل برنامج من برامج الدرجات العلمية بتحديد توصيفات البرنامج – Program Descriptors (PD) – التي يتم من خلالها تحديد نواتج التعلم، والوحدات المعرفية – Knowledge Units (KUs) – التي يدرسها الطلبة في البرنامج. وكما ذُكر سابقاً، فقد تم تصميم هذا الإطار بالتوافق مع التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات، وإرشادات المركز الوطني للتقويم والاعتماد الأكاديمي.

تتوافق توصيفات البرنامج في هذا الإطار مع توصيفات مستويات الإطار الوطني للمؤهلات التي تساعد المؤسسات التعليمية على تصميم نواتج التعلم للبرنامج Program Learning Outcomes (PLOs)، وهي مجموعة من المعارف والمهارات والقيم التي من المتوقع أن يكتسبها الخريجون عند استكمال دراسة البرنامج. ويهدف هذا الإطار إلى المساهمة في وضع الحد الأدنى من توصيفات البرنامج التي تُراعَى عند صياغة نواتج التعلم لكل برنامج من برامج الدرجات العلمية في الأمن السيبراني. وتستطيع كل مؤسسة تعليمية إضافة نواتج تعلم أخرى إلى برامجها التعليمية في الأمن السيبراني وفق ما تراه مناسباً.

ويصف هذا الإطار الوحدات المعرفية في الأمن السيبراني حيث أن الوحدة المعرفية هي مجموعة من المواضيع ذات الصلة التي تشكّل محتوى المنهج الذي يتم تدريسه، ومجموعة من نواتج التعلم التي يكتسبها الطلبة بعد إكمال دراسة هذه الوحدة. وتحدد نواتج التعلم الخاصة بكل وحدة معرفية الحد الأدنى لما يُتوقع أن يتعلمه الطالب ويقدر على فعله بعد إتمام دراسة تلك الوحدة المعرفية بنجاح، ومن المهم أن تُراعي المؤسسات التعليمية العمق والتوسع والتدرج في تلك النواتج بما يناسب مستوى البرنامج، وأن تُضمّن نواتج التعلم الخاصة بمهارات التواصل والقيم في المقررات الدراسية. ويحدد الإطار الحد الأدنى من الوحدات المعرفية الأساسية التي يجب أن يغطيها البرنامج بالإضافة إلى قائمة بالوحدات المعرفية الاختيارية. وتستطيع المؤسسات التعليمية

[١] برنامج مراكز التميّز الأكاديمي في الدفاع السيبراني (CAE-CD) هو مبادرة برعاية وكالة الأمن القومي ووزارة الأمن الداخلي في الولايات المتحدة الأمريكية.

طرح الوحدات المعرفية الاختيارية ذات العلاقة ببرامجها والتي يستطيع الطلبة الاختيار من بينها لاستكمال متطلبات تخرجهم. ومن المهم ملاحظة أن الوحدة المعرفية ليست بالضرورة مقرراً دراسياً؛ فبالإمكان تغطية وحدة معرفية بمقرر دراسي واحد أو أكثر، كما يجوز أن يغطي المقرر الدراسي وحدة معرفية واحدة أو أكثر بشكل كامل أو بشكل جزئي.

بالنسبة لبرامج درجة البكالوريوس، فيميز هذا الإطار بين برنامج متخصص في الأمن السيبراني وبرنامج متخصص بأحد تخصصات تقنية المعلومات مع مسار للأمن السيبراني في ذلك البرنامج.

وقد تم استخلاص الوحدات المعرفية في هذا الإطار من المصادر التالية:

١. البرنامج الإرشادي والوحدات المعرفية للمراكز الوطنية للتميّز الأكاديمي في الدفاع السيبراني (CAE-CD)، عام ٢٠١٩.

٢. مناهج الأمن السيبراني من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠١٧.

٣. مناهج علوم الحاسوب من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠١٣.

كما تم إجراء الإضافات والتعديلات اللازمة لتلبية الاحتياجات الوطنية في هذا المجال، وللتوافق مع الأطر ذات الصلة في المملكة.

وهناك ثلاثة أنواع من المتطلبات في هذا الإطار لكل برنامج من برامج الدراسات العليا وهي:

١. متطلبات القبول Admission Requirements: قائمة بالمتطلبات التي يجب على الطالب أن يستوفيها قبل قبوله في البرنامج.

٢. الوحدات المعرفية الأساسية Core KUs: وحدات معرفية إلزامية يجب على الطالب استكمالها بشكل كامل كمتطلب أساسي للتخرج.

٣. الوحدات المعرفية الاختيارية Elective KUs: قائمة بالوحدات المعرفية الاختيارية التي تستطيع المؤسسة التعليمية و/أو الطالب الاختيار من بينها لاستكمال عدد الوحدات المعرفية المطلوبة للتخرج.

١-٣ المتطلبات السابقة ومتطلبات الرياضيات

تعد بعض الوحدات المعرفية متطلبات سابقة لوحدات معرفية أخرى، ومن المهم أن يُراعَى ذلك في الخطط الدراسية للطلبة وترتيبها الزمني بشكل مناسب.

وبالإضافة لذلك، فإن هناك ارتباطاً أساسياً بين علم الرياضيات والعديد من مجالات الأمن السيبراني، وتتطلب معظم برامج الأمن السيبراني بعض الوحدات المعرفية الأساسية في الرياضيات. ولكن الوحدات المعرفية في الرياضيات المطلوبة لبرنامج معيّن تعتمد بشكل كبير على طبيعة هذا البرنامج وتركيزه؛ ولذلك فإنه من المهم أن تُراعي المؤسسات التعليمية التي تقدم برامج البكالوريوس أو الدبلوم المتوسط في مجال الأمن السيبراني تضمين الوحدات المعرفية في الرياضيات ذات الصلة ببرامجها التي تلبي المتطلبات الأساسية للوحدات المعرفية في الأمن السيبراني في برامجها بشكل صحيح.

١-٤ هيكل الوثيقة

تم تنظيم الجزء المتبقي من هذه الوثيقة كما يلي:

القسم الثاني يستعرض برامج الأمن السيبراني المغطاة بالإضافة إلى توصيفات البرامج المستهدفة ومتطلبات الوحدات المعرفية لكل منها. القسم الثالث يصف بشكل تفصيلي جميع الوحدات المعرفية.

٢ البرامج[٢]

٢-١ الدبلوم المتوسط [٣]

٢-١-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• معرفة عامة ومترابطة وفهم للأسس والنظريات والمبادئ والمفاهيم التقنية في مجال الأمن السيبراني. • معرفة وفهم المنهجيات التحليلية التي تستخدم في مواضيع الأمن السيبراني وتفسير المعلومات المتعلقة بها.	• توظيف مجموعة من المعارف النظرية والتقنية في العلوم ذات الصلة وتكييفها لتعكس الفهم النظري في سياقات محددة وغير مألوفة في مجال الأمن السيبراني. • توظيف التفكير النقدي والإبداع، وتقديم الحلول العملية المبتكرة في سياقات متوسطة التعقيد وغير مألوفة، مرتبطة بمجال الأمن السيبراني. • استخدام منهجيات الدراسة والتقصي للاستفادة من نتائجها لحل مشكلات متوسطة التعقيد في الأمن السيبراني. • اختيار واستخدام مجموعة متنوعة من الممارسات والأدوات التقنية وتكييفها للقيام بأنشطة عملية متوسطة التعقيد في مجال الأمن السيبراني. • التواصل بطرق مناسبة؛ وإظهار الفهم والمعرفة ونقلها للمستفيدين في مجال الأمن السيبراني. • تحليل البيانات العددية وتفسيرها، واستخدام التمثيلات البيانية في سياقات متوسطة التعقيد، مرتبطة بمجال الأمن السيبراني.	• الالتزام بأخلاقيات المهنة للأمن السيبراني، وإظهار المواطنة المسؤولة. • إدارة التعلم والعمل ذاتيًا، وتحديد الأهداف والعمل على تحقيقها، واتخاذ القرارات المتعلقة بالتعلم بقدر متوسط من الاستقلالية. • إدارة المهام والأنشطة المتعلّقة بالأمن السيبراني والعمل تحت إشراف غير مباشر. • العمل بشكل تعاوني، وقيادة فرق العمل لأداء مجموعة من المهام، وبقدر من المسؤولية، والعمل على تحقيق الأهداف المشتركة بفاعلية. • تعزيز الجوانب الصحية والنفسية والاجتماعية ذات العلاقة بمجال الأمن السيبراني.

[٢] تمت الاستفادة من المصادر التالية لإعداد محتوى متطلبات البرامج: [١]، [٢].

[٣] يتوافق هذا البرنامج مع برنامج الدبلوم المتوسط في المستوى الخامس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-١-٢ متطلبات القبول

- شهادة ثانوية عامة أو ما يعادلها.

٢-١-٣ الوحدات المعرفية الأساسية

- أساسيات الأمن السيبراني Cybersecurity Foundations (CSF)
- مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
- مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- أساسيات الشبكات Basic Networking (BNW)
- أساسيات البرمجة Basic Scripting and Programming (BSP)
- الدفاع عن الشبكات Network Defense (NDF)
- مفاهيم نظم التشغيل Operating Systems Concepts (OSC)
- التهديدات السيبرانية Cyber Threats (CTH)
- السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics and Compliance (PLE)
- تحليل المخاطر السيبرانية Security Risk Analysis (SRA)

٢-١-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (٣) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٢ البكالوريوس (مسار في الأمن السيبراني)[٤]

٢-٢-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• معرفة بنطاق واسع ومتعمق من الأسس والنظريات والمبادئ والمفاهيم الأساسية في مجال الأمن السيبراني. • المعرفة والفهم المتعمق للعمليات والأدوات والتقنيات، والسياسات والممارسات المستخدمة في الأمن السيبراني. • مجموعة من المعارف المتخصصة والمتعلقة بالتطورات الحالية والمستجدة في مجال الأمن السيبراني.	• تحليل وتقييم المعلومات المعقدة والمتنوعة في مجال الأمن السيبراني. • التقييم النقدي واختيار واستخدام أساليب ومنهجيات وأدوات الأمن السيبراني لحل المشكلات، وتقليل المخاطر، وأداء أعمال الأمن السيبراني . • استخدام منهجيات الدراسة والتقصي والأبحاث في مشاريع وأنشطة الأمن السيبراني. • أداء مجموعة من المهام والإجراءات باستخدام أدوات الأمن السيبراني في العمليات المعقّدة والمتنوّعة. • التواصل بالطرق المناسبة ونقل المعرفة والمهارات المتخصصة وبناء علاقات مهنية واجتماعية. • استخدام العمليات الرياضية والأساليب الكمية؛ لمعالجة البيانات والمعلومات في سياقات معقدة ومتنوعة في مجال الأمن السيبراني.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار المواطنة المسؤولة. • اتخاذ قرارات بنّاءة في الحالات التي تتطلب الاعتماد على النفس للعمل والتعلم والابتكار باستقلالية. • إدارة المهام المتعلقة بالأمن السيبراني باستقلالية. • العمل بشكل تعاوني وبنّاء، والقدرة على القيادة وريادة الأعمال وأداء مجموعة من المهام بمسؤولية. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

٢-٢-٢ متطلبات القبول

- شهادة ثانوية عامة أو ما يعادلها.

[٤] يتوافق هذا البرنامج مع برامج البكالوريوس في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٢-٣ الوحدات المعرفية الأساسية

- أساسيات الأمن السيبراني Cybersecurity Foundations (CSF)
- مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
- مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- أساسيات الشبكات Basic Networking (BNW)
- أساسيات البرمجة Basic Scripting and Programming (BSP)
- الدفاع عن الشبكات Network Defense (NDF)
- مفاهيم نظم التشغيل Operating Systems Concepts (OSC)
- التهديدات السيبرانية Cyber Threats (CTH)
- السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics and Compliance (PLE)
- تحليل المخاطر السيبرانية Security Risk Analysis (SRA)
- تراكيب البيانات Data Structures (DST)
- قواعد البيانات Databases (DAT)

٢-٢-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (٤) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٣ البكالوريوس (برنامج في الأمن السيبراني)[٥]

٢-٣-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• معرفة بنطاق واسع ومتعمق من الأسس والنظريات والمبادئ والمفاهيم الأساسية في مجال الأمن السيبراني. • المعرفة والفهم المتعمق للعمليات والأدوات والتقنيات، والسياسات والممارسات المستخدمة في الأمن السيبراني. • مجموعة من المعارف المتخصصة والمتعلقة بالتطورات الحالية والمستجدة والمواضيع المتقدمة في مجال الأمن السيبراني.	• تحليل وتقييم المعلومات المعقدة والمتنوعة في مجال الأمن السيبراني. • التقييم النقدي واختيار واستخدام أساليب ومنهجيات وأدوات الأمن السيبراني لحل المشكلات، وتقليل المخاطر، وأداء أعمال الأمن السيبراني. • استخدام منهجيات الدراسة والتقصي والأبحاث في مشاريع وأنشطة الأمن السيبراني. • أداء نطاق واسع من المهام والإجراءات باستخدام أدوات الأمن السيبراني في العمليات المعقدة والمتنوعة، والإبداع والابتكار في هذا الجانب. • التواصل بالطرق المناسبة ونقل المعرفة والمهارات المتخصصة والمفاهيم المتقدمة وبناء علاقات مهنية واجتماعية. • استخدام العمليات الرياضية والأساليب الكمية؛ لمعالجة البيانات والمعلومات في سياقات معقدة ومتنوعة في مجال الأمن السيبراني.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار المواطنة المسؤولة. • اتخاذ قرارات بنّاءة في الحالات التي تتطلب الاعتماد على النفس للعمل والتعلم والابتكار باستقلالية. • إدارة المهام المتعلقة بالأمن السيبراني باستقلالية. • العمل بشكل تعاوني وبنّاء، والقدرة على القيادة وريادة الأعمال وأداء مجموعة واسعة من المهام بمسؤولية. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

٢-٣-٢ متطلبات القبول

- شهادة الثانوية العامة أو ما يعادلها.

[٥] يتوافق هذا البرنامج مع برامج البكالوريوس في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٣-٣ الوحدات المعرفية الأساسية

- أساسيات الأمن السيبراني Cybersecurity Foundations (CSF)
- مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
- مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- أساسيات التشفير Basic Cryptography (BCY)
- أساسيات الشبكات Basic Networking (BNW)
- أساسيات البرمجة Basic Scripting and Programming (BSP)
- الدفاع عن الشبكات Network Defense (NDF)
- مفاهيم نظم التشغيل Operating Systems Concepts (OSC)
- التهديدات السيبرانية Cyber Threats (CTH)
- السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics and Compliance (PLE)
- تحليل المخاطر السيبرانية Security Risk Analysis (SRA)
- الخوارزميات Algorithms (ALG)
- تراكيب البيانات Data Structures (DST)
- قواعد البيانات Databases (DAT)
- تقنية وبروتوكولات الشبكات Network Technology and Protocols (NTP)
- إدارة أمن الشبكات Network Security Administration (NSA)
- تأمين نظم التشغيل Operating Systems Hardening (OSH)

٢-٣-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (٨) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٤ الدبلوم العالي (للمختصين في تقنية المعلومات)[٦]

٢-٤-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• نطاق متعمق ومتخصص من المعارف النظرية والتقنية والفهم للمواضيع الأساسية في الأمن السيبراني؛ لحماية الأنظمة السيبرانية والدفاع عنها، والاستجابة للحوادث السيبرانية، والتعافي منها. • المعرفة والفهم الدقيق للعمليات، والتقنيات، والسياسات والممارسات المستخدمة في الأمن السيبراني. • فهم عميق للتطورات الجديدة والمواضيع المتقدمة في الأمن السيبراني.	• اختيار المفاهيم النظرية والمنهجيات والتقنيات والأدوات الخاصة بإجراء أعمال الأمن السيبراني وتقييمها واستخدامها في سياقات معقدة ومتقدمة. • تقييم المفاهيم والمبادئ والنظريات الرئيسة في الأمن السيبراني، ومراجعتها بشكل نقدي، وإبداء الرأي فيها. • تقديم وتصميم حلول إبداعية في سياقات معقدة ومتقدّمة لمشكلات في الأمن السيبراني. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • استخدام الطرق الكمية و الكيفية؛ لمعالجة البيانات والمعلومات في سياقات معقدة ومتقدمة في الأمن السيبراني.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم والمواطنة المسؤولة. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال واستقلالية عالية في مجال الأمن السيبراني. • التعاون والمشاركة بفاعلية في مشاريع مهنية، وتولي دور القيادة، وتحمّل مسؤولية عالية. • المشاركة الفعالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

٢-٤-٢ متطلبات القبول

- شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة.
- كفاءة اللغة الإنجليزية.

٢-٤-٣ الوحدات المعرفية الأساسية

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني (المدرجة في القسم٢-٢-٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.

[٦] يتوافق هذا البرنامج مع برنامج الدبلوم العالي في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية.

٢-٤-٤ الوحدات المعرفية الاختيارية

- يجب على الطلبة إكمال (٨) وحدات معرفية اختيارية على الأقل قبل التخرج، وتشمل الوحدات المعرفية الاختيارية المتاحة لهذا البرنامج جميع الوحدات المعرفية باستثناء كلٍ من:
  - الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني (المدرجة في القسم ٢-٢-٣).
  - الوحدات المعرفية التالية:
    - الوعي والفهم Awareness and Understanding (AUU)
    - أساسيات التشفير Basic Cryptography (BCY)
    - الجريمة السيبرانية Cyber Crime (CCR)
    - مشتريات المكونات Component Procurement (CPP)
    - أخلاقيات الأمن السيبراني Cybersecurity Ethics (CSE)
    - أنظمة إدارة قواعد البيانات Database Management Systems (DMS)
    - إدارة نظام تشغيل لينكس Linux System Administration (LSA)
    - إدارة نظام ويندوز Windows System Administration (WSA)

٢-٥ الدبلوم العالي (لغير المختصين في تقنية المعلومات)[٧]

٢-٥-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• نطاق من المعارف النظرية المتخصصة والفهم للمواضيع الأساسية في الأمن السيبراني؛ لتحليل المخاطر، والتخطيط لحماية الأنظمة والدفاع عنها، وإدارة الاستجابة للحوادث والتهديدات السيبرانية. • المعرفة والفهم الدقيق للنواحي التنظيمية والأخلاقية، والعمليات، والسياسات، والممارسات، والحوكمة، وإدارة المخاطر، ومتابعة الالتزام بالضوابط والمعايير في مجال الأمن السيبراني. • فهم عميق للتطورات الجديدة في الأمن السيبراني.	• تطبيق المبادئ والمنهجيات والمفاهيم والأدوات الخاصة في سياقات متقدمة في الأمن السيبراني. • تحليل وبناء وتحديث السياسات، والنواحي التنظيمية والأخلاقية، ومتابعة الالتزام بها، وإدارة المخاطر، والحوكمة في مجال الأمن السيبراني. • تقييم المفاهيم والمبادئ والمنهجيات الرئيسة ومراجعتها بشكل نقدي، وإبداء الرأي فيها، وتقديم حلول إبداعية في سياقات معقدة ومتقدّمة لمشكلات في الأمن السيبراني. • أداء مجموعة من المهام والإجراءات باستخدام أدوات لتقييم المخاطر السيبرانية. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • استخدام الطرق الكمية والكيفية؛ لمعالجة البيانات والمعلومات في سياقات متقدمة في الأمن السيبراني.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم والمواطنة المسؤولة. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال واستقلالية عالية في مجال الأمن السيبراني. • التعاون والمشاركة بفاعلية في مشاريع مهنية، وتولي دور القيادة، وتحمّل مسؤولية عالية. • المشاركة الفعالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

٢-٥-٢ متطلبات القبول

- شهادة بكالوريوس.
- كفاءة اللغة الإنجليزية.

[٧] يتوافق هذا البرنامج مع برنامج الدبلوم العالي في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية.

٢-٥-٣ الوحدات المعرفية الأساسية

- أساسيات الأمن السيبراني Cybersecurity Foundations (CSF)
- مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
- مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- التهديدات السيبرانية Cyber Threats (CTH)
- السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics and Compliance (PLE)
- تحليل المخاطر الأمنية Security Risk Analysis (SRA)

٢-٥-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا وحدتين معرفيتين اختياريتين على الأقل قبل التخرج.

٦-٢ الماجستير[٨]

٢-٦-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• معرفة بنطاق واسع ومتعمق من الموضوعات النظرية والتقنية في مجال الأمن السيبراني. • فهم عميق للعمليات والممارسات في الأمن السيبراني لحماية الأنظمة السيبرانية والدفاع عنها والاستجابة للهجمات السيبرانية المتقدمة والتعافي منها. • فهم عميق للتطورات والنظريات الحديثة والمتقدمة في الأمن السيبراني.	• استخدام مجال واسع من الأدوات والأساليب والممارسات المتخصصة القائمة على معرفة بأحدث التطورات في مجال الأمن السيبراني. • تخطيط وتنفيذ الأبحاث السيبرانية المتقدمة والمشاريع الابتكارية لتطوير منتجات وخدمات الأمن السيبراني. • استخدام مجال كبير من المنهجيات والأساليب والممارسات في سياقات معقدة ومتقدمة في مجال الأمن السيبراني وتقييمها وإجراء مراجعة نقدية لها. • استخدام عمليات وتقنيات وأدوات متقدمة ومتخصصة؛ للقيام بالأعمال المعقدة في الأمن السيبراني. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • استخدام الطرق الكمية والكيفية؛ لمعالجة البيانات والمعلومات في سياقات معقدة ومتقدمة في الأمن السيبراني.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم والمواطنة المسؤولة. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال واستقلالية عالية في مجال الأمن السيبراني. • التعاون والمشاركة بفاعلية في مشاريع مهنية، وتولي دور القيادة، وتحمّل مسؤولية عالية. • المشاركة الفعالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

٢-٦-٢ متطلبات القبول:

- شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة.
- كفاءة اللغة الإنجليزية.

[٨] يتوافق هذا البرنامج مع برنامج الماجستير في المستوى السابع في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٦-٣ الوحدات المعرفية الأساسية:

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني (المدرجة في القسم ٢-٢-٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.
- إتمام رسالة أو مشروع حول موضوع في الأمن السيبراني.

٢-٦-٤ الوحدات المعرفية الاختيارية:

- يجب على الطلبة إكمال (٧) وحدات معرفية اختيارية على الأقل قبل التخرج، وتشمل الوحدات المعرفية الاختيارية المتاحة لهذا البرنامج جميع الوحدات المعرفية باستثناء كلٍ من:
  - الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني (المدرجة في القسم ٢-٢-٣).
  - الوحدات المعرفية التالية:
    - الوعي والفهم Awareness and Understanding (AUU)
    - أساسيات التشفير Basic Cryptography (BCY)
    - الجريمة السيبرانية Cyber Crime (CCR)
    - مشتريات المكونات Component Procurement (CPP)
    - أخلاقيات الأمن السيبراني Cybersecurity Ethics (CSE)
    - أنظمة إدارة قواعد البيانات Database Management Systems (DMS)
    - إدارة نظام تشغيل لينكس Linux System Administration (LSA)
    - إدارة نظام ويندوز Windows System Administration (WSA)

٢-٧ الدكتوراه[٩]

٢-٧-١ توصيفات البرنامج

المعارف	المهارات	القيم والمسؤولية والاستقلالية
• معرفة وفهم عميق لنطاق واسع من الموضوعات في مجال الأمن السيبراني، تتكامل فيها الموضوعات المتقدمة والنظريات المتخصصة، والمبادئ والمفاهيم الرائدة اللازمة لإيجاد معرفة جديدة وأصيلة، وتتضمّن تكامل المجالات فيما بينها. • المعرفة والفهم التفصيلي الدقيق بعمليات، وتقنيات، وسياسات، وممارسات الأمن السيبراني لحماية البيانات والأنظمة والشبكات. • معرفة وفهم شامل للتطورات الحديثة والقضايا والتحديات الناشئة في الأمن السيبراني.	• تقويم المفاهيم والمبادئ والنظريات الحديثة، والجمع بينها، والمراجعة النقدية لها، وتطوير حلول إبداعية ومبتكرة ورائدة لقضايا ومشكلات ومنتجات وخدمات عالية التعقيد وحديثة في مجال الأمن السيبراني. • استخدام نطاق واسع من المنهجيات والأساليب والسياسات والممارسات في مجال الأمن السيبراني وتقييمها وإجراء مراجعة نقدية لها. • تطوير مناهج البحث والاستقصاء المتقدّمة وتكييفها وتطبيقها؛ لإيجاد معرفة أصيلة تُسهم بشكل كبير في الأمن السيبراني. • استخدام عمليات وتقنيات وأدوات وأجهزة متقدمة وحديثة، في مجال الأمن السيبراني، للقيام بأنشطة عملية مستجدة وصعبة وعالية التعقيد. • التواصل بطرق متعددة؛ لنشر المعرفة الأصيلة والرؤى الجديدة وتعزيزها، وإجراء حوار علمي ومهني مع الأقران والمجموعات المتخصصة والمجتمع ككل. • معالجة البيانات الكمية والكيفية وتفسيرها، واستخدامها في البحوث والمشاريع أو الابتكارات الحديثة وعالية التعقيد، المرتبطة بمجال الأمن السيبراني.	• إظهار مستوى عالٍ من النزاهة والقيم الأكاديمية في مجال الأمن السيبراني عند التعامل مع القضايا الأخلاقية والمهنية الناشئة والبحث والمعرفة، ودعمها. • تطوير الخبرات المهنية بصورة مستمرة، واتخاذ قرارات استراتيجية أكاديمية ومهنية باستقلالية عالية. • صياغة أو استحداث حلول مبتكرة للمهمات المعقدة. • التعاون والمشاركة في المجموعات البحثية والمهنية المتنوعة باحترافية عالية، وتولي زمام المبادرة والقيادة فيها، وتحمّل مسؤولية أنشطته العلمية. • تعزيز العلاقات المهنية وخدمة المجتمع في مجال الأمن السيبراني.

[٩] يتوافق هذا البرنامج مع برنامج الدكتوراه في المستوى الثامن في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٧-٢ متطلبات القبول

- شهادة الماجستير في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة.
- كفاءة اللغة الإنجليزية.

٢-٧-٣ الوحدات المعرفية الأساسية

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني (المدرجة في القسم٢-٢-٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.
- إتمام رسالة علمية حول موضوع في الأمن السيبراني.

٢-٧-٤ الوحدات المعرفية الاختيارية

- يجب على الطلبة إكمال (٣) وحدات معرفية اختيارية على الأقل قبل التخرج، وتشمل الوحدات المعرفية الاختيارية المتاحة لهذا البرنامج جميع الوحدات المعرفية باستثناء كلٍ من:
  - الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني (المدرجة في القسم ٢-٢-٣).
  - الوحدات المعرفية التالية:
    - الوعي والفهم Awareness and Understanding (AUU)
    - أساسيات التشفير Basic Cryptography (BCY)
    - الجريمة السيبرانية Cyber Crime (CCR)
    - مشتريات المكونات Component Procurement (CPP)
    - أخلاقيات الأمن السيبراني Cybersecurity Ethics (CSE)
    - أنظمة إدارة قواعد البيانات Database Management Systems (DMS)
    - إدارة نظام تشغيل لينكس Linux System Administration (LSA)
    - إدارة نظام ويندوز Windows System Administration (WSA)

	الدبلوم المتوسط	البكالوريوس (مسار في الأمن السيبراني)	البكالوريوس (برنامج في الأمن السيبراني)	الدبلوم العالي (لغير المختصين في تقنية المعلومات)	الدبلوم العالي (للمختصين في تقنية المعلومات)	الماجستير	الدكتوراه
متطلبات القبول	شهادة الثانوية العامة أو ما يعادلها			شهادة بكالوريوس	شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة		شهادة الماجستير في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة
	كفاءة اللغة الإنجليزية						
الوحدات المعرفية الأساسية	CSF, CDP, ISC, BNW, BSP, NDF, OSC, CTH, PLE, SRA	CSF, CDP, ISC, BNW, BSP, NDF, OSC, CTH, PLE, SRA, DST, DAT	CSF, CDP, ISC, BCY, BNW, BSP, NDF, OSC, CTH, PLE, SRA, ALG, DST, DAT, NTP, NSA, OSH	CSF, CDP, ISC, CTH, PLE, SRA	إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية	إتمام رسالة أو مشروع حول موضوع في الأمن السيبراني	إتمام رسالة علمية حول موضوع في الأمن السيبراني
الوحدات المعرفية الاختيارية	٣ وحدات معرفية اختيارية على الأقل	٤ وحدات معرفية اختيارية على الأقل	٨ وحدات معرفية اختيارية على الأقل	وحدتين معرفيتين اختياريتين	٨ وحدات معرفية اختيارية على الأقل	٧ وحدات معرفية اختيارية على الأقل	٣ وحدات معرفية اختيارية على الأقل
	من المستحسن أن تقتصر الوحدات المعرفية الاختيارية على تلك التي تغطي مواضيع متقدمة نسبيًا						

الشكل١: ملخص متطلبات القبول، والوحدات المعرفية الأساسية، والوحدات المعرفية الاختيارية لجميع البرامج.

٣ الوحدات المعرفية

أساسيات الأمن السيبراني Cybersecurity Foundations (CSF)

الوصف	تقدم هذه الوحدة المعرفية معارف عامة حول المفاهيم الأساسية في مجال الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أهمية الأمن السيبراني ٢. المخاطر والتهديدات والثغرات السيبرانية ٣. المحافظة على السرية والسلامة والتوافر ٤. ضبط الوصول والتوثيق والتصريح وعدم الإنكار ٥. التشفير واستخداماته ٦. الحوكمة وإدارة المخاطر السيبرانية ٧. حماية البيانات والأنظمة والشبكات ٨. الدراية الأمنية ورصد التهديدات السيبرانية ٩. اكتشاف الحوادث السيبرانية والاستجابة لها ١٠. التقنيات والحلول المستخدمة في الأمن السيبراني ١١. الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المصطلحات والمفاهيم الأساسية في مجال الأمن السيبراني. ٢. استعراض المخاطر والتهديدات والثغرات السيبرانية. ٣. شرح المنهجيات والتقنيات المستخدمة لحماية البيانات والأنظمة والشبكات. ٤. مناقشة الإجراءات المناسبة لإدارة المخاطر السيبرانية والاستجابة للحوادث السيبرانية.

مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)

الوصف	تتضمن هذه الوحدة المعرفية المعارف والمهارات الخاصة بأساسيات التصميم الآمن لتصميم أنظمة سيبرانية آمنة وموثوقة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أساسيات وأهمية التصميم الآمن للبرامج والأنظمة ٢. فصل المهمات ٣. العزل ٤. دمج العناصر مع بعضها في مكون واحد ٥. تصميم الوحدات ٦. البساطة في التصميم ٧. تقليص التنفيذ ٨. التصميم المفتوح ٩. التسوية الكاملة ١٠. تصميم الدفاع الأمني متعدد الطبقات ١١. نماذج مستويات أمن النظم وصلاحيات الوصول ١٢. وضع السلامة والأمان في حالة الأعطال ١٣. تقليل المفاجآت في أداء الأجهزة ١٤. تقليص سطح الثقة ١٥. التصميم الآمن وسهولة الاستخدام ١٦. علاقات الثقة ١٧. أنماط البرمجة الآمنة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التعبير عن مبادئ التصميم الآمن. ٢. شرح أهمية مبادئ تصميم الأمن السيبراني وأثر كل مبدأ على تصميم الأنظمة الموثوقة. ٣. تمييز مبدأ التصميم الذي تمت مخالفته لكل نقطة من نقاط الضعف الأمنية الشائعة في الأنظمة. ٤. تحليل مبادئ تصميم الأمن السيبراني المطلوبة في إعدادات معينة. ٥. تطبيق مبادئ تصميم الأمن السيبراني على برامج و/أو أنظمة غير معقدة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٥].

مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة حول مكونات أنظمة تقنية المعلومات الشائعة والآثار العامة للأمن السيبراني المرتبطة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. حماية الأجهزة الطرفية في الشبكات ٢. أجهزة التخزين ٣. بنى الأنظمة ٤. البيئات الافتراضية والحوسبة السحابية ٥. بيئات التحكم الإشرافي وجمع البيانات (SCADA) وبيئات الاستجابة اللحظية والبنى التحتية الحساسة ٦. الشبكات المحلية والشبكات اللاسلكية والإنترنت ٧. التعيينات الشبكية ٨. مكونات أمن الشبكات ٩. أنظمة رصد ومنع التسلل ١٠. الاستجابة للحوادث السيبرانية ١١. الخدمات المدارة ١٢. أمن البرمجيات ١٣. إدارة الإعدادات ١٤. التحديثات والإصلاحات البرمجية ١٥. فحص الثغرات الأمنية ١٦. الأشخاص ودورهم الأمني ١٧. الأمن المادي والبيئي ١٨. إنترنت الأشياء
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التعرّف على مكونات أنظمة تقنية المعلومات من أجهزة وبرمجيات، وتوضيح وظائفها الأساسية. ٢. شرح التأثيرات الرئيسية للأمن السيبراني في بيئات تقنية المعلومات الحالية والمستقبلية. ٣. التعبير عن أنظمة الأمن السيبراني الشائعة ومكوناتها وأنشطتها وقيمها بالنسبة للأمن السيبراني.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

أساسيات التشفير Basic Cryptography (BCY)

الوصف	توفر هذه الوحدة المعرفية مقدمة في خوارزميات وتطبيقات التشفير الأساسية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الوظائف الأمنية للتشفير ٢. خوارزميات التشفير المتماثلة ٣. البيانات الكتلية والبيانات الانسيابية ٤. خوارزميات التشفير غير المتماثلة ٥. إنشاء وإدارة وتبادل وتوزيع المفاتيح ٦. الشهادات الرقمية ٧. دوال الاختزال ٨. التواقيع الرقمية ٩. مقاومة التعارض ١٠. بروتوكولات ومعايير التشفير الشائعة ١١. أنواع الهجمات في التشفير ١٢. الإخفاقات في تنفيذ خوارزميات التشفير ١٣. التشفير باستخدام مفاتيح عامة بدون شهادات رقمية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المكونات الرئيسية لأي نظام تشفير. ٢. التمييز بين خوارزميات التشفير المتماثلة وغير المتماثلة. ٣. اقتراح آلية تشفير مناسبة لمتطلبات وإعدادات معينة. ٤. إظهار استخدامات وقوة كل آلية تشفير والمسائل المتعلقة بتنفيذها. ٥. شرح وظائف الأمن الرئيسية التي يمكن تحقيقها باستخدام التشفير. ٦. توضيح استخدام البنية التحتية للمفاتيح العامة في إجراء التواقيع الرقمية وتشفير البيانات. ٧. تطبيق هجوم جميع الاحتمالات، وهجوم كلمات القاموس، وهجوم حساب التكرار لكسر البيانات المشفرة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

أساسيات الشبكات Basic Networking (BNW)

الوصف	تقدم هذه الوحدة المعرفية مقدمة حول الشبكات وتشمل: العمليات، المكونات، الطبقات، البروتوكولات، الخدمات، التطبيقات، الأدوات، أمن الشبكات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نموذج ISO OSI ونموذج TCP/IP في الشبكات ٢. وسائط الشبكات السلكية والبصرية واللاسلكية ٣. بنى الشبكات وهيكليتها ٤. أنواع الشبكات: PAN، LAN، WAN، DMZ، VLAN، NAT ٥. التقسيمات والتجميعات الشبكية ٦. أجهزة الشبكات الشائعة: الموجهات Routers، المبدلات Switches، جدران الحماية Firewalls ٧. بروتوكولات وخدمات وتطبيقات الشبكات: IP، TCP، UDP، ICMP، SSH، VoIP، HTTP، SMTP، VLAN، NTP، DNS، ونحو ذلك ٨. الأدوات الأساسية لإدارة الشبكات ٩. لمحة شاملة عن المسائل المتعلقة بأمن الشبكات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المفاهيم الأساسية لشبكات البيانات بما فيها المكونات والطبقات والبروتوكولات والخدمات والتطبيقات والأدوات. ٢. اقتراح التصميم والهيكلية للشبكة بناء على سيناريو إعدادات معين. ٣. تحديد مسار حزم البيانات بالنسبة لروابط بسيطة. ٤. تطبيق أدوات الشبكة للتعرف على سير حزم البيانات المترابطة. ٥. إظهار كيفية إجراء التعيينات الشبكية. ٦. توضيح الثغرات الأمنية والتهديدات الشائعة في الشبكات.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

أساسيات البرمجة Basic Scripting and Programming (BSP)

الوصف	تتضمن هذه الوحدة المعرفية المعارف والمهارات المتعلقة بكتابة نصوص برمجية وبرامج بسيطة لتطبيق خوارزميات من أجل حل مسائل معينة باستخدام لغات البرمجة وفق الإرشادات العامة لكتابة برمجيات آمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أساسيات تطوير البرمجيات ٢. مبادئ و ممارسات تصميم البرامج ٣. المتغيرات وأنواع البيانات ٤. الجمل و التعابير البرمجية ٥. العمليات المنطقية الأساسية ٦. القرارات والتفرعات ٧. الحلقات في البرمجة و أنواعها ٨. الوظائف والإجراءات والاستدعاءات ٩. تقنيات اكتشاف ومعالجة الأخطاء البرمجية ١٠. أساسيات تراكيب البيانات والخوارزميات ١١. السلاسل النصية والمصفوفات والسجلات ١٢. التنفيذ المتسلسل والمتوازي ١٣. كتابة النصوص البرمجية في أنظمة ويندوز ولينكس و اعتبارات النظام. ١٤. المفاهيم الأساسية للبرمجة الآمنة: الصلاحيات، فحص الحدود، التحقق من صحة المدخلات، فحص نوع البيانات والتحقق من مدخلات الوحدات البرمجية، معالجة الأخطاء البرمجية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم البرامج البسيطة باستخدام مبادئ وممارسات البرمجة الآمنة. ٢. تطوير وتنفيذ النصوص البرمجية والبرامج باستخدام الشروط والحلقات المركبة من أجل أتمتة مهمات نظام برمجي لحل مشكلة معينة. ٣. تطوير وتنفيذ برامج آمنة وموثوقة مع الأخذ في الاعتبار خصائص بيئات وأنظمة التشغيل.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٦].

الدفاع عن الشبكات Network Defense (NDF)

الوصف	تتضمن هذه الوحدة المعرفية المفاهيم والمهارات والمعرفة والأدوات اللازمة للدفاع عن الشبكات وحمايتها ضد التهديدات السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الهجمات ضد الشبكات ٢. تأمين الشبكات ٣. تقليص الانكشاف وسطح الهجمات ومتجهاتها ٤. الدفاع بعمق ٥. تركيب وتشغيل جدران الحماية ٦. المنطقة والخوادم الوسيطة ٧. الشبكات الخاصة الافتراضية (VPN) ٨. مصائد الهجمات وشبكات مصائد الهجمات ٩. تركيب وتشغيل أنظمة رصد ومنع التسلل ١٠. مراقبة أمن الشبكات ١١. تحليل مرور البيانات في الشبكات ١٢. تصيّد التهديدات ١٣. رصد أنماط الهجمات ١٤. ضبط الوصول في الشبكات ١٥. تطوير وتطبيق سياسات الشبكات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح المفاهيم الرئيسية في الدفاع عن الشبكات. ٢. استخدام أدوات الدفاع عن الشبكات لحمايتها من الثغرات الأمنية والتهديدات والهجمات وللاستجابة للحوادث. ٣. تحليل تنفيذ السياسات الأمنية لحماية الشبكات. ٤. فحص العمليات المتعلقة بالدفاع عن الشبكات.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

مفاهيم نظم التشغيل Operating Systems Concepts (OSC)

الوصف	تتضمن هذه الوحدة المعرفية مقدمة عامة عن الأدوار والوظائف والخدمات الأساسية لنظم التشغيل.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. حالات الصلاحيات الممنوحة وغير الممنوحة ٢. العمليات وإدارة العمليات ٣. حزم التعليمات والتزامن ٤. الجدولة ٥. إدارة الذاكرة ٦. إدارة المدخلات والمخرجات ٧. أنظمة الملفات ٨. البيئات الافتراضية ومشغلات الأجهزة الافتراضية (Hypervisors) ٩. التصميم الآمن في نظم التشغيل: ضبط الوصول، فصل النطاقات، عزل العمليات، تغليف الموارد، منح أدنى الصلاحيات الممكنة ١٠. إدارة الأحداث
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح الأدوار والوظائف والخدمات الأساسية لنظم التشغيل. ٢. إظهار كيفية تعامل نظم التشغيل مع مكونات الأجهزة والتطبيقات البرمجية الأخرى. ٣. شرح مسائل الأمن السيبراني الرئيسية المتعلقة بنظم التشغيل.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

التهديدات السيبرانية Cyber Threats (CTH)

الوصف	تتضمن هذه الوحدة المعرفية المعارف والمهارات الخاصة بالتهديدات والهجمات السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نماذج وأنواع التهديدات السيبرانية ٢. نموذج المهاجم السيبراني: الموارد، القدرات، القصد، الدوافع، كراهية المجازفة، الوصول ٣. أساليب الهجمات: الأبـواب الخلفية، أحصنة طـروادة، الفيروسات، برمجيات الفدية، الهجمات اللاسلكية ، الهندسة الاجتماعية، القنوات السرية ٤. تخمين وكسر كلمة المرور ٥. اعتراض البيانات والانتحال واختطاف الجلسة ٦. تهديدات كشف وتغيير وتخريب البيانات ٧. تهديدات الإنكار للعمليات ٨. هجوم تعطيل الخدمة، والهجوم الموزع لتعطيل الخدمة، وبرمجيات الويب التي تعمل بشكل تلقائي ٩. انتحال عنوان الشبكة المادي MAC، وهجمات تطبيقات الويب، والحوسبة السحابية، والهجمات المستجدة ١٠. التهديدات المستمرة المتقدمة ١١. الوقائع الدالة على حدوث الهجمات السيبرانية وتوقيتها ١٢. أسطح الهجمات ومتجهات الهجمات وأشجار الهجمات ١٣. التهديدات الداخلية ١٤. مصادر معلومات التهديدات السيبرانية ١٥. استراتيجيات وأدوات إعداد نماذج التهديدات السيبرانية ١٦. تهديدات أنظمة التشفير ١٧. المسائل القانونية للتهديدات السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصنيف موارد وقدرات وتقنيات ودوافع المهاجمين. ٢. سرد وشرح ومقارنة أنواع الهجمات السيبرانية. ٣. تمييز وتحديد الوقائع الدالة على حدوث الهجمات السيبرانية. ٤. استخدام أدوات إعداد نماذج التهديدات السيبرانية.

تمـت الاسـتفادة من المصـادر التالية لإعداد محتوى هـذه الوحدة المعرفية: [٢]، [٧].

تخطيط وإدارة الأمن السيبراني Cybersecurity Planning and Management (CPM)

الوصف	تتضمن هذه الوحدة المعرفية المهارات والقدرات الضرورية لتصميم خطط وعمليات الأمن السيبراني للمنظمات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المعارف العامة والشائعة المتعلقة بالتخطيط والإدارة في مجال الأمن السيبراني ٢. التخطيط والإدارة على المستويات العملية والتكتيكية والاستراتيجية ٣. الوظائف التنفيذية العليا ذات العلاقة بالأمن السيبراني ٤. الأمن السيبراني كعنصر أساسي في الاستراتيجيات ٥. استمرارية الأعمال والتعافي من الكوارث ٦. عمليات وإجراءات الاستجابة للحوادث السيبرانية ٧. خطة حماية الملكية الفكرية ٨. إدارة تنفيذ ضوابط الوصول ٩. إدارة التحديثات والإصلاحات وضبط التغيير
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل وظائف أمن الأنظمة ونقاط القوة والضعف فيها. ٢. تصميم وتحضير خطط طوارئ تتضمن استمرارية الأعمال، والتعافي من الكوارث والاستجابة للحوادث السيبرانية. ٣. تصميم خطة إدارة التحديثات والإصلاحات والتغيير، وخطة حماية الملكية الفكرية، وخطة تنفيذ ضوابط الوصول. ٤. تحديد وتوضيح الأدوار والمسؤوليات في تخطيط الأمن السيبراني والإدارة الأمنية.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

السياسات والتشريعات والأخلاقيات والالتزام بها
Policy, Legal, Ethics and Compliance (PLE)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بتشريعات ومعايير ولوائح وإرشادات وسياسات وأخلاقيات الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أفضل الممارسات لأخلاقيات العمل في مجال الأمن السيبراني للمنظمات والأفراد ٢. القضايا المتعلقة بأخلاقيات وممارسات استخدام منصات التواصل الاجتماعي ٣. التشريعات الوطنية والدولية لمكافحة الجرائم السيبرانية ٤. السلطات القضائية والاتفاقات والمعاهدات والمنظمات الدولية ذات العلاقة بالأمن السيبراني ٥. معايير وضوابط الأمن السيبراني الوطنية والدولية (مثلاً: ضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني، PCI DSS، ISO 27001، HIPAA) ٦. تشريعات ولوائح الخصوصية وحماية البيانات (مثلاً: GDPR) ٧. تشريعات ولوائح حماية الملكية الفكرية ٨. الإرشادات وأفضل الممارسات في التوجهات الحديثة (مثلاً: استخدام الأجهزة الشخصية في العمل(BYOD)، إرشادات الحماية لإنترنت الأشياء) ٩. أفضل الممارسات للمواءمة مع تشريعات وضوابط ومعايير الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة القضايا المتعلقة بأخلاقيات وممارسات استخدام التقنية والأمن السيبراني. ٢. مناقشة التشريعات واللوائح والإرشادات والسياسات الرئيسية في مجال الأمن السيبراني. ٣. التعرف على المسائل التشريعية والأخلاقية المهمة عند التعامل مع البيانات. ٤. شرح الممارسات الصحيحة للموائمة مع تشريعات وضوابط ومعايير الأمن السيبراني.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٨].

إدارة البرامج الأمنية Security Program Management (SPM)

الوصف	تقدم هذه الوحدة المعرفية المعارف الضرورية لتصميم وتشغيل وإدارة برامج الأمن السيبراني لحماية المنظمات والدفاع عنها في الفضاء السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أهداف وغايات برامج الأمن السيبراني ٢. قياس الفاعلية ٣. الأدوار والمسؤوليات ٤. السياسات الأمنية ٥. الالتزام بالتشريعات واللوائح المعمول بها ٦. أفضل ممارسات وأطر الأمن السيبراني ٧. وضع خط الأساس للأمن السيبراني ٨. مراقبة وضبط برامج الأمن السيبراني ٩. التوعية والتدريب والتعليم في مجال الأمن السيبراني ١٠. الأمن المادي ١١. أمن الموظفين ١٢. التعرف على الأنظمة والبيانات ١٣. خطط أمن الأنظمة ١٤. إدارة الإعدادات والتحديثات والإصلاحات ١٥. توثيق الأنظمة ١٦. إدارة برامج الاستجابة للحوادث السيبرانية ١٧. إدارة برامج التعافي من الكوارث ١٨. التصديق والاعتماد
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتحضير وإدارة برنامج الأمن السيبراني مع وضع الأهداف والغايات والمقاييس لمنظمة معينة. ٢. قياس الفاعلية لبرنامج معين في الأمن السيبراني.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

تحليل المخاطر السيبرانية Security Risk Analysis (SRA)

الوصف	تتضمن هذه الوحدة المعرفية المعارف والمهارات الخاصة بالنماذج والمنهجيات والعمليات لتقييم المخاطر السيبرانية وإدارتها والتعامل معها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مبادئ ومفاهيم تحليل وإدارة مخاطر الأمن السيبراني ٢. دورة وخطوات إدارة المخاطر ٣. منهجيات تقدير وتحليل المخاطر السيبرانية التحليلية والكمية ٤. منهجيات قياس وتقييم المخاطر السيبرانية ٥. معايير وأطر إدارة المخاطر السيبرانية ٦. عمليات إدارة المخاطر السيبرانية على عدة مستويات في المنظمة ٧. اقتصاديات تخفيف وتقليل المخاطر السيبرانية ٨. نقل وقبول المخاطر السيبرانية والتعامل معها ٩. سياسات التعامل مع المخاطر السيبرانية بالنسبة للتقنيات والأفراد والكيانات. ١٠. خصائص المنظمات التي تؤثر على تحليل وإدارة المخاطر السيبرانية ١١. التواصل فيما يخص المخاطر السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. ربط المخاطر بسياسات الأمن السيبراني. ٢. شرح المنهجيات الرئيسية لإدارة المخاطر السيبرانية. ٣. تقييم وتصنيف المخاطر السيبرانية بالنسبة للتقنيات والأفراد والكيانات. ٤. اختيار المنهجية المناسبة للتعامل مع المخاطر السيبرانية مع الأخذ بعين الاعتبار المزايا والعيوب.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٩].

الخوارزميات المتقدمة Advanced Algorithms (AAL)

الوصف	توفر هذ الوحدة المعرفية المعارف والمهارات اللازمة لتصميم وتطبيق وتحليل الخوارزميات التحسينية والتقريبية المتقدمة من أجل حل مشاكل معينة بطريقة صحيحة وفعالة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. فلاتر بلوم ٢. مصنفات بايز ٣. التطبيق والتبسيط ٤. خوارزميات البرمجة الديناميكية ٥. سلسلة ماركوف مونتي كارلو ٦. الترميز وضغط البيانات ٧. خوارزميات الذكاء الاصطناعي ٨. التدفق الأقصى/ والقص الأدنى وتطبيقاتها ٩. المطابقة المستقرة ١٠. صعوبة المسائل ومجموعة NP ١١. البرمجة الخطية: الخصائص والتطبيقات ١٢. الخوارزميات التقريبية ١٣. الخوارزميات العشوائية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتطبيق وتحليل خوارزميات متقدمة لحل مسائل حقيقية بكفاءة وجودة عالية. ٢. شرح مجموعات صعوبة المسائل P و NP و NP التامة و NP الصعبة. ٣. تطبيق فلاتر بلوم، مصنفات بايز، التطبيق والتبسيط، الترميز وضغط البيانات، وخوارزميات الذكاء الاصطناعي لحل المسائل. ٤. تحليل صعوبة مسألة معينة. ٥. تصميم خوارزميات تقريبية لمسائل NP صعبة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٤].

ضبط الوصول Access Control (ACC)

الوصف	توفر هذه الوحدة المعرفية المعارف بتقنيات ضبط الوصول.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الأمن المادي للبيانات: أمن مركز البيانات، الوصول بمفتاح، بطاقات المفاتيح، كاميرات المراقبة، الأمن على مستوى كبائن الخوادم، إتلاف البيانات ٢. ضبط الوصول الإلكتروني للبيانات: قوائم ضبط الوصول، سياسات المجموعات، كلمات المرور، ضبط الوصول الاحترازي، ضبط الوصول الإجباري، ضبط الوصول بناء على الدور الوظيفي، ضبط الوصول بناء على الخصائص، ضبط الوصول بناء على القواعد، ضبط الوصول بناء على السجلات التاريخية، ضبط الوصول بناء على الهوية، ضبط الوصول بناء على المنظمة، الهويات المتحدة وضبط الوصول ٣. تصميم البنية الآمنة: مبادئ بنية الأمن وحماية المعلومات في أنظمة الحاسب ٤. تقنيات منع تسرب البيانات: التحكم بالحدود والقنوات والوجهات المصرح بها، ومنهجيات مشاركة البيانات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح قوائم ضبط الدخول. ٢. شرح مفاهيم ضبط الوصول المادي والإلكتروني. ٣. توضيح ومقارنة طرق التصريح والتوثيق.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

التشفير المتقدم Advanced Cryptography (ACR)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول خوارزميات التشفير المتقدمة وتطبيقاتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مراجعة لنظرية الأرقام ٢. مراجعة للاحتمالات والإحصاء ٣. خوارزميات AES، RSA، EC ٤. RSA الأساسي والمبطن ٥. خوارزميات التشفير غير العسكرية وغير الحساسة Suite B ٦. أنواع هجمات التشفير: تحليل الفرق، المهاجم في المنتصف، التحليل الخطي ٧. الاختزال والتواقيع ٨. إدارة المفاتيح ٩. الأوضاع والاستخدامات المناسبة ١٠. تحليل التشفير الكلاسيكي ١١. هجمات القنوات الجانبية: التوقيت، استهلاك الطاقة، هجمات تحليل فرق الأخطاء ١٢. التشفير المعتمد على الهوية ١٣. التواقيع الرقمية ١٤. الشبكات الخاصة الافتراضية ١٥. التشفير ما بعد الحوسبة الكمية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح دور وطريقة عمل خوارزميات وبروتوكولات التشفير المتقدمة. ٢. تحليل مستويات الأمن بالنسبة للتشفير. ٣. شرح دور التشفير في التطبيقات الشائعة. ٤. تحليل انتشار الأخطاء عبر أنظمة التشفير. ٥. تحليل قوة الأمن في خوارزميات التشفير. ٦. تطبيق خوارزميات التشفير المتقدمة في سيناريوهات معينة. ٧. إجراء تحليل التشفير الكلاسيكي. ٨. شرح كيفية عمل هجمات القنوات الجانبية وكيفية تجنبها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

الخوارزميات Algorithms (ALG)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات اللازمة لتصميم وتطبيق وتحليل الخوارزميات لحل المسائل الحوسبية بطريقة صحيحة وفعالة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نمو الدوال ٢. تحليل الخوارزميات ٣. خوارزميات البحث ٤. التكرار والاستدعاء الذاتي ٥. خوارزميات الترتيب ٦. خوارزميات الرسومات ٧. خوارزميات "فرق تسد" ٨. الخوارزميات المعتمدة على الطمع ٩. خوارزميات البرمجة الديناميكية ١٠. التعقيد الحوسبي وصعوبة الحل وفئات المسائل الحسابية (NP-Hard، NP ،P، NP-Complete)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح طرق تحليل وتصميم الخوارزميات. ٢. تحليل الخوارزميات وتقييم فعاليتها. ٣. تصميم الخوارزميات لحل المسائل الحوسبية بطريقة صحيحة وفعالة. ٤. تصنيف المسائل الحوسبية حسب صعوبتها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [١٠].

تقنية وبروتوكولات الشبكات المتقدمة
Advanced Network Technology and Protocols (ANT)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول مفاهيم بناء الشبكات المتقدمة والمسائل المعقدة في أمن الشبكات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. خوارزميات وبروتوكولات التوجيه المتقدمة: MPLS، OSPF، BGP ٢. الشبكات المعرّفة بالبرمجيات ٣. شبكات IPv6 ٤. المسائل الأمنية لشبكات IPv6 ٥. جودة الخدمة ٦. خدمات الشبكات ٧. تنفيذ الشبكات الاجتماعية والمسائل الأمنية المتعلقة بها ٨. الهواتف الشبكية ٩. الإرسال متعدد الوجهات ١٠. تأمين أنظمة أسماء النطاقات DNS ١١. ترجمة عناوين الشبكة NAT ١٢. الفحص العميق لحزم البيانات ١٣. أمن طبقة النقل
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح عمل بروتوكولات الشبكات المتقدمة الشائعة. ٢. تحليل أمن بروتوكولات الشبكات المتقدمة. ٣. تشغيل أدوات الشبكة لفحص أداء بروتوكولات الشبكات المتقدمة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

الاتصالات التناظرية Analog Telecommunications (ATC)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة حول أنظمة الاتصالات التناظرية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات إرسال الإشارات ٢. بنى الاتصالات التناظرية ٣. القنوات والمبدلات ٤. درجة الخدمة ٥. الحجب ٦. نماذج وصول المكالمات ٧. مسائل التداخل
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المكونات الرئيسية لأنظمة الاتصالات التناظرية، ورسم تخطيطي لمكونات هذه الأنظمة. ٢. التمييز بين أنواع التضمين وشرح مميزاتها وتطبيقاتها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

الأدوات التحليلية Analytical Tools (ATT)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة للتعرف على الهجمات السيبرانية ومراقبتها وحجبها وتحويلها والاستجابة لها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مقاييس الأداء ٢. تحليل البيانات ٣. استخبارات الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتنفيذ وإدارة استخدام المقاييس لتحديد الفاعلية للبرنامج الأمني بشكل كامل. ٢. استخدام الطرق والتقنيات لتحديد وتقييم المنفعة من مقاييس الأداء. ٣. استخدام التقنيات للتعامل مع كميات كبيرة من البيانات للتعرف على الهجمات السيبرانية وحجبها وتحويلها والاستجابة لها. ٤. جمع وتحليل ونشر المعلومات الأمنية التي تشمل معلومات التهديدات وقدرات العدو ولا تقتصر عليها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

الوعي والفهم Awareness and Understanding (AUU)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المخاطر السيبرانية والممارسات السيبرانية الصحية وتثقيف المستخدمين والتوعية بالثغرات الأمنية والتهديدات السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. إدراك المخاطر السيبرانية والتواصل بشأنها ٢. الممارسات السيبرانية الصحية ٣. تثقيف المستخدمين في الأمن السيبراني ٤. التوعية بالثغرات الأمنية والتهديدات السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح الممارسات السيبرانية الصحية وتثقيف المستخدمين في الأمن السيبراني والتوعية بالثغرات الأمنية والتهديدات السيبرانية. ٢. عرض برامج التثقيف والتدريب والتوعية في الأمن السيبراني (SETA). ٣. شرح المخاطر السيبرانية وإدراكها والتواصل بشأنها في مجال الأمن السيبراني والخصوصية.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

استمرارية الأعمال، والتعافي من الكوارث، وإدارة الحوادث السيبرانية
Business Continuity, Disaster Recovery and Incident Management (BDR)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول استمرارية الأعمال والتعافي من الكوارث وتقنيات إدارة الحوادث السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الاستجابة للحوادث: التنبؤ بها واكتشافها والتخفيف من أضرارها ٢. التعافي من الكوارث: خطط التعافي من الكوارث ٣. استمرارية الأعمال: التخطيط للطوارئ، الاستجابة للحوادث، الاستجابة للطوارئ، النسخ الاحتياطية، التعافي
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح معنى الصمود، وتحديد البيئات التي تظهر فيها أهميته. ٢. مناقشة أساسيات خطط استمرارية الأعمال وخطط التعافي من الكوارث. ٣. إعداد خطط واقعية أو مبنية على حالة معينة للتعافي من الكوارث واستمرارية الأعمال. ٤. شرح المخاطر الأمنية المحتملة التي بالإمكان أن تنتج عن النسخ الاحتياطية.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

الحوسبة السحابية Cloud Computing (CCO)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة حول تقنيات الحوسبة السحابية وخدامتها ونماذجها وأمنها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منصات البيئات الافتراضية ٢. الخدمات السحابية: SaaS، PaaS، DaaS، IaaS ٣. مشغلات الأجهزة الافتراضية (Hypervisors) وتنفيذ الحوسبة السحابية ٤. البنى الموجهة نحو الخدمة ٥. نماذج تنصيب الخدمة: خاص، عام، مجتمعي، هجين ٦. أمن السحابة الحوسبية ٧. التخزين ٨. المسائل التشريعية ومسائل الخصوصية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح خدمات الحوسبة السحابية. ٢. مناقشة مزايا وعيوب البيئات الافتراضية. ٣. تنصيب تطبيقات سحابية. ٤. تخصيص موارد للمستخدمين والتطبيقات بكفاءة. ٥. مناقشة أهمية إدارة الموارد في الحوسبة السحابية. ٦. شرح المتطلبات للبيئات السحابية الآمنة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٤].

الجريمة السيبرانية Cyber Crime (CCR)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة عن الجرائم السيبرانية والانتهاكات في الفضاء السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنواع الجرائم السيبرانية: التسلل، برامج الفدية، التنصت، انتهاك الملكية الفكرية، الاحتيال، الابتزاز، تعطيل الخدمات، تسريب البيانات أو إتلافها أو تعديلها ٢. المطاردة والتصيّد في الفضاء السيبراني ٣. التنمر السيبراني ٤. انتحال الهوية ٥. ارتكاب الجرائم من خلال الفضاء السيبراني ٦. الإرهاب السيبراني ٧. تشريعات مكافحة الجرائم السيبرانية: التشريعات الوطنية، التشريعات الدولية، الاتفاقيات الدولية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح الجرائم السيبرانية المحتملة والمطاردة السيبرانية والتنمر السيبراني وغيرها من السلوكيات المسيئة في الفضاء السيبراني. ٢. استخدام تطبيقات الأمن السيبراني للدفاع ضد الجرائم والانتهاكات.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [١١].

مشتريات المكونات Component Procurement (CPP)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول جوانب الأمن السيبراني خلال عمليات المشتريات وأمن المكونات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مخاطر سلاسل الإمداد ٢. أمن سلاسل الإمداد ٣. الفحص الأمني للمورّدين
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف التهديدات والمخاطر الأمنية للأجهزة والبرمجيات عند شراء مكونات الأنظمة. ٢. كشف الاختراقات في أمن مكونات الأجهزة والبرمجيات ومنع حدوثها. ٣. إيجاد موردين وناقلين موثوقين لمكونات الأنظمة.

تمـت الاسـتفادة من المصـادر التالية لإعداد محتوى هـذه الوحدة المعرفية: [٣].

أخلاقيات الأمن السيبراني Cybersecurity Ethics (CSE)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بالمسائل الأخلاقية في مجال الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المحافظة على الخصوصية وسرية المعلومات عند تأدية أعمال الأمن السيبراني ٢. حماية حقوق المستخدمين عند تأدية أعمال الأمن السيبراني ٣. المواثيق والأطر ذات العلاقة بأخلاقيات الأمن السيبراني ٤. الجوانب الأخلاقية في حماية الأنظمة والشبكات الحساسة ذات الأثر والأهمية على المجتمع والأفراد ٥. التوازن بين حماية الأنظمة والشبكات وتمكين الاستفادة منها ٦. المسؤولية الوطنية والاجتماعية في أعمال الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المواضيع الأساسية في أخلاقيات الأمن السيبراني. ٢. ممارسة أعمال الأمن السيبراني مع الالتزام بالجوانب الأخلاقية المتعلقة به.

قواعد البيانات Databases (DAT)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لإدارة أنظمة قواعد البيانات واستخدامها وحمايتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنواع أنظمة إدارة قواعد البيانات: علاقاتية، هرمية، غير علاقاتية (NoSQL)، قائمة على الكائنات (Object-Based)، موجهة للكائنات (Object-Oriented)، موزعة ٢. نماذج أمن قواعد البيانات: الاستدلال، التجميع، الحقن، الاختزال، التشفير، تلف البيانات، الوصول غير المصرّح به، ضوابط الوصول إلى قواعد البيانات (Clark-Wilson، RBAC، MAC، DAC)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مقارنة نماذج قواعد البيانات وتنفيذ متطلبات قواعد بيانات باستخدام نموذج معين. ٢. توضيح الجوانب الأمنية المتعلقة بقواعد البيانات وأنظمة إدارة قواعد البيانات.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

إدارة البيانات Data Administration (DBA)

الوصف	تقدم هذه الوحدة المعرفية معارف عامة عن دورة حياة البيانات وجودتها وأمنها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. دورة حياة البيانات: الحصول على البيانات وصونها وتحويلها واستخدامها وتوزيعها وأرشفتها وتنقيتها ٢. جودة البيانات: الدقة والاكتمال والصلة والاتساق والسلامة والتنقية والتحقق والتأكد من الصحة ٣. سهولة الوصول إلى البيانات ٤. منفعة البيانات ٥. تخزين وأرشفة البيانات: تخزين البيانات، الأرشفة طويلة الأمد والبيانات الضخمة ٦. أنظمة إدارة البيانات (مثل HBASE، MongoDB، Hadoop) ٧. ضوابط البيانات: الملكية، الإشراف، الإدارة، الحيازة، الحوكمة ٨. سياسات البيانات: السياسات الداخلية والخارجية ٩. أمن البيانات: ضبط الوصول وتصنيف البيانات والتشفير
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح مراحل دورة حياة البيانات ومناقشة المسائل الأمنية ذات العلاقة. ٢. تحليل جودة البيانات وسهولة الوصول إليها ومنفعتها. ٣. إدارة إنشاء البيانات وتغييرها وتوزيعها وتخزينها وحذفها بطريقة آمنة. ٤. مناقشة وشرح ملكية البيانات والإشراف عليها وإدارتها وحيازتها وحوكمتها. ٥. توضيح أهمية تصنيف البيانات في الأمن السيبراني.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

الاتصالات الرقمية Digital Communications (DCO)

الوصف	تقدم هـذه الوحدة المعرفية المعارف بأنظمة الاتـصـالات الرقمية والبروتوكولات ذات العلاقة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مكونات نظام الاتصالات الرقمية ٢. طرق الترميز ٣. إرسال الإشارات الرقمية ٤. إشارات الانتشار الطيفي ٥. الوصول إلى قنوات الاتصال متعددة المستخدمين: TDMA، CDMA، FDMA ،SDMA ،PDMA
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح أنظمة الاتصالات الرقمية والأنظمة الفرعية والتضمينات. ٢. عرض أحدث منهجيات الاتصالات الرقمية. ٣. التمييز بين نماذج الاتصالات الرقمية المختلفة ومناقشة الإيجابيات والسلبيات لكل منها.

تمـت الاسـتفادة من المصـادر التالية لإعداد محتوى هـذه الوحدة المعرفية: [٢].

التحقيق الجنائي الرقمي Digital Forensics (DFS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بتقنيات التحقيق الجنائي الرقمي والمهارات؛ لتطبيقها في أعمال البحث والتحقيق بطريقة تراعي المتطلبات التشريعية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مصطلحات التحقيقات الجنائية الرقمية ٢. الامتثال للتشريعات: التشريعات المعمول بها، الإقرارات، الشهادات، الحالات السابقة ٣. عمليات البحث والتحقيق السيبرانية ٤. الحصول على الأدلة وحفظها: حظر الكتابة، إجراءات التصوير، التحقيق الجنائي الرقمي الحي، تحليل الأدلة وتوثيقها ٥. تحليل الأدلة: تحليل السبب الجذري، البيانات الوصفية وإعادة تجميع الملفات ٦. تسجيل النتائج وتقديمها: الجدول الزمني والمسببات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. حلّ مشكلة تحقيق سيبرانية معينة باستخدام تقنيات وأدوات التحقيقات الجنائية الرقمية. ٢. توضيح المسائل التشريعية والتنظيمية المتعلقة بالتحقيقات الجنائية الرقمية وعمليات البحث والتحري وفق الأنظمة واللوائح والتعليمات والقرارات المرعية في المملكة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣]

سلامة البيانات وتوثيقها Data Integrity and Authentication (DIA)

الوصف	توفر هذه الوحدة المعرفية المعارف حول تقنيات سلامة البيانات وتوثيقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. قوة التوثيق: التوثيق بعوامل متعددة، التوثيق باستخدام الأداة المشفرة، الأجهزة المشفرة، التوثيق بالقياسات الحيوية، كلمات المرور لمرة واحدة، والتوثيق القائم على المعرفة ٢. تقنيات هجمات كلمات المرور: الهجوم بالقاموس، الهجوم بجميع الاحتمالات، الهجوم بجداول قوس المطر، التصيد الإلكتروني، الهندسة الاجتماعية، الهجوم باستخدام البرمجيات الضارة، التجسس، التحليل بدون اتصال، أدوات كسر كلمة المرور ٣. تقنيات تخزين كلمات المرور: دوال الاختزال في التشفير، مقاومة التعارض، إضافة بيانات عشوائية، عداد التكرار، اشتقاق المفتاح القائم على كلمة المرور ٤. سلامة البيانات: رموز توثيق الرسائل (HMAC ،CBC-MAC)، التواقيع الرقمية، التشفير والتوثيق، وأشجار الاختزال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المفاهيم الأساسية في التوثيق والتصريح وضبط الوصول وسلامة البيانات. ٢. توضيح نقاط القوة والضعف في تقنيات التوثيق. ٣. عرض الهجمات الشائعة على كلمات المرور.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

التعلّم العميق Deep Learning (DLL)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات اللازمة لتطوير وتطبيق الشبكات العصبية الاصطناعية الحديثة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الشبكات العصبية الاصطناعية: التصنيف الثنائي، الانحدار اللوجستي، دالة تكلفة الانحدار اللوجستي، النزول المتدرج، المشتقات، حوسبة الرسومات، حوسبة المتجهات ٢. الشبكات العصبية الاصطناعية الضحلة: تمثيل الشبكات العصبية الاصطناعية، دوال التنشيط، دوال التنشيط غير الخطية، مشتقات دوال التنشيط، النزول المتدرج، الانتشار الأمامي، الانتشار العكسي وحوسبة الرسومات ٣. الشبكات العصبية الاصطناعية الالتفافية: الشبكات الكلاسيكية والشبكات العصبية المتكررة ودوال الخسارة والتحسين ٤. التعلم العميق بدون إشراف ٥. التعلم المعزز العميق ٦. شبكات الأعداء التوليدية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح أساسيات التعلّم العميق وبنى الشبكات العميقة. ٢. تحديد شبكات التعلّم العميق وتدريبها، واستخدامها لحل المشاكل. ٣. مناقشة المسائل المفتوحة والشائعة في أبحاث التعلّم العميق.

أنظمة إدارة قواعد البيانات Database Management Systems (DMS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المفاهيم الأساسية لأنظمة إدارة قواعد البيانات بالإضافة إلى المهارات والقدرات اللازمة لاستخدام أنظمة إدارة قواعد البيانات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنواع قواعد البيانات: المسطحة، العلاقاتية، الشبكية، الهرمية، القائمة على الكائنات (Object-Based)، الموجهة للكائنات (Object-Oriented)، المبنية على قيم المفاتيح، الموزعة ٢. التعامل مع البيانات من خلال لغة الاستعلام الهيكلية(SQL): SELECT ،INSERT ،DELETE ،UPDATE ٣. تعريف البيانات في لغة SQL ٤. إدارة قواعد البيانات بلغة SQL: إنشاء وحذف المستخدمين والصلاحيات وضبط الوصول ٥. مفاهيم قواعد البيانات: الفهرسة والاستدلال والتجميع والتمثيل المتعدد ٦. أمن قواعد البينات وحمايتها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز بين نماذج قواعد البيانات. ٢. التمييز بين أدوار قواعد البيانات، وأنظمة إدارة قواعد البيانات وخوادم قواعد البيانات. ٣. إنشاء قواعد البيانات وإدارتها وتشغيلها. ٤. إدارة ضوابط الوصول ومستويات الصلاحيات في أنظمة إدارة قواعد البيانات. ٥. رسم الهياكل لتخزين البيانات في أنظمة إدارة قواعد البيانات. ٦. تصميم قواعد البيانات وتنفيذها لتطبيق معين.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

بنية الأنظمة الموزعة Distributed Systems Architecture (DSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الأنظمة الموزعة وكيفية الاتصال فيما بينها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المفاهيم العامة للأنظمة الموزعة ٢. أمثلة على الأنظمة الموزعة ٣. البروتوكولات والطبقات ٤. حوسبة الأداء العالي ٥. مشغلات الأجهزة الافتراضية (Hypervisors) وتنفيذ الحوسبة السحابية ٦. الثغرات الأمنية وأمثلة على استغلالها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف مكونات وواجهات معيار شبكي معين. ٢. شرح عملية في أحد نظم التشغيل وتقديم بنى متعددة لتشغيل العمليات وتمكين الاتصال فيما بينها. ٣. وصف الحوسبة عالية الأداء وحالات الاستخدام التي تميّزها عن الإنترنت الاعتيادية. ٤. فحص أسطح الهجمات لنماذج الحوسبة الموزعة المتعددة مع التأكيد على أن كل واجهة تقدم مجموعة من الثغرات الأمنية المحتملة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

تراكيب البيانات Data Structures (DST)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول أنـواع البيانات المجردة والعمليات الأساسية للتعامل معها، بالإضافة للمهارات اللازمة لتطبيقها لحلّ المسائل.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. البيانات العددية ٢. السلاسل النصية ٣. القوائم: قائمة متصلة، قائمة مزدوجة الاتصال، وجداول الاختزال ٤. المصفوفات ٥. المتجهات ٦. الأكوام ٧. الصفوف ٨. الأكداس ٩. المخزنات المؤقتة ١٠. الأشجار ١١. الكائنات ١٢. بنية البيانات في لغات البرمجة ١٣. الفئات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تنفيذ أنواع البيانات المجردة الشائعة. ٢. استخدام أنواع بيانات مجردة معينة وعملياتها من أجل تنفيذ حلول لمسائل معينة. ٣. التفريق بين مختلف تراكيب البيانات واستخداماتها ومميزاتها وعيوبها. ٤. تصميم مواصفات لتراكيب بيانات مطلوبة بناءً على احتياجات معينة. ٥. توضيح مفهوم التجريد والتعرف على حـالات الإخـلال بالتجريد لمواصفات تراكيب بيانات معينة.

تمـت الاسـتفادة من المصـادر التالية لإعداد محتوى هـذه الوحدة المعرفية: [٢].

التحقيق الجنائي الرقمي في الأجهزة Device Forensics (DVF)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات لتطبيق تقنيات التحقيق الجنائي الرقمي في فحص الأجهزة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تحليل أجهزة الهاتف الجوال: الأجهزة الذكية واللوحية ٢. الأنظمة المدمجة: نظام تحديد المواقع العالمي (GPS) ولوحات تشغيل الألعاب وأجهزة التلفاز الذكية ٣. أجهزة إنترنت الأشياء
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق تقنيات وأنشطة التحقيق الجنائي الرقمي على أجهزة الهاتف الجوال والأنظمة المدمجة وأجهزة إنترنت الأشياء. ٢. مناقشة الجوانب التشريعية المرتبطة بعمليات التحقيقات الجنائية الرقمية على أجهزة الهاتف الجوال والنظم المدمجة وأجهزة إنترنت الأشياء.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

الأنظمة المدمجة وإنترنت الأشياء
Embedded Systems and Internet of Things (ESI)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الأنظمة المدمجة وإنترنت الأشياء والمسائل الأمنية المتعلقة بها، بالإضافة للمهارات والقدرات اللازمة لتصميم مكونات الأنظمة المدمجة وإنترنت الأشياء وبرمجتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. استخدامات وتطبيقات الأنظمة المدمجة وإنترنت الأشياء ٢. المكونات الأساسية للأنظمة المدمجة وإنترنت الأشياء من أجهزة وبرمجيات ٣. الاتصالات والشبكات بين أجهزة الأنظمة المدمجة وإنترنت الأشياء ٤. معالجة المقاطعات ومسائل التوقيت وإدارة الموارد في الأنظمة المدمجة وإنترنت الأشياء ٥. نظم التشغيل للأنظمة المدمجة وإنترنت الأشياء ٦. برمجة الأنظمة المدمجة وإنترنت الأشياء ٧. المسائل الأمنية في الأنظمة المدمجة وإنترنت الأشياء
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف مكونات وتطبيقات الأنظمة المدمجة وإنترنت الأشياء. ٢. شرح الجوانب الخاصة بنظم التشغيل والشبكات والاتصالات في الأنظمة المدمجة وإنترنت الأشياء. ٣. تصميم مكونات الأنظمة المدمجة وإنترنت الأشياء وبرمجتها.

المحاسبة الجنائية الرقمية Forensic Accounting (FAC)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول تقنيات التحقيق الجنائي الرقمي للبحث والتحري المالي، والمهارات والقدرات اللازمة لتطبيقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المحاسبة الاستقصائية ٢. الإبلاغ عن عمليات الاحتيال المالي ٣. اختلاس الأصول ٤. الأساليب غير المباشرة لإعادة بناء الدخل ٥. غسيل الأموال ٦. التدفقات المالية الدولية ٧. خدمات التقاضي ٨. إدارة الأدلة ٩. الأضرار الاقتصادية وتقييم الأعمال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف التلاعبات الشائعة في القوائم المالية وطرق اكتشافها. ٢. تقدير الإيرادات والدخل المخفي. ٣. توضيح طرق غسيل الأموال وطرق اكتشافها ومنعها. ٤. تقييم خسائر عمليات الاحتيال والسرقات والأضرار الناجمة عنها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

الأساليب المنهجية Formal Methods (FMD)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المنطق الرياضي والمهارات اللازمة لتطبيقها في تصميم الأنظمة الآمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مفهوم الأساليب المنهجية ٢. المنطق الرياضي ٣. دور الأساليب المنهجية في تصميم الأنظمة وهندسة البرمجيات ٤. حدود إمكانيات الأساليب المنهجية ٥. ضوابط الوصول الإلزامية Bell-LaPadula ٦. أدوات الاستنتاج المؤتمتة ٧. نمذجة الأنظمة ومواصفاتها ٨. البراهين ٩. فحص النماذج والبحث عنها ١٠. لغات تأكيد البرامج
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق الأساليب المنهجية في أوضاع حقيقية. ٢. توضيح قيمة الأساليب المنهجية وتقنيات التحليل بالمقارنة مع الاختبارات في التحقق والتأكد من صحة البرمجيات. ٣. تطبيق الأساليب المنهجية على تصاميم البرمجيات. ٤. شرح مزايا وعيوب لغات المواصفات المنهجية. ٥. تحليل أمن البرمجيات والأنظمة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٤].

منع الاحتيال وإدارة الحد منه Fraud Prevention and Management (FPM)

الوصف	تقدم هذه الوحدة المعرفية المعارف والقدرات لتصميم الخطط والعمليات لمنع الاحتيال والتخفيف من أضراره.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مقدمة عن الاحتيال والمصطلحات المتعلقة به ٢. التدقيق ومنع الاحتيال: المنهج العلمي وقانون بينفورد ٣. التعامل مع البيانات: جمع البيانات وتنظيفها والتحقق منها وتطبيعها ٤. فهم البيانات: التحليل والرسم البياني والترتيب والفهرسة والتلخيص والتنظيم ٥. الاختبارات الرقمية للاحتيال: القيم المستخدمة بشكل متكرر، المقادير المتساوية، التقريب، تحليل النسبة/التباين، اختبار القيم المتطرفة، الاختبارات الإحصائية، اختبارات العشوائية ٦. نمذجة الاحتيال: طرق تعلم الآلة للكشف عن الاحتيال ٧. الكشف المتقدم للاحتيال ومنعه
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تقييم تكلفة وفاعلية منهجيات كشف الاحتيال ومنعه. ٢. شرح المسائل التشريعية والأخلاقية المتعلقة بالكشف عن الاحتيال ومنعه. ٣. تطبيق أدوات وتقنيات الكشف عن الاحتيال ومنعه.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

بنية الأجهزة والعتاد Hardware Architecture (HAA)

الوصف	تتضمن هذه الوحدة المعرفية مقدمة عن مزايا معايير بنى الأجهزة والعتاد (Hardware) والثغرات الأمنية المحتملة فيها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. البنى المعيارية ٢. معايير واجهة الأجهزة والعتاد (Hardware) ٣. البنى الشائعة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. فهم فكرة البنى المعيارية ومزايا المعايير الموحدة. ٢. وصف المعايير المختلفة لواجهات الأجهزة والعتاد ابتداءً من تصميم حزم الدوائر المدمجة ومروراً بالناقلات (مثل ISA، PCI) لمنصات الربط، وانتهاءً بمعايير الشبكات مثل معيار IEEE 802.3.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

أمن الأجهزة والعتاد والبرمجيات الثابتة Hardware/Firmware Security (HFS)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتصلة بمكونات الأجهزة والعتاد والبرمجيات الثابتة والمسائل الأمنية المتعلقة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الثغرات المادية: قنوات اتصال غير مستخدمة وغير آمنة، منصات الاختبار، مسارات الاختبار، الأبواب الخلفية، أحصنة طروادة، الدارات الخفية، إضافة الشوائب إلى أشباه الموصلات، الأعطال المستحثة، الهندسة العكسية، الوصول غير المصرح به إلى الذاكرة ٢. هجمات القنوات الجانبية على الأجهزة والعتاد: التوقيت، تحليل الطاقة، الكهرومغناطيسية، تحليل الترددات اللاسلكية، إضافة عتاد، القنوات خارج النطاق ٣. هجمات المصدر: الأجزاء المزيفة والمقلدة والمقرصنة وتعطيل سلاسل التوريد ٤. هجمات تدمير الأجهزة ٥. مكونات أمن الأجهزة: هويات الأجهزة القابلة للتحقق، مولدات الأرقام العشوائية، التواقيع الرقمية لتشغيل ذاكرة القراءة فقط، وحدات التشفير المبنية على العتاد، أجهزة التحكم الأمنية/المعالجات المساعدة ومسرعات التشفير ٦. سمات الأمن المادي: التأكد من صحة الجهاز، الخوارزميات الأمنية المقبولة/المفتوحة، توليد الأرقام العشوائية القوية، مصدر التوقيت الآمن، واجهة المطور المعيارية، التوثيق الواضح، النسخ الاحتياطية للمفاتيح وحمايتها، المقاومة ضد التلاعب، قابلية التوسع ٧. ثغرات محمّل التشغيل: هجمات قطاع التشغيل، وضع المستخدم المنفرد، التشغيل لنظم تشغيل غير آمنة، إعادة إعداد محمل التشغيل ٨. الثغرات الأمنية في الرموز المصغرة ٩. ثغرات البرمجيات الثابتة: إعادة تحميل BIOS/PROMs ١٠. الدور الأمني للطبقات الوسيطة: طبقة تجريد الأجهزة والعتاد وطبقات البيئات الافتراضية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح الثغرات الأمنية الرئيسية في الأجهزة والعتاد. ٢. استخدام قدرات أمن الأجهزة والعتاد. ٣. شرح تهيئة الأنظمة وتحميل البرمجيات والتأكد من صحتها. ٤. مناقشة الدور الأمني لطبقات تجريد الأجهزة والعتاد.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

التحقيق الجنائي الرقمي للمضيف Host Forensics (HOF)

الوصف	تقدم هذه الوحدة المعرفية القدرات والمهارات اللازمة للبحث والتحقيق في مضيف شبكة باستخدام طرق التحقيقات الجنائية الرقمية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنظمة الملفات والتحقيق الجنائي الرقمي لأنظمة الملفات ٢. تحليل مشغلات الأجهزة الافتراضية (Hypervisors) ٣. تحليل التشفير ٤. جداول قوس المطر ٥. فلترة الملفات المعروفة ٦. إخفاء المعلومات ٧. إعادة تجميع الملفات ٨. تحقيقات النظام الحي ٩. تحليل الجدول الزمني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحديد البيانات القابلة للاسترداد من بيئات أنظمة تشغيل متعددة. ٢. عرض منهجيات التحقيق الجنائي الرقمي للمضيف.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

الهندسة العكسية للأجهزة والعتاد Hardware Reverse Engineering (HRE)

الوصف	تقدم هذه الوحدة المعرفية المعارف والقدرات والمهارات لتحديد وظيفة مكونات عتاد معينة ومدخلاتها ومخرجاتها وبياناتها المخزنة باستخدام إجراءات وطرق الهندسة العكسية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أساسيات الهندسة العكسية ٢. المحفزات، جمع البيانات، تحليل البيانات ٣. تطوير المواصفات ٤. تحسين القدرات وأساليب التعديل ٥. اكتشاف التعديل ٦. منهجيات التحفيز وقياس الأجهزة ٧. معايير JTAG IEEE 1149.1 ٨. تعريف الواجهات وتعدادها ٩. التفكيك إلى مكونات بناء على الوظائف
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض طرق الهندسة العكسية للعتاد. ٢. تطبيق عملية التقاط البيانات وقياسها وجمعها من أجل تحديد وظيفة مكون عتاد معطى.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

بنى توكيد المعلومات Information Assurance Architectures (IAA)

الوصف	تقدم هذه الوحدة المعرفية المعارف بالبنى الأمنية المستخدمة لحماية أنظمة المعلومات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الدفاع بعمق ٢. المناطق الوسيطة المعزولة (DMZs) ٣. الخوادم الوسيطة ٤. التكوين والأمن ٥. التوالي ٦. الخصائص الناشئة ٧. التبعيات ٨. مجموعات TCB الفرعية ٩. البنى المؤسسية والبنى الأمنية ١٠. تصميم الشبكة الآمنة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز والربط بين مراحل ومكونات بنية توكيد المعلومات. ٢. إظهار المعرفة بقدرات المنهجيات الحالية وحدودها من أجل تقييم حلول بنى تأمين المعلومات وتخطيطها وتنفيذها والحفاظ عليها. ٣. فحص الثغرات الأمنية المحتملة لبنية معينة. ٤. تصميم بنى توكيد المعلومات لتطبيقات معينة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

الالتزام بتوكيد المعلومات Information Assurance Compliance (IAC)

الوصف	توفر هذه الوحدة المعرفية المعارف بالقواعد واللوائح والمسائل المتعلقة بالتدقيق والالتزام بالتشريعات واللوائح المعمول بها في الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. العلاقة بين الالتزام والتدقيق ٢. أنواع التدقيق: داخلي وخارجي ٣. أغراض التدقيق: المتطلبات، المواصفات، السياسة، المعايير، التشريعات، الضوابط التنظيمية والداخلية ٤. عملية التدقيق: الميثاق، خط الأساس، الأنشطة، إعداد التقارير، النتائج، التوصيات، الاستجابة، استراتيجية تقليل جوانب القصور ٥. مراقبة الالتزام ٦. التدريب على الالتزام
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز بين متطلبات الالتزام الإلزامية والاختيارية. ٢. تصميم وتخطيط وإجراء عمليات التدقيق لفحص الالتزام.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

معايير توكيد المعلومات Information Assurance Standards (IAS)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتصلة بالمعايير المتعلقة بتوكيد المعلومات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المعايير الوطنية ذات العلاقة بالأمن السيبراني ٢. اللوائح التنظيمية والمعايير الدولية ذات العلاقة بالأمن السيبراني (مثل NIST) ٣. المعايير التجارية (مثل PCI/DSS) ٤. المعايير المفتوحة (مثل OWSAP)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مقارنة أنواع مختلفة من التشريعات واللوائح التنظيمية والسياسات والأطر والمعايير الوطنية والدولية. ٢. شرح تأثير المعايير على أنظمة معينة. ٣. توضيح تأثير المعايير على المقاولين الفرعيين والعملاء. ٤. سرد أحكام المعايير الرئيسية وشرحها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

أنظمة التحكم الصناعية Industrial Control Systems (ICS)

الوصف	توفر هذه الوحدة المعرفية المعارف بأنظمة التحكم الصناعية إلى جانب الثغرات الأمنية التي ترتبط بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مكونات الأجهزة والعتاد لأنظمة التحكم الصناعية ٢. منطق السلم ٣. أجهزة التحكم المنطقي القابلة للبرمجة ٤. برتوكولات (ICCP، OPC، DNP3، PROFINET، MODBUS، SERIAL) ٥. ربط الشبكات (Bluetooth، 900MHz، ZIGBEE، RS232/485، X.25) ٦. أنواع أنظمة التحكم الصناعية (مثل أنظمة توزيع الطاقة، التصنيع) ٧. نماذج أنظمة التحكم الصناعية (المستندة إلى الوقت مقابل المستندة إلى الأحداث) ٨. الثغرات الأمنية الشائعة في أنظمة البنى التحتية الحساسة ٩. مكونات أمن نظام التحكم الإشرافي وتحصيل البيانات(SCADA)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف تطبيقات أجهزة التحكم المنطقي القابلة للبرمجة من أجل الأتمتة. ٢. سرد وشرح ومناقشة مكونات وتطبيقات أنظمة التحكم الصناعية. ٣. وصف طرق التحكم والتمييز بينها. ٤. تنفيذ وتقييم الوظائف الأمنية داخل شبكة صناعية. ٥. عرض بروتوكولات أنظمة التحكم الصناعية الشائعة والمقارنة بينها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

بحث موجه/ دراسة مستقلة Independent/Directed Study/Research (IDR)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتصلة بالمواضيع الحديثة والناشئة في مجال الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التقنيات الناشئة إلى جانب المسائل الأمنية ذات العلاقة ٢. الأدوات والأساليب والمنهجيات الناشئة المتعلقة بالأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة التقنيات المتقدمة الحديثة والناشئة إلى جانب المسائل الأمنية ذات العلاقة. ٢. تطبيق وعرض ومناقشة استخدام الأدوات والأساليب والمنهجيات المتقدمة الحديثة والناشئة في الأمن السيبراني.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

أنظمة كشف/منع التسلل Intrusion Detection/Prevention Systems (IDS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المنهجيات والأساليب لاكتشاف وتحليل الثغرات الأمنية والتهديدات، بالإضافة للمهارات اللازمة لاستخدامها للتخفيف من أضرار المخاطر المصاحبة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الفحص العميق لحِزَم البيانات ٢. تحليل ملفات السجلات ٣. دمج السجلات ٤. المقارنة والتحليل المتبادَلَيْن للسجلات ٥. كشف الأداء الشاذ للشبكة: إنشاء ملف التعريف الشخصي والخوارزميات الشاذة والمنهجيات الإحصائية وأساليب الارتباط ومنهجيات المنطق الضبابي والذكاء الاصطناعي وخوارزميات الترشيح والشبكات العصبية ٦. كشف إساءة الاستخدام: كشف التوقيع ٧. الكشف القائم على المواصفات ٨. كشف ومنع التسلل القائم على الأنظمة المضيفة ٩. كشف ومنع التسلل القائم على الشبكة: وضع التخفّي ١٠. كشف التسلل الموزَّع ١١. أنظمة كشف التسلل الهرمية ١٢. مصائد الهجمات وشبكات مصائد الهجمات ١٣. الاستجابة للتسلل: إعادة تهيئة الجهاز، الإخطارات، التسجيل، مصيدة SNMP، البريد الإلكتروني، الإنذار المرئي/الصوتي، تسجيل التتبّع، تطبيق الافتتاح، انقطاع الجلسة، مقاطعة الجلسة، إعادة الاتصال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. كشف حالات التسلل إلى المضيف والشبكة والاستجابة لها. ٢. تطبيق أدوات الكشف عن البرامج الضارة والأجهزة غير المصرح بها على الشبكة. ٣. تصميم الإجراءات التصحيحية للاستجابة لحالات التسلل المكتشفة. ٤. إعداد وتركيب وتهيئة نظام كشف/منع التسلل، وتحسين أدائها ودقتها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

إدارة الهوية Identity Management (IMM)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق إدارة الهوية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التعرف والتوثيق: الأشخاص والأجهزة، ضبط الوصول للشبكة، إدارة الهوية والوصول، الأدوار، الأنظمة متعددة المنهجيات للتعرف والتوثيق، أنظمة التوثيق المعتمدة على الخصائص الحيوية، الدقة / معدل قبول الخطأ / معدل رفض الخطأ، المقاومة، الخصوصية، سهولة الاستخدام وقابلية التساهل للمنهجيات ٢. ضوابط الأصول المادية والمنطقية: أجهزة الأنظمة، أصول الشبكات، أجهزة النسخ الاحتياطي/التخزين، ضوابط الوصول القائمة على القواعد، ضوابط الوصول القائمة على الدور الوظيفي، منهجيات تتبع المخزون، ومنهجيات إنشاء الهوية ٣. الهوية كخدمة ٤. خدمات هوية الأطراف الخارجية ٥. الهجمات ضد ضبط الوصول وطرق مواجهتها: هجمات كلمة المرور، هجمات تعتمد على القاموس، هجمات جميع الاحتمالات وهجمات انتحال الشخصية/ البريد الإلكتروني، التحقق من الهوية متعدد العوامل، سياسة كلمة المرور القوية، ملفات كلمة المرور الآمنة، والوصول المحدود إلى الأنظمة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز بين المفاهيم التالية: 'تحديد الهوية' و 'التوثيق' و 'تصريح الدخول'. ٢. مناقشة مسارات التدقيق وأهمية حفظ السجلات في تحديد الهوية والتوثيق. ٣. تطبيق مفاهيم أدنى الصلاحيات وفصل المهام والمسؤوليات. ٤. شرح الهجمات ضد ضبط الوصول ومناقشة طرق مواجهتها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

أمن تخزين المعلومات Information Storage Security (ISS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق تأمين تخزين المعلومات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تشفير الأقراص والملفات: تشفير الأجهزة مقابل تشفير البرمجيات ٢. محو البيانات: الاستبدال، إزالة المغنطة، طرق الإتلاف المادي والبقايا العالقة في ذاكرة التخزين ٣. قناع البيانات: لأجل الاختبار والتعتيم والخصوصية ٤. أمن قاعدة البيانات: الوصول، التوثيق، التدقيق، نماذج تكامل التطبيقات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح تشفير الأقراص والملفات باستخدام العتاد والبرمجيات. ٢. شرح أساليب محو البيانات. ٣. شرح تطبيقات تقنيع البيانات. ٤. مناقشة الوصول إلى قاعدة البيانات والتوثيق والتدقيق وتكامل التطبيقات.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

مقدمة في نظرية الحوسبة Introduction to the Theory of Computation (ITC)

الوصف	تقدم هذه الوحدة المعرفية المعارف بنماذج آلات الحالات المنتهية ودورها واستخداماتها في الحوسبة. وتقدم كذلك المهارات والقدرات لتحليل تعقيد مسائل الحوسبة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نماذج الآلات ٢. نماذج آلات تيورِنْق ٣. نماذج آلات الحالات المنتهية المحددة وغير المحددة ٤. نظرية اللغات المنهجية ٥. القابلية للحوسبة وعدم القابلية للحوسبة ٦. القابلية للحوسبة في آلات تيورنق ٧. تحليل الخوارزميات ٨. قياسات التعقيد: الوقت والتخزين والاتصالات وأعداد وحدات المعالجة ٩. رمز O الكبير في تحليل تعقيد الخوارزميات ١٠. أفضل وأسوأ ومتوسط درجة التعقيد ١١. الحدود العليا والدنيا لدرجة التعقيد ١٢. فئات درجة تعقيد: NP، P، وصعوبة التعامل
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح نظرية الآلات المجردة ونماذج الآلات. ٢. التفريق بين الوظائف القابلة وغير القابلة للحوسبة. ٣. شرح التعقيد وتقييم المتطلبات من الموارد لحوسبة المسائل. ٤. تحليل مسائل معينة باستخدام آلات الحالات المنتهية المحددة وغير المحددة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٤].

أمن دورة حياة الأنظمة والمنتجات Life-Cycle Security (LCS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المفاهيم الأمنية، والمهارات لتطبيقها لتحسين الجوانب الأمنية خلال دورة حياة الأنظمة والمنتجات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مراحل ومسائل دورة حياة الأنظمة: التهيئة، المتطلبات، التصميم، التطوير، الاختبار، النشر، العمليات، الصيانة، والإنهاء ٢. تعيين الثغرات الأمنية وإدارتها وإمكانية تتبعها ٣. نمذجة التهديدات ٤. نموذج نضج توكيد البرمجيات ٥. دور إدارة المشاريع والبرامج ٦. دور إدارة العمليات ٧. أهمية الثقافة والتدريب ٨. عمليات ونماذج التطوير ٩. إدارة الإعدادات ١٠. تهديدات التطوير
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض وتطبيق الممارسات والعمليات والمنهجيات لتأمين البرمجيات. ٢. سرد مراحل دورة حياة الأنظمة وشرح كل مرحلة مع المسائل الأمنية المتعلقة بها. ٣. سرد وشرح عناصر نماذج النضج.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

البرمجة منخفضة المستوى Low Level Programming (LLP)

الوصف	تقدم هذه الوحدة المعرفية المهارات لأداء العمليات منخفضة المستوى بأمان باستخدام لغات البرمجة منخفضة المستوى.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. دعم الوصول منخفض المستوى في لغة C ٢. البرمجة بلغة التجميع ٣. أمن دوال المكتبات ٤. المؤشرات والتعامل معها ٥. تكوين الوحدات البرمجية في البرامج منخفضة المستوى ٦. طرق البرمجة الدفاعية ٧. ترجمة وتجميع وربط ملفات الكائنات ٨. الاستدعاءات في لغة التجميع
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق البرمجة منخفضة المستوى لتنفيذ مكونات نظم التشغيل وبرامج تشغيل العتاد. ٢. مناقشة فوائد ومخاطر استخدام البرمجة منخفضة المستوى.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

إدارة نظام تشغيل لينكس Linux System Administration (LSA)

الوصف	تقدم هذه الوحدة المعرفية المهارات لأداء العمليات الأساسية في إدارة نظم التشغيل لينكس.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تثبيت نظام التشغيل ٢. إدارة حسابات المستخدمين: ضبط الوصول، سياسات كلمة المرور، منهجيات التوثيق، وسياسات المجموعات ٣. واجهات سطر الأوامر ٤. إدارة الإعدادات ٥. التحديثات والتصحيحات ٦. حفظ وتدقيق الأحداث ٧. إدارة خدمات النظام ٨. البيئات الافتراضية ٩. النسخ الاحتياطية واستعادة البيانات ١٠. أمن نظام الملفات ١١. إعدادات الشبكة ١٢. كشف التسلل إلى المضيف ١٣. تطوير السياسات الأمنية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تثبيت وإعداد وتشغيل وصيانة نظام لينكس بطريقة آمنة. ٢. إعداد حسابات المستخدمين وإعداد وتطبيق سياسات التوثيق. ٣. تصميم وتنفيذ إعدادات التدقيق. ٤. تنفيذ عمليات النّسخ الاحتياطية والاستعادة. ٥. شرح أهمية مراجعة سجلات الأمن وتثبيت التحديثات والتصحيحات بشكل دوري.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

التحقيقات الجنائية الرقمية في الوسائط Media Forensics (MEF)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات اللازمة للبحث والتحقيق في الوسائط الرقمية باستخدام طرق التحقيق الجنائي الرقمي.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الحصول على وسيط التخزين ٢. توثيق الأدلة: التحقق والتأكد من صحتها والاختزال ٣. البيانات الوصفية: أختام الوقت للتحديث والوصول والتغيير MAC Timestamps ٤. الاستحواذ الثابت والاستحواذ الحيّ ٥. التصوير المتناثر والتصوير الكامل ٦. المساحات التخزينية المتبقية ٧. الملفات والمجموعات والتقسيميات المخفية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض طرق تحليل التحقيق الجنائي الرقمي على وسائط معينة. ٢. تطبيق منهجيات التحقيق الجنائي الرقمي في وسائط معينة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

تعلم الآلة Machine Learning (MLL)

الوصف	تقدم هذه الوحدة المعرفية المعارف في خوارزميات تعلم الآلة والنماذج الرياضية والإحصائية، كما تقدم أيضا المهارات اللازمة لاستخدام هذه الخوارزميات والنماذج في تطبيقات تعلم الآلة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الانحدار الخطي ٢. التصنيف الخطي ٣. الانحدار اللوجستي ٤. الجيران الأقرب ٥. مقاييس التقييم: AUC، الدقة، الاستدعاء، التحديد، MAPE، MSE، RMSE ٦. اختبار الفرضية ٧. النزول المتدرج ٨. أشجار القرارات ٩. الغابات العشوائية ١٠. آلات متجهات الدعم ١١. المصنِّفات الاحتمالية ١٢. الشبكات العصبية الاصطناعية ١٣. التقسيم إلى فئات ١٤. مفاهيم الجبر الخطي: المرمِّزات الآلية، SVD، PCA ١٥. التعلم المعزَّز
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق خوارزميات ونماذج تعلُّم الآلة لحل مسائل التصنيف والانحدار والتجميع. ٢. تقييم وتفسير نتائج الخوارزميات. ٣. تحليل ومعالجة مجموعات البيانات الضخمة.

تقنيات الهاتف الجوال Mobile Technologies (MOT)

الوصف	تقدم هذه الوحدة المعرفية المعارف بتقنيات الهاتف الجوال بما في ذلك العتاد والاتصالات والإدارة وبيئات البرمجة الخاصة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المعايير والبنى الأساسية وتطورها الزمني: 2G، 3G، LTE/4G، 5G ٢. خيارات التصميم ٣. التشفير ٤. استخدام SS7 للهاتف الجوال ٥. إشارات RRC ٦. الفوترة والشحن ٧. أمن الهاتف الجوال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح طريقة عمل أنظمة الهاتف الجوال في تأمين المكالمات الصوتية والبيانات. ٢. شرح كيفية الحفاظ على الاتصال بالشبكة أثناء الحركة. ٣. مناقشة طرق تأمين أنظمة الهاتف الجوال واتصالاته.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

إدارة أمن الشبكات Network Security Administration (NSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بإدارة وصيانة أمن البنى التحتية للمنظمات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. ربط أهداف الأعمال بأهداف التقنيات ٢. حلول الأمن الرئيسية وفئات وميزات المنتجات ٣. تعارض الأمن السيبراني مع الحلول التقنية ٤. أفضل الممارسات في مجال الأمن السيبراني ٥. تطبيق سياسات أمن الشبكات ٦. وضع المخاطرة والقابلية للمخاطرة ٧. أدوات مراقبة الشبكات والأنظمة ٨. تقييم حالات الأمن السيبراني والاستجابة لها وإدارتها ٩. اكتشاف الحوادث السيبرانية ١٠. عمليات الاستجابة للحوادث السيبرانية وإدارتها ١١. عمليات النشر والترقية ١٢. اختبار قبول المستخدم ١٣. خطط الحجب ١٤. فترات الصيانة وإدارتها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل الاحتياجات والتوصية بالحلول والمنتجات والتقنيات. ٢. اختيار أفضل ممارسات الأمن السيبراني لتلبية أهداف الأعمال وفقاً لافتراضات المخاطر. ٣. حماية أصول تقنية المعلومات والبنية التحتية من التهديدات المحتملة. ٤. تنفيذ مراقبة الأنظمة لكشف الأنماط الشاذة، وإجراء تحديثات وتعديلات دورية للأنظمة. ٥. ممارسة أنشطة الاستجابة للحوادث السيبرانية مثل الانتهاكات والتسلل وسرقة المعلومات. ٦. تخطيط واختبار وتنفيذ وتقييم نشر البرمجيات والعتاد.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

تقنية وبروتوكولات الشبكات Network Technology and Protocols (NTP)

الوصف	تقدم هذه الوحدة المعرفية المعارف الخاصة ببروتوكولات الشبكات ومكوناتها، وتقدم كذلك المهارات اللازمة لاستخدام الأدوات لمراقبة وتحليل الشبكات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مبدلات الشبكات والبروتوكولات الخاصة بها (مثل ARP ،RARP) والمسائل الأمنية في الطبقة الثانية ٢. بروتوكول الإنترنت الإصدار الرابع IPv4 ٣. بروتوكول الإنترنت الإصدار السادس IPv6 ٤. التوجيه في بروتوكولات الإنترنت الإصدار الرابع (IPv4) والإصدار السادس (IPv6): جداول ومقاييس التوجيه، المسائل الأمنية في الطبقة الثالثة وحزمة البروتوكولات الأمنية IPsec ٥. التسمية في الشبكات: أدلة وخدمات أسماء النطاقات DNS ،NetBIOS ٦. تحليل الشبكات واكتشاف الأخطاء وإصلاحها وبروتوكول تدفق الشبكة: Netflow
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض وشرح بناء الطبقة الثانية من الشبكات. ٢. توضيح تراكيب بروتوكولات الإنترنت الإصدار الرابع (IPv4) والإصدار السادس (IPv6). ٣. مناقشة الثغرات الأمنية الشائعة في الشبكات. ٤. اكتشاف وتخفيف أضرار المسائل الأمنية للطبقتين الثانية والثالثة في الشبكات. ٥. تطبيق أدوات تحليل الشبكات لاستكشاف الأخطاء وإصلاحها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

التحقيق الجنائي الرقمي في الشبكات Network Forensics (NWF)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات اللازمة للبحث والتحقيق في تدفق البيانات في الشبكات وتحليلها باستخدام طرق التحقيق الجنائي الرقمي.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التقاط حزم البيانات وتحليلها ٢. كشف ومنع التسلل ٣. تداخل التحقيق الجنائي الرقمي للأجهزة والشبكات ٤. تحليل ملفات السجلات المحفوظة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض منهجيات التحقيق الجنائي الرقمي في الشبكات. ٢. تحليل تدفق البيانات في الشبكات. ٣. اكتشاف الأنشطة الخبيثة والأنماط الشاذة وآثارها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

إدارة نظم التشغيل Operating Systems Administration (OSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات اللازمة لتنفيذ العمليات الأساسية في إدارة نظم التشغيل.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تثبيت نظام التشغيل ٢. إدارة حسابات المستخدمين: ضبط الوصول، سياسات كلمة المرور، طرق التوثيق، سياسات المجموعات ٣. واجهات سطر الأوامر ٤. إدارة الإعدادات ٥. التحديثات والتصحيحات ٦. تسجيل وتدقيق الأحداث ٧. إدارة خدمات النظام ٨. البيئات الافتراضية ٩. النسخ الاحتياطية واستعادة البيانات ١٠. أمن نظام الملفات ١١. إعدادات الشبكة ١٢. كشف التسلل إلى الجهاز المضيف ١٣. إعداد السياسات الأمنية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. إعداد حسابات المستخدمين وإعداد وتطبيق سياسات التوثيق. ٢. تصميم وتنفيذ إعدادات التدقيق. ٣. تنفيذ عمليات النّسخ الاحتياطية والاستعادة. ٤. مراجعة سجلات الأمن والنظام. ٥. تثبيت التحديثات والتصحيحات.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

تأمين نظم التشغيل Operating Systems Hardening (OSH)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لتأمين نظم التشغيل.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التثبيت الآمن ٢. إزالة المكونات غير الضرورية ٣. صيانة نظام الملفات: عزل البيانات الحساسة ٤. قيود المستخدم: الوصول والتفويضات ٥. إدارة المستخدمين والمجموعات والملفات ٦. معايير ومتطلبات كلمات المرور ٧. إيقاف الخدمات غير الضرورية التي ليس لها حاجة ٨. إغلاق المنافذ غير الضرورية التي ليس لها حاجة ٩. إدارة التصحيحات وتحديث البرمجيات ١٠. البيئات الافتراضية ١١. فحص الثغرات الأمنية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض خطوات تأمين نظام تشغيل معين وفقاً لتطبيقات معينة. ٢. إجراء التثبيت الآمن لنظام تشغيل وتعطيل المكونات والخدمات والمنافذ التي ليس لها حاجة. ٣. إجراء تصحيحات وتحديثات دورية لأنظمة التشغيل.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

نظرية نظم التشغيل Operating Systems Theory (OST)

الوصف	تقدم هذه الوحدة المعرفية المعارف لمفاهيم نظم التشغيل ومكوناتها وواجهاتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. حالات الصلاحيات ٢. العمليات، وحزم التعليمات، وإدارة العمليات وحزم التعليمات ٣. إدارة الذاكرة والذاكرة الافتراضية ٤. الاتصالات ما بين العمليات ٥. التوازي والتزامن وحالات الوصول لطريق مسدود ٦. أنظمة الملفات ٧. المدخلات والمخرجات ٨. نظم تشغيل الاستجابة اللحظية والمسائل الأمنية ذات العلاقة ٩. بنى نظم التشغيل الموزعة والمسائل الأمنية ذات العلاقة ١٠. حالات السباق ١١. حالات تجاوز سعة المخزن المؤقت ١٢. البيئات الافتراضية ١٣. دلالات الواجهات الواضحة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح وعرض نظرية نظم التشغيل وتنفيذها. ٢. تصميم وتنفيذ التغييرات في بنى نظم التشغيل.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

الخصوصية Privacy (PRI)

الوصف	تتضمن هذه الوحدة المعرفية المعارف والمهارات حول مفاهيم ومبادئ الخصوصية وطرق تقييم حفظها والتقنيات المساعدة على ذلك وأفضل الممارسات والمعايير وتشريعات الخصوصية ذات العلاقة و سبل تطبيقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مفاهيم ومبادئ الخصوصية ٢. الخصوصية وحفظ البيانات ٣. ملكية البيانات وتصنيفاتها ٤. معلومات التعرف الشخصية ٥. الممارسات ذات العلاقة بحفظ الخصوصية (تحديد الغرض لحفظ أو مشاركة البيانات ، تقليل البيانات المحفوظة حسب الغرض، الشفافية، طلب الموافقة للمشاركة، تقييد الاستخدام، جودة البيانات، السلامة، السرية، المسؤولية، التدقيق) ٦. المخاطر وأنواع الهجمات على الخصوصية ٧. سبل تقييم أثر الخصوصية ٨. التشريعات واللوائح والقوانين الدولية للخصوصية: مثل GDPR، Data Protection Act، HIPPA وغيرها ٩. أدوات وتقنيات تحسين وحفظ الخصوصية ١٠. السياسات و الإجراءات لحفظ الخصوصية في المنظمات ١١. قضايا الخصوصية في التقنيات الناشئة مثل :إنترنت الأشياء، FinTech، وغيرها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح مفاهيم ومبادئ الخصوصية. ٢. إيضاح الفرق بين الحفاظ على الخصوصية وحفظ البيانات. ٣. تحديد الأدوات والتقنيات التي تحسن من حفظ الخصوصية. ٤. مناقشة أثر تشريعات ولوائح الخصوصية الوطنية والدولية على عمل المنظمات والأفراد. ٥. تقييم أثر الخصوصية على أمثلة معطاة. ٦. مناقشة القضايا المعاصرة ذات العلاقة بالخصوصية على المستويين الوطني والدولي.

اختبار الاختراق Penetration Testing (PTT)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق استغلال الثغرات الأمنية للوصول للأنظمة والتحكم بها، كما تقدم المهارات والقدرات اللازمة لاستخدام وتطبيق هذه الطرق.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات فرضيات العيوب ٢. منهجيات أخرى (مثل OSSTMM) ٣. تحديد العيوب من الوثائق ٤. تحديد العيوب من تحليل الرموز المصدرية ٥. فحص الثغرات الأمنية ٦. فئات الهجمات ٧. العيوب التي تؤدي إلى ثغرات ٨. التعداد والاستطلاع ٩. اكتشاف سطح الهجمات ١٠. متجهات الهجمات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تخطيط وإجراء اختبارات الاختراق على شبكة معينة أو نظام معين. ٢. مناقشة ومقارنة فئات وأنواع الهجمات. ٣. شرح الأنواع المختلفة للثغرات وطرق استغلالها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

فحص ضمان الجودة / الوظيفة QA/Functional Testing (QAT)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المنهجيات المتبعة لتقييم مدى تلبية وحدة وظيفية للمتطلبات المطلوبة منها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات الاختبارات: اختبارات الصندوق الأبيض والرمادي والأسود ٢. تحليل تغطية الاختبار ٣. الإنتاج الآلي واليدوي لمدخلات الاختبار ٤. تنفيذ الاختبار ٥. التأكد من صحة النتائج
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتطوير اختبارات فعالة ومنسقة ومنظمة. ٢. إجراء اختبار وظيفي أمني لإظهار التنفيذ الكامل والصحيح للسياسات والآليات الأمنية. ٣. إجراء اختبار وظيفي للتأكد من صحة تنفيذ السياسات الأمنية.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

مبادئ الترددات الراديوية Radio Frequency Principles (RFP)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الاتصالات عبر الـترددات اللاسلكية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أساسيات الإشعاع الكهرومغناطيسي ٢. الهوائيات ٣. تضمين المعلومات ٤. التضمين الرقمي ٥. التمثيل الطيفي ٦. عرض المجال Bandwidth ٧. معدل الأخطاء BER ٨. نسب الطاقة والإشارة والتشويش والعلاقة بينها S/N، Eb/No ٩. تقييد الوصول في الترددات اللاسلكية ١٠. مبادئ الانتشار
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح منهجيات عزل انبعاثات الترددات اللاسلكية. ٢. شرح طرق تعتيم إرسال الترددات اللاسلكية. ٣. شرح العلاقة بين نقل البيانات والتضمين والتعقيد ومعدل الخطأ المقبول وانتشار الإشارة.

تمـت الاسـتفادة من المصـادر التالية لإعداد محتوى هـذه الوحدة المعرفية: [٢].

توكيد البرمجيات Software Assurance (SAS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بطرق ومنهجيات توكيد البرمجيات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المبادئ الأمنية: الفصل، العزل، دمج العناصر في مكون واحد، منح أدنى الصلاحيات، البساطة، التقليل، وضع السلامة والأمان في حالة الأعطال، تصميم الوحدات، تصميم الطبقات الأمنية المتعددة، تقليل المفاجآت، التصميم المفتوح، سهولة الاستخدام، تقليص سطح الهجمات ٢. أمن التصاميم البديلة ٣. مراجعة أنماط التصميمات الآمنة ٤. مستويات المتطلبات الأمنية لبيانات النظام ٥. مسار التدقيق ٦. طرق النمذجة الأمنية وتعيين الثغرات ٧. زيادة الصمود ٨. مراجعات التصميم
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق مبادئ التصميم الأمني. ٢. توضيح تأثيرات تصميم النظام وبنيته على الأمن. ٣. تصميم نظام معيّن لتلبية المتطلبات الأمنية بالشكل الأمثل. ٤. بناء تصميم آمن باستخدام النمذجة وتقييم الثغرات الأمنية. ٥. مناقشة كيف يمكن أن تساعد مراجعة التصميم على تحسين الأمن بشكل كبير.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

التحكم بالأنظمة System Control (SCC)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق التحكم بالأنظمة بما فيها الكشف عن الهجمات، والتعويض عن أضرارها، ومواجهتها ومنعها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. ضبط الوصول: التحكم بالوصول إلى الموارد، وسلامة الضوابط ٢. نماذج التصاريح: إدارة التصاريح عبر أنظمة متعددة وتمييز التصريح عن التوثيق ٣. اكتشاف التسلل: الأنماط الشاذة، إساءة الاستخدام [القائم على القواعد، والقائم على التوقيع] والطرق القائمة على المواصفات ٤. الهجمات: الأشجار والرسومات والهجمات المحددة ٥. الدفاعات: التوزيع العشوائي للعناوين ASLR، تغيير عناوين الإنترنت IP، تحمل التسلل ٦. التدقيق: حفظ السجلات، تحليل السجلات، العلاقة بالكشف عن حالات التسلل ٧. البرمجيات الضارة: الفيروسات، الديدان البرمجية، وبرمجيات الفدية ٨. نماذج الثغرات: نماذج RISOS، CWE، CVE، PA ٩. اختبار الاختراق: منهجية فرضية العيوب، OSSTMM، ISSAF، PTES، GISTA ١٠. التحقيق الجنائي الرقمي: متطلبات الأنظمة للتحقيق الجنائي الرقمي ١١. التعافي والصمود: آليات التوافر
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. فحص الاعتبارات الأمنية الداخلة في التحكم بالنظام نفسه. ٢. كشف الهجمات المتعلقة بالتحكم بالأنظمة والتعويض عن أضرارها ومواجهتها ومنعها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

بروتوكولات الاتصالات الآمنة Secure Communication Protocols (SCP)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول بروتوكولات الاتصالات الآمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. بروتوكولات طبقة التطبيقات والنقل: SSL/TLS، SSH، HTTPS، HTTP ٢. الهجمات على بروتوكول أمن طبقة النقل TLS: هجمات تخفيض المستوى، تزوير الشهادات، آثار سرقة الشهادات الجذرية، شفافية الشهادة ٣. طبقة الإنترنت/الشبكة: حزمة البروتوكولات الأمنية IPsec، الشبكات الافتراضية الخاصة VPN ٤. بروتوكولات الحفاظ على الخصوصية: Tor، Mixnet، الرسائل والإشارات السرية ٥. طبقة ربط البيانات: بروتوكولات RADIUS، PPP، L2TP
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. ممارسة بروتوكولات الاتصالات الآمنة (مثل SSL/TLS، SSH، HTTPS، RADIUS، PPP، L2TP، VPN، IPsec). ٢. شرح الهجمات الشائعة على بروتوكولات الاتصالات المختلفة، وكيفية الحماية منها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٣].

أمن سلاسل الإمداد Supply Chain Security (SCS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بالمسائل الأمنية المتعلقة بمكونات الطرف الثالث المستخدمة في بناء أنظمة معقدة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مخاطر سلاسل الإمداد: مخاطر الأمن السيبراني المتعلقة بالطرف الثالث وأفضل الممارسات للتعامل معها ٢. توجهات التطوير على المستوى العالمي ٣. الإنتاج خارج الحدود ٤. نقل ولوجستيات مكونات تقنية المعلومات ٥. تقييم ممارسات التطوير لدى الطرف الثالث ٦. قدرات وحدود الهندسة العكسية للبرمجيات والعتاد ٧. عملية التوريد والمشتريات: الأمن المادي، تقسيم التصنيع، قابلية التتبع، فحص الشحنات، التأكد من صحتها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة المسائل والمخاطر السيبرانية المتعلقة بالاستعانة بمصادر خارجية لتوريد وتطوير ودمج العتاد والبرمجيات. ٢. شرح الثغرات الأمنية الشائعة في مكونات سلسلة الإمداد. ٣. شرح طرق التعامل مع المخاطر السيبرانية المتعلقة بسلاسل الإمداد وطرق تخفيفها وشرح التحديات في هذه الطرق.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

برمجة النظم Systems Programming (SPG)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لتطوير برمجيات معقدة على المستوى المنخفض.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. واجهات وتفاعلات العتاد والبرمجيات ٢. أنواع برامج النظم: بيئات التطوير، نظم التشغيل، الخدمات، وظائف الشبكات، برامج تشغيل الأجهزة، أطر التخزين، محركات الألعاب ٣. تصميم الخدمات في طبقات ٤. واجهات برمجة التطبيقات (API) ٥. برمجة الواجهات الداخلية لنظم التشغيل ٦. برمجة المستوى المنخفض: لغة التجميع، لغة C ٧. تحسين للموارد ٨. إدارة الموارد ٩. تقليص الوقت الزائد للتشغيل ١٠. التحكم المباشر بالوصول إلى الذاكرة والتحكم بالانسياب ١١. إدارة الذاكرة في برمجيات الأنظمة ١٢. المخاوف الأمنية في برمجيات الأنظمة ١٣. مراقبة وتسجيل برمجيات الأنظمة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطوير برامج بإمكانها العمل بشكل صحيح باستخدام موارد محدودة. ٢. تطبيق نهج الطبقات للوصول إلى واجهات برمجة التطبيقات (API). ٣. تنفيذ وظائف جديدة في لب نظام التشغيل أو برامج تشغيل الأجهزة. ٤. تنفيذ وظائف الأنظمة بدون استخدام مكتبات خارجية.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

ممارسات البرمجة الآمنة Secure Programming Practices (SPP)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لتطوير وتنفيذ برمجيات آمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الثغرات والعيوب البرمجية الشائعة وأفضل الممارسات لتفاديها ٢. ممارسات البرمجة الدفاعية ٣. استخدامات التشفير في البرمجة ٤. منهجيات فحص البرامج ومراجعتها من الجوانب الأمنية ٥. التحليل الثابت والتحليل الديناميكي للبرامج ٦. بناء الدوال البرمجية بطريقة آمنة وضبط الوصول لها ٧. فحص المدخلات والتحقق منها ٨. التعامل مع أنواع البيانات ونطاقاتها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح الثغرات والعيوب البرمجية الشائعة. ٢. مناقشة أفضل الممارسات والمنهجيات لتطوير وفحص البرمجيات الآمنة. ٣. تصميم وتطوير برمجيات آمنة تلبي متطلباتها الوظيفية.

الهندسة العكسية للبرمجيات Software Reverse Engineering (SRE)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات اللازمة لإجراء الهندسة العكسية على برمجيات قابلة للتنفيذ لتحديد وظائفها وتأثيرها وتفاصيل تنفيذها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تحليل البرمجيات الضارة ٢. أدوات وتقنيات الهندسة العكسية ٣. التحليل الثابت والتحليل الديناميكي ٤. وضع الحماية والفحص Sandboxing ٥. تقنيات منع الهندسة العكسية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. استخدام طرق الهندسة العكسية للبرمجيات. ٢. تطبيق أدوات الهندسة العكسية للبرمجيات لاكتشاف وظائف وتفاصيل التنفيذ وطريقة عمل البرمجيات الضارة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

التحليل الأمني للبرمجيات Software Security Analysis (SSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الأدوات والطرق المستخدمة لتحليل أمن البرمجيات في صورة الرموز الثنائية أو المصدرية، كما تقدم المهارات والقدرات اللازمة لاستخدام هذه الأدوات والطرق لتحليل أمن البرمجيات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات الاختبار ٢. تحليل الرموز البرمجية المصدرية والثنائية ٣. طرق التحليل الثابت والديناميكي ٤. وضع الحماية والفحص Sandboxing ٥. أدوات وطرق التحليل الشائعة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف الأدوات والطرق المستخدمة للتحليل الأمني للبرمجيات. ٢. تطبيق أدوات التحليل الأمني للبرمجيات لتحليل مكونات البرمجيات غير المعروفة.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

هندسة أمن الأنظمة Systems Security Engineering (SSE)

الوصف	تقدم هذه الوحدة المعرفية المهارات اللازمة للمشاركة في تطوير أنظمة آمنة واسعة النطاق باستخدام التقنيات والطرق ذات العلاقة في كافة مراحل دورة حياة النظام.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تصميم الاختبار ٢. منهجيات الاختبار ٣. الخصائص الناشئة ٤. هندسة الأنظمة ٥. دمج الأنظمة ٦. تحليل قرار الصناعة أو الشراء ٧. تحليل أمن الأنظمة ٨. مكونات النظام المؤسسي
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. المشاركة في تطوير مكونات الأنظمة من خلال واحد أو أكثر من الأنشطة التالية: جمع وتحليل المتطلبات، التصميم، التطوير والتنفيذ، الفحص، الصيانة. ٢. تحليل المكونات في نظام مركّب. ٣. تحليل تصميم نظام معيّن، وتقييم مدى تلبيته لمتطلبات أمن النظام.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

تحليل الثغرات الأمنية Vulnerability Analysis (VLA)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات المتعلقة باكتشاف ثغرات الأنظمة والشبكات، والتعرف عليها، وتحديد السبب الجذري لها، وتخفيف أضرارها ومعالجتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تعريف الثغرات الأمنية ٢. طرق نمذجة الأنظمة ٣. تعيين الثغرات الأمنية ٤. خصائص وتصنيف الثغرات الأمنية ٥. التصنيف: تجاوز سعة المخزن المؤقت، تصعيد الصلاحيات، الجذور الخفية، أحصنة الطروادة، الأبواب الخلفية، الفيروسات، البرمجة الموجهة للعودة، ثغرات الهندسة الاجتماعية، وتأثير الصلاحيات الإدارية على الثغرات الأمنية ٦. الأسباب الجذرية للثغرات الأمنية ٧. استراتيجيات تخفيف الأضرار ٨. تحليل التدابير المضادة ٩. الإفصاح عن الثغرات الأمنية ١٠. أدوات وطرق اكتشاف الثغرات الأمنية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق أدوات وطرق اكتشاف الثغرات الأمنية. ٢. بناء خريطة الثغرات الأمنية لنظام معيّن. ٣. تتبّع الثغرات الأمنية لتحديد أسبابها الجذرية. ٤. عرض التدابير المضادة لتخفيف أضرار الثغرات الأمنية وتحليل هذه التدابير. ٥. مناقشة السيناريوهات التي يجب فيها الإفصاح عن الثغرات الأمنية.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢]، [٣].

تقنيات البيئة الافتراضية Virtualization Technologies (VTT)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بالبيئات الافتراضية الحديثة للمضيف وتنفيذها ونشرها واستخدامها ومكونات أنظمتها وأمنها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. بنى البيئات الافتراضية ٢. طرق البيئات الافتراضية لتنفيذ الرموز البرمجية ٣. إدارة الذاكرة في البيئات الافتراضية ٤. الشبكات في البيئات الافتراضية ٥. التخزين في البيئات الافتراضية ٦. جدولة الآلات الافتراضية ٧. الترحيل واللقطات ٨. طبقات الإدارة الافتراضية ٩. التحقيقات الجنائية الرقمية في البيئات الافتراضية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح مفاهيم البيئة الافتراضية. ٢. شرح بنى البيئات الافتراضية والتمييز بينها. ٣. تصميم البيئات الافتراضية وبنائها وتنفيذها وضبط إعداداتها.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

أمن تطبيقات الويب Web Application Security (WAS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بالتقنية والأدوات والممارسات المتعلقة بتطبيقات الويب، كما تقدم المهارات اللازمة لتطبيق هذه الأدوات والممارسات لتطوير ونشر تطبيقات ويب آمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تقنيات تطبيقات الويب: بروتوكول HTTP، تصاميم الترميز، بنى تطبيقات الويب، وتقنيات/ لغات JSON، XML، AJAX ٢. الضوابط من طرف الخادم ٣. التوثيق ٤. إدارة الجلسات ٥. ضوابط الوصول ٦. الضوابط من طرف العميل ٧. الثغرات القائمة على المدخلات: حقن SQL، حقن SQL الأعمى، النصوص البرمجية عبر المواقع، تزوير الطلب عبر المواقع ٨. هجمات JavaScript، هجمات معلومات التصفح المحفوظة Cookies ٩. ثغرات المدخلات الخاصة بالوظيفة ١٠. مهاجمة منطق التطبيقات ١١. الهجمات الحديثة الشائعة ١٢. ثغرات الاستضافة المشتركة ١٣. ثغرات خادم التطبيقات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح تقنيات تطبيقات الويب الشائعة والمسائل الأمنية ذات العلاقة. ٢. تطوير ونشر تطبيقات ويب آمنة. ٣. شرح مبادئ أمن تطبيقات الويب.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

إدارة نظام ويندوز Windows System Administration (WSA)

الوصف	توفر هذه الوحدة المعرفية المعارف والمهارات لإجراء العمليات الأساسية في إدارة نظام مايكروسوفت ويندوز.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تثبيت نظام التشغيل ٢. إدارة حسابات المستخدمين: ضبط الوصول، سياسات كلمات المرور، طرق التوثيق، سياسات المجموعات ٣. واجهات سطر الأوامر ٤. إدارة الإعدادات ٥. التحديثات والتصحيحات ٦. تسجيل وتدقيق الأحداث ٧. إدارة خدمات النظام ٨. البيئات الافتراضية ٩. إعداد النسخ الاحتياطية واستعادة البيانات ١٠. أمن نظام الملفات ١١. إعدادات الشبكة: أمن المنافذ ١٢. كشف التسلل إلى المضيف ١٣. إعداد السياسات الأمنية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تثبيت وإعداد وتشغيل وصيانة نظام تشغيل "مايكروسوفت ويندوز" بطريقة آمنة. ٢. إعداد حسابات المستخدمين وإعداد وتطبيق سياسات التوثيق. ٣. تصميم وتنفيذ إعدادات التدقيق. ٤. إجراء عمليات النُّسخ الاحتياطية والاستعادة. ٥. عرض أهمية مراجعة السجلات الأمنية وتثبيت التحديثات والتصحيحات بشكل دوري.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [٢].

شبكات الاستشعار اللاسلكية Wireless Sensor Networks (WSN)

الوصف	تتضمن هذه الوحدة المعرفية المعارف المتعلقة بمبادي شبكات الاستشعار اللاسلكية، والتحديات والنواحي الأمنية المتعلقة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أجهزة الاستشعار اللاسلكية ٢. تطبيقات شبكات الحساسات اللاسلكية ٣. نشر شبكات الاستشعار اللاسكلية: منظم، عشوائي، البنية، التحكم بقوة الإشارة، التغطية، التنقل ٤. تحديد المواقع ٥. التزامن ٦. خصائص الإرسال اللاسلكي ٧. الوصول للقناة ٨. جدولة السبات ٩. استهلاك الطاقة بشكل فعال ١٠. الخدمات الشبكية المتمحورة حول البيانات ١١. التحكم بالازدحام، واعتمادية النقل ١٢. النواحي الأمنية المرتبطة بشبكات الاستشعار اللاسلكية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. إجراء عمليات محاكاة لشبكات الاستشعار اللاسلكية لسيناريوهات معيّنة. ٢. إجراء تجارب حقيقية لشبكات الاستشعار اللاسلكية الآمنة بناءً على إعدادات معيّنة. ٣. تطبيق آليات تحديد المواقع والتزامن واستهلاك الطاقة بشكل فعال.

تمت الاستفادة من المصادر التالية لإعداد محتوى هذه الوحدة المعرفية: [١٢].

المصادر

[١] الإطار الوطني للمؤهلات من هيئة تقويم التعليم والتدريب، عام ٢٠٢٠.

[٢] البرنامج الإرشادي والوحدات المعرفية للمراكز الوطنية للتميّز الأكاديمي في الدفاع السيبراني (CAE-CD)، عام ٢٠١٩.

[٣] مناهج الأمن السيبراني من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠١٧.

[٤] مناهج علوم الحاسوب من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠١٣.

[٥] كتاب "أنماط الأمن في الممارسة: تصميم بنيات آمنة باستخدام أنماط البرمجيات Security Patterns in Practice: Designing Secure Architectures Using Software Patterns"، إدواردو فرناندیز-بوغليوني، الطبعة الأولى، عام ٢٠١٣.

[٦] كتاب "اكتمال البرمجة: دليل عملي لبناء البرامج Code Complete: A Practical Handbook of Software Construction"، ستيف ميكونل، الطبعة الثانية، عام ٢٠١٤.

[٧] كتاب "نمذجة التهديد: التصميم من أجل الأمن Threat Modeling: Designing for Security"، آدم شوستاك، عام ٢٠١٤.

[٨] كتاب "الأخلاقيات في تقنية المعلومات Ethics in Information Technology"، سينجاج ليرنينج، الطبعة الخامسة، عام ٢٠١٤.

[٩] كتاب "مجموعة أدوات تقييم مخاطر أمن المعلومات: تقييمات عملية من خلال جمع البيانات وتحليل البيانات Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis"، جيسون مارتن، مارك تالبيس، عام ٢٠١٣.

[١٠] كتاب "مقدمة للخوارزميات Introduction to Algorithms"، توماس كورمن، تشارلز ليزرسون، رونالد رايفست، كليفورد ستين الطبعة الثالثة، عام ٢٠٠٩.

[١١] نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

[١٢] كتاب "ربط شبكات الحساسات اللاسلكية Networking Wireless Sensors"، باسكار كريشنامشاري، عام ٢٠٠٩.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority