الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي للمواءمة مع الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

- أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج الجهة خارج النطاق المحدد للاستلام.

- برتقالي – مشاركة محدودة

المستلم يمكنه مشاركة المعلومات في نفس الجهة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

- أخضر – مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في نفس الجهة أو جهة أخرى على علاقة معهم أو في نفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

- أبيض – غير محدود

قائمة المحتويات

مقدمة

اشتملت اختصاصات الهيئة الوطنية للأمن السيبراني الواردة في تنظيمها على «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»، وانطلاقًا من حرص الهيئة على بناء وتطوير برامج أكاديمية وطنية عالية الجودة في مجال الأمن السيبراني، فقد عملت الهيئة مع وزارة التعليم وهيئة تقويم التعليم والتدريب وعدد من الجامعات في المملكة على إعداد «الإطار السعودي للتعليم العالي في الأمن السيبراني»(سايبر-التعليم).

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.

يمكن الاستفادة من هذا الإطار وتطبيقه على البرامج التعليمية والدرجات العلمية في تخصصات الأمن السيبراني التي يتم تدريسها في المؤسسات التعليمية العامة والخاصة للتعليم العالي في المملكة العربية السعودية. ويغطي هذا الإطار توصيفات برامج الدرجات العلمية للتعليم العالي في تخصصات الأمن السيبراني، بالإضافة إلى ملخص متطلبات القبول، والوحدات المعرفية الأساسية، والوحدات المعرفية الاختيارية لجميع البرامج كما هو موضح بالشكل ١.

	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						

الشكل ١: ملخص متطلبات القبول، والوحدات المعرفية الأساسية، والوحدات المعرفية الاختيارية لجميع البرامج

أهداف إطار سايبر-التعليم

١. أن يكون دليلًا إرشاديًا يمكن الاستفادة منه في تطوير وتقييم واعتماد برامج التعليم العالي في الأمن السيبراني.

٢. وضع الحد الأدنى من متطلبات الخطط الدراسية لبرامج التعليم العالي في الأمن السيبراني؛ لضمان جودتها الأكاديمية وقدرتها على تخريج كوادر مؤهلة تأهيلًا عاليًا في مجال الأمن السيبراني.

٣. مواءمة مخرجات برامج التعليم العالي في الأمن السيبراني مع الاحتياج للكوادر الوطنية العاملة في مجال الأمن السيبراني.

خطوات المواءمة مع إطار سايبر-التعليم

التقييم الذاتي

التحكيم

قرار المواءمة

آلية المواءمة مع إطار سايبر-التعليم

١. التقييم الذاتي

١-١ تعبئة

تقوم المؤسسة التعليمية بتعبئة نموذج المواءمة المتوفر على صفحة الإطار عبر: https://nca.gov.sa/pages/scyberedu.html

١-٢ مشاركة

عبر البريد الإلكتروني scyber-edu@nca.gov.sa، ترسل المؤسسة التعليمية طلب مواءمة برنامج محدد مع الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)، بالتفاصيل التالية:

- اسم البرنامج.
- الدرجة العلمية للبرنامج.
- عدد ساعات البرنامج.
- نموذج المواءمة بعد تعبئته.
- معلومات ضابط الاتصال.

١-٣ تقييم أولي

- تعمل الهيئة تقييم أولي لطلب المواءمة المقدم وتتم مراجعة نموذج المواءمة.
- تشارك الهيئة التغذية الراجعة على نموذج المواءمة مع المؤسسة التعليمية، وتطلب من المؤسسة التعليمية تزويدها بالوثائق الداعمة.

آلية المواءمة مع إطار سايبر-التعليم

١. التقييم الذاتي

١-٤ تحديث

تحدث المؤسسة التعليمية نموذج المواءمة حسب التغذية الراجعة، وتشارك ما يلي عبر البريد الإلكتروني scyber-edu@nca.gov.sa:

- نموذج المواءمة بعد التحديث.
- الوثائق والأدلة الداعمة، مع مراعاة التالي:
  - أن يكون حجم مرفقات البريد الإلكتروني ١٠ ميجابايت أو أقل، وفي حال الاحتياج إلى مشاركة ملفات أكبر من ١٠ ميجابايت، تتم مشاركتها عبر عدة رسائل إلكترونية.
  - أن تكون الملفات المرفقة بأحد الصيغ التالية (.PDF, .docx, .xlsx, .7z).

٢. التحكيم

١.٢ المراجعة

- تقوم الهيئة بمراجعة نموذج المواءمة المحدث مع الملفات والوثائق الداعمة.

٢.٢ التحكيم

- تشارك الهيئة نموذج المواءمة المحدث والوثائق الداعمة مع عدد من المحكمين المستقلين لإعداد تقرير المواءمة.
- يشارك المحكمين تقرير المواءمة مع فريق الهيئة.
- يتم إعداد التقرير النهائي لقرار المواءمة بحسب تقارير المحكمين.

٣. قرار المواءمة

تشارك الهيئة تقرير المواءمة مع المؤسسة التعليمية، وتكون مستويات القرار كالتالي:

٣-١ «موائم»

- تصدر الهيئة وثيقة مواءمة للبرنامج لمدة خمس سنوات.
- تدرج الهيئة البرنامج كبرنامج موائم بموقع الهيئة الوطنية للأمن السيبراني.

٣-٢ «موائم مشروط»

- تطلب الهيئة من المؤسسة التعليمية تطوير خطة علاجية لمواءمة البرنامج المعني مع إطار سايبر-التعليم.
- تشارك المؤسسة التعليمية الخطة العلاجية مع الهيئة، وتلتزم بتنفيذها خلال سنة.
- تصدر الهيئة وثيقة مواءمة للبرنامج لمدة سنة.
- تدرج الهيئة البرنامج كبرنامج موائم مشروط بموقع الهيئة الوطنية للأمن السيبراني.

٣-٣ «غير موائم»

- تطلب الهيئة من المؤسسة التعليمية معالجة الملاحظات الواردة في التقرير.
- يحق للمؤسسة التعليمية التقديم لطلب مواءمة البرنامج بعد سنة من الطلب السابق.

نموذج المواءمة

محتويات النموذج:

Cover Page	Program General Information	ProgramCourses	Alignment
Intermediate Diploma	Bachelors (Cybersecurity Track)	Bachelors (Cybersecurity Major)	
Higher Diploma (IT Background)	HigherDiploma(Non-ITBackground)	Masters	Doctoral

١. صفحة الغلاف (Cover Page)

٢. ورقة عمل معلومات البرنامج العامة (Program General Information)

٣. ورقة عمل مقررات البرنامج (Program Courses)

٤. ورقة عمل المواءمة (Alignment)

٥. صفحات برامج التعليم العالي في الأمن السيبراني التي يُعرّفها الإطار:

٥-١. برنامج الدبلوم المتوسط

٥-٢. برنامج البكالوريوس (مسار في الأمن السيبراني)

٥-٣. برنامج البكالوريوس (برنامج في الأمن السيبراني)

٥-٤. برنامج الدبلوم العالي (لغير المختصين في تقنية المعلومات)

٥-٥. برنامج الدبلوم العالي (للمختصين في تقنية المعلومات)

٥-٦. برنامج الماجستير

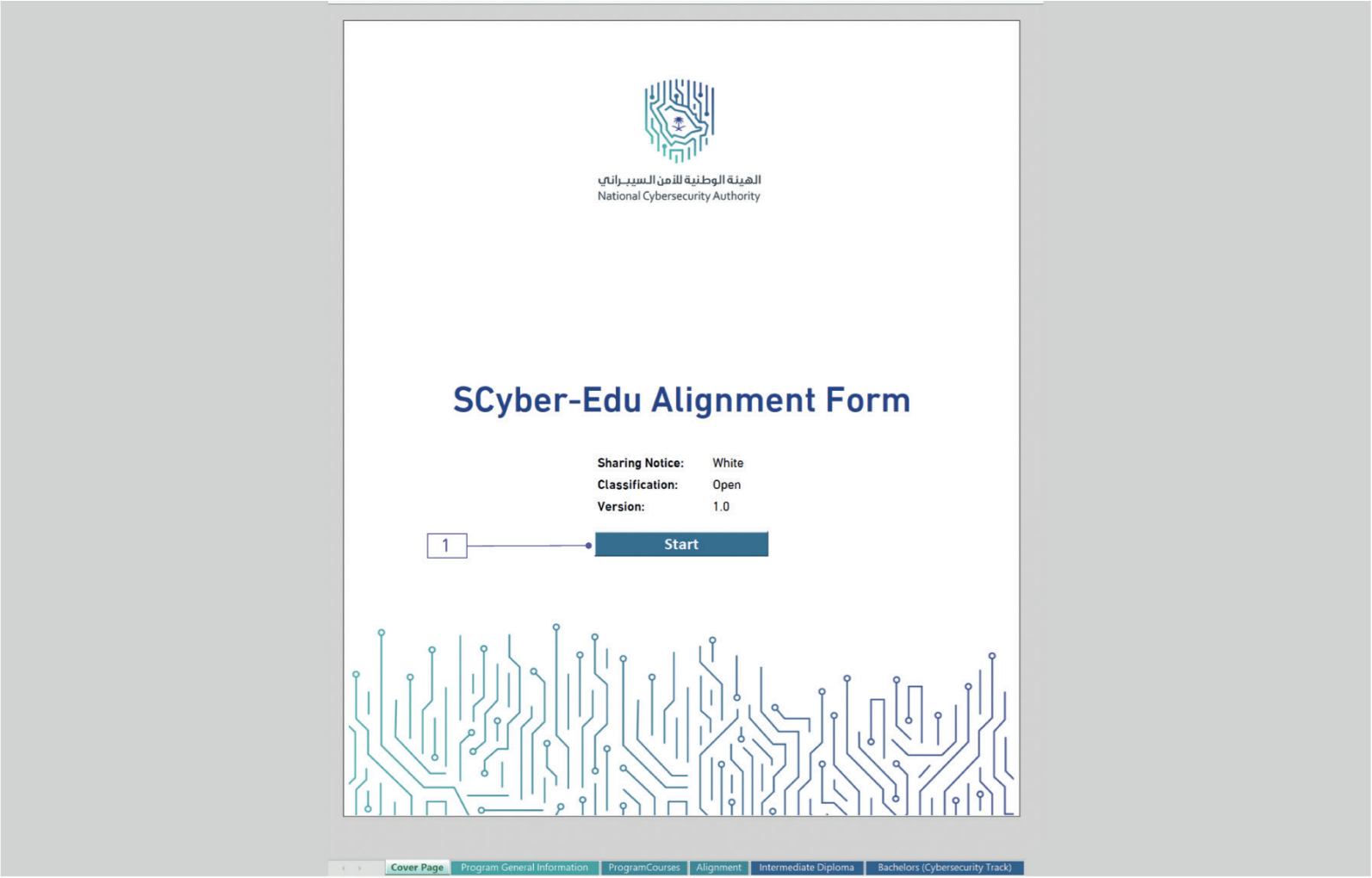
٥-٧. برنامج الدكتوراه

ملاحظة: يلزم تعبئة نموذج المواءمة بشكل مستقل لكل برنامج عالٍ في الأمن السيبراني، وإن كانت هذه البرامج تتبع لنفس المؤسسة التعليمية.

خطوات تعبئة نموذج المواءمة

١. صفحة الغلاف (Cover Page)

١-١. الضغط على زر البداية "Start".



٢. ورقة عمل معلومات البرنامج العامة (Program General Information)

٢-١. إدخال المعلومات العامة للبرنامج (اسم المؤسسة التعليمية، ودرجة البرنامج، واسم البرنامج، ومدة البرنامج، وعدد المقررات، وعدد الساعات المعتمدة، ونبذة عن البرنامج)

٢-٢. إدخال متطلبات القبول للبرنامج.

٢-٣. إدخال نواتج تعلم البرنامج.

٢-٤. الضغط على زر التالي «Next».


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority
Previous
Next
Program General Information (1 - 4)
2.4
2.1
2.2
2.3
General Information about the Program
University Name
Program
Title
Period (in years)
Number of Courses
Total Credit Hours
Please select a program
Program Summary
Index
Admission Requirements
1
2
3
4
5
Other
Index
Program Learning Outcomes (PLOs)
1
2
3
4
5
6
7
8
Program
Please select a program
Please select a program
Intermediate Diploma
Bachelors (Cybersecurity Track)
Bachelors (Cybersecurity Major)
Higher Diploma (IT Background)
Higher Diploma (Non-IT Background)
Masters
Doctoral

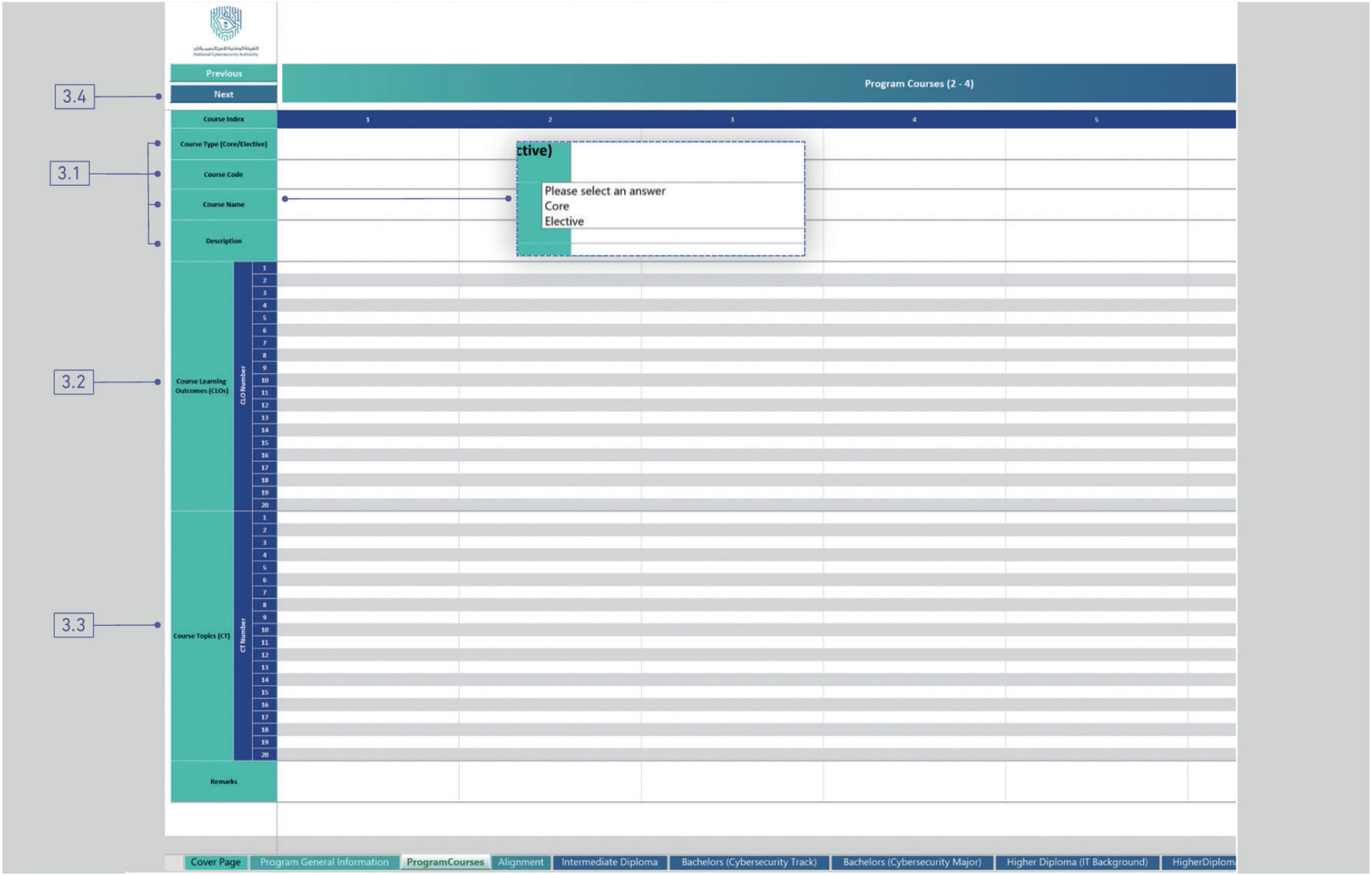
٣. ورقة عمل مقررات البرنامج (Program Courses Sheet)

٣-١. إدخال معلومات مقررات البرنامج المعني، لكل مقرر (نوع المقرر -إلزامي أو اختياري-، ورمز المقرر، واسم المقرر، وتوصيف المقرر).

٣-٢. إدخال نواتج تعلم لكل مقرر.

٣-٣. إدخال مواضيع لكل مقرر.

٣-٤. الضغط على زر التالي «Next».


3.4
3.1
3.2
3.3
Previous
Next
Program Courses (2 - 4)
Course Index
Course Type (Core/Elective)
Course Code
Course Name
Description
ctive)
Please select an answer
Core
Elective
Course Learning Outcomes (CLOs)
CLO Number
Course Topics (CT)
CT Number
Remarks
Cover Page
Program General Information
ProgramCourses
Alignment
Intermediate Diploma
Bachelors (Cybersecurity Track)
Bachelors (Cybersecurity Major)
Higher Diploma (IT Background)
HigherDiplom

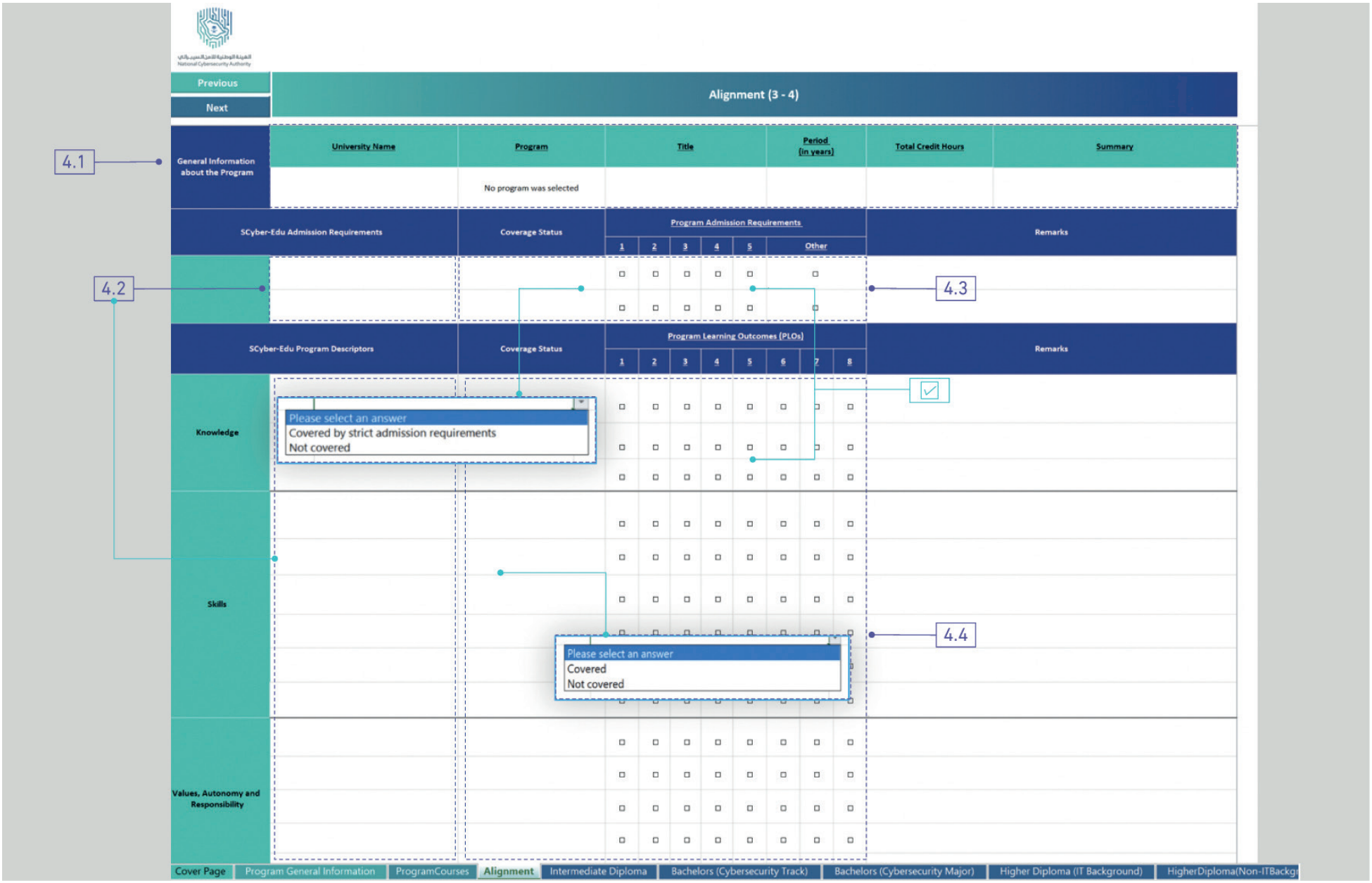
٤. ورقة عمل المواءمة (Alignment)

٤-١. تُعبأ تلقائيًا من مدخلات خطوة ٢-١ بورقة عمل معلومات البرنامج العامة (Program General Information).

٤-٢. تُعبأ تلقائيًا من متطلبات البرنامج المقابل بإطار سايبر-التعليم.

٤-٣. ربط متطلبات القبول للبرنامج المعني، وذلك بتحديد حالة التغطية (Coverage Status)، وتحديد رقم/أرقام متطلبات القبول (Program Admission Requirements) الذين يحققون متطلبات قبول البرنامج المقابل بإطار سايبر-التعليم.

٤-٤. ربط نواتج تعلم البرنامج المعني، وذلك بتحديد حالة التغطية (Coverage Status)، وتحديد رقم/أرقام نواتج تعلم البرنامج (Program Learning Outcome) التي تحقق نواتج تعلم البرنامج المقابل بإطار سايبر-التعليم.


Previous
Next
Alignment (3 - 4)
General Information about the Program
University Name
Program
Title
Period (in years)
Total Credit Hours
Summary
No program was selected
SCyber-Edu Admission Requirements
Coverage Status
Program Admission Requirements
1 2 3 4 5 Other
Remarks
SCyber-Edu Program Descriptors
Coverage Status
Program Learning Outcomes (PLOs)
1 2 3 4 5 6 7 8
Remarks
Knowledge
Skills
Values, Autonomy and Responsibility
Please select an answer
Covered by strict admission requirements
Not covered
Please select an answer
Covered
Not covered
4.1
4.2
4.3
4.4
Cover Page
Program General Information
ProgramCourses
Alignment
Intermediate Diploma
Bachelors (Cybersecurity Track)
Bachelors (Cybersecurity Major)
Higher Diploma (IT Background)
HigherDiploma(Non-ITBackg

٤-٥. ربط متطلبات الرياضيات للبرنامج المعني، وذلك بتحديد حالة التغطية (Coverage Status)، وتحديد رموز المقررات التي تحقق متطلبات الرياضيات للبرنامج المقابل بإطار سايبر-التعليم -إن وجدت-.

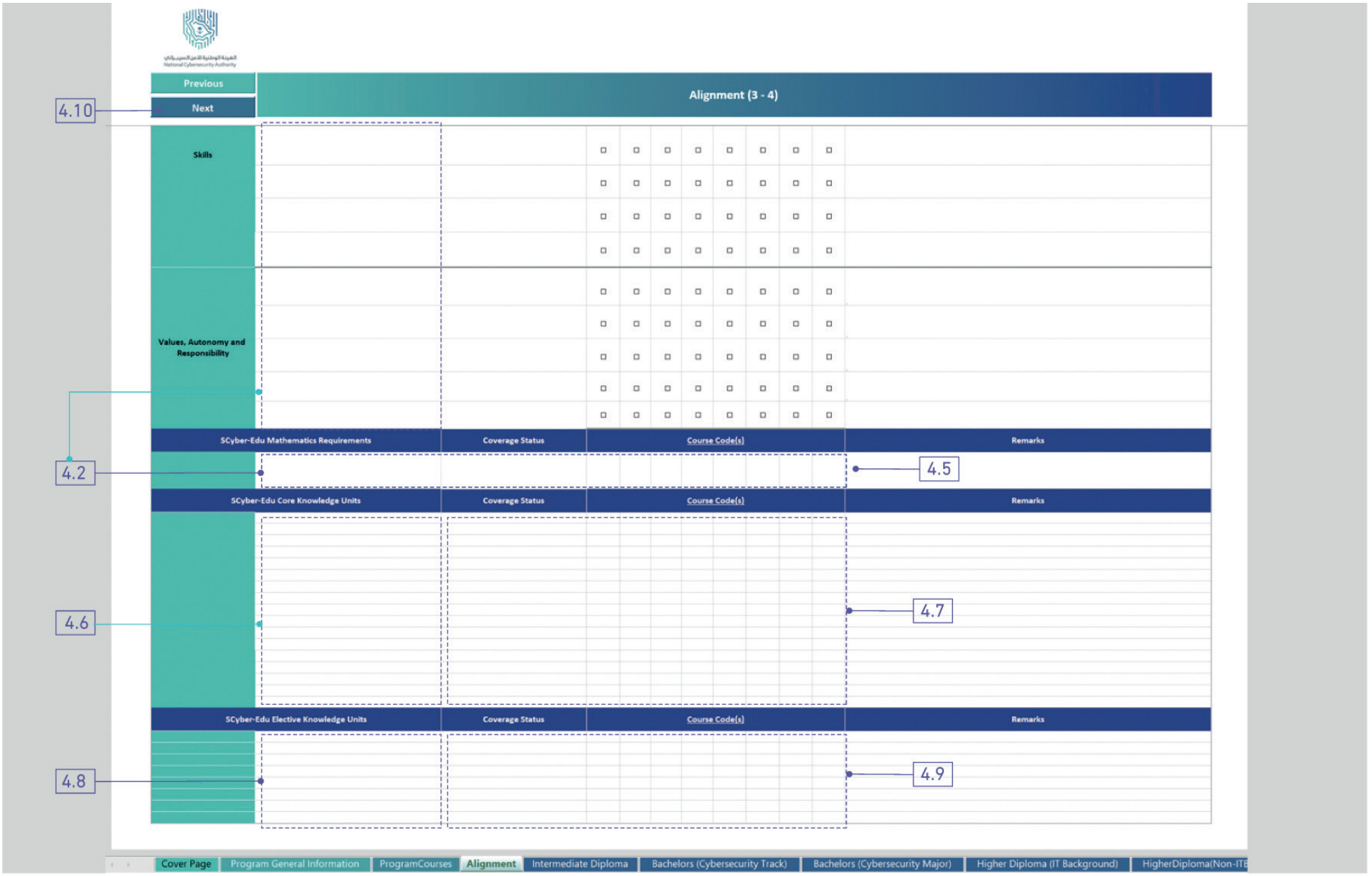
٤-٦. تُعبأ تلقائيًا من الوحدات المعرفية الأساسية للبرنامج المقابل بإطار سايبر-التعليم.

٤-٧. ربط مقررات البرنامج المعني بالوحدات المعرفية الأساسية للبرنامج المقابل بإطار سايبر-التعليم، وذلك بتحديد حالة التغطية (Coverage Status) ورموز المقررات التي تحقق متطلبات هذه الوحدات المعرفية.

٤-٨. تحديد الوحدات المعرفية الاختيارية من القائمة المنسدلة للوحدات المعرفية المخصصة للبرنامج المقابل بإطار سايبر-التعليم.

٤-٩. ربط مقررات البرنامج المعني بالوحدات المعرفية الاختيارية التي تم اختيارها وذلك بتحديد حالة التغطية (Coverage Status) ورموز المقررات التي تحقق متطلبات هذه الوحدات المعرفية.

٤-١٠. ومن ثم الضغط على زر التالي «Next».


Previous
Next
Alignment (3 - 4)
Skills
Values, Autonomy and Responsibility
SCyber-Edu Mathematics Requirements
Coverage Status
Course Code(s)
Remarks
SCyber-Edu Core Knowledge Units
SCyber-Edu Elective Knowledge Units
4.10
4.2
4.5
4.6
4.7
4.8
4.9
Cover Page
Program General Information
ProgramCourses
Alignment
Intermediate Diploma
Bachelors (Cybersecurity Track)
Bachelors (Cybersecurity Major)
Higher Diploma (IT Background)
HigherDiploma(Non-ITE

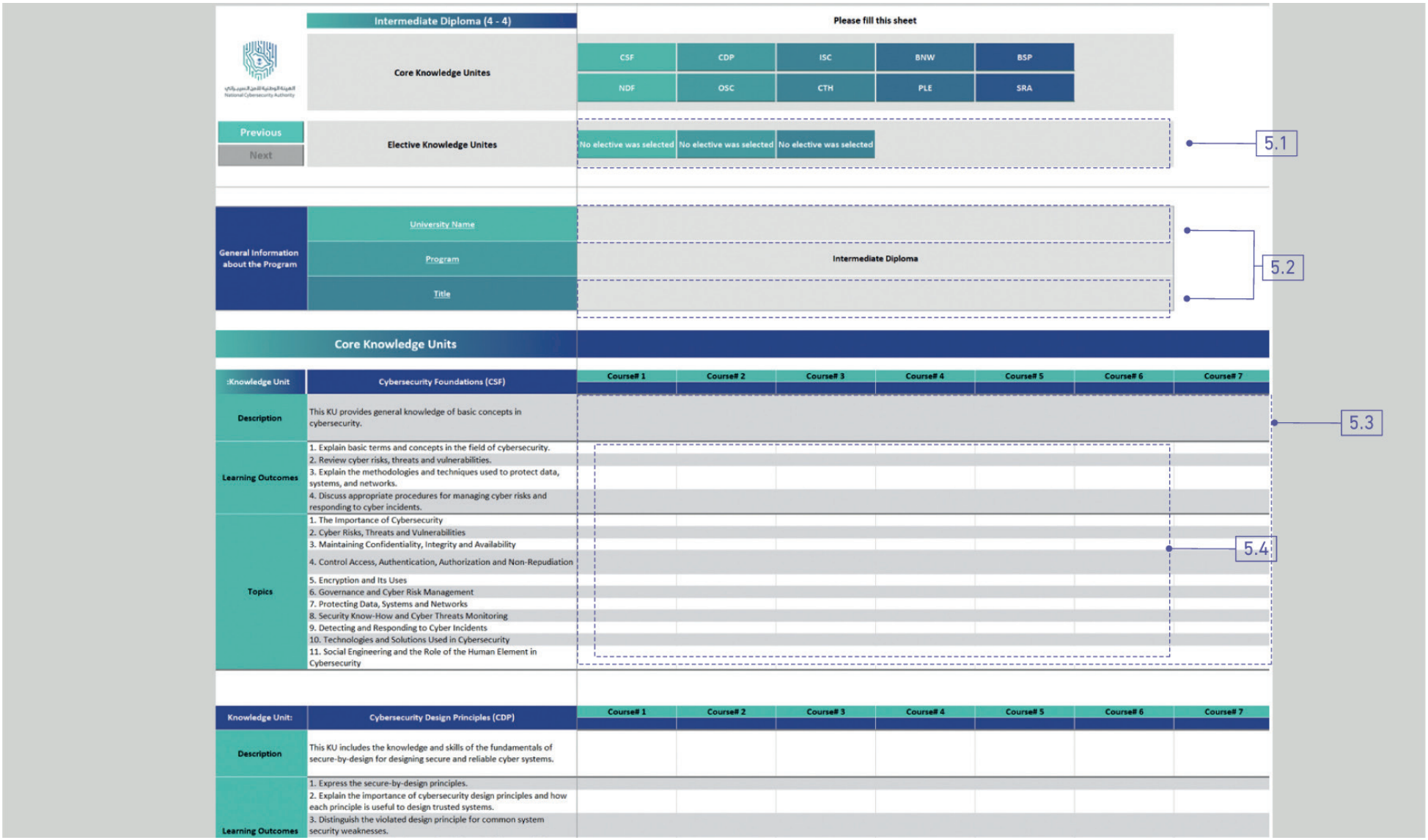
٥. أوراق عمل برامج التعليم العالي في الأمن السيبراني (مثال: برنامج الدبلوم المتوسط)

٥-١. تُعبأ تلقائيًا من مدخلات خطوة ٤-٧ بورقة عمل المواءمة (Alignment).

٥-٢. تُعبأ تلقائيًا من مدخلات خطوة ٢-١ بورقة عمل معلومات البرنامج العامة (Program General Information).

٥-٣. تُعبأ تلقائيًا من مدخلات خطوة ٣ بورقة عمل (Program Courses)، وعرضها كقوائم منسدلة من نواتج تعلم المقررات ومواضيعها.

٥-٤. ربط نواتج التعلم ومواضيع المقررات للبرنامج المعني حسب استيفائها لنواتج تعلم ومواضيع الوحدات المعرفية للبرنامج المقابل بإطار سايبر-التعليم.



Intermediate Diploma (4 - 4)

Please fill this sheet

Core Knowledge Unites: CSF, CDP, ISC, BNW, BSP, NDF, OSC, CTH, PLE, SRA

Previous / Next

Elective Knowledge Unites: No elective was selected | No elective was selected | No elective was selected

5.1

General Information about the Program

University Name

Program: Intermediate Diploma

Title

5.2

Core Knowledge Units

:Knowledge Unit	Cybersecurity Foundations (CSF)	Course# 1	Course# 2	Course# 3	Course# 4	Course# 5	Course# 6	Course# 7
Description	This KU provides general knowledge of basic concepts in cybersecurity.							
Learning Outcomes	1. Explain basic terms and concepts in the field of cybersecurity.							
	2. Review cyber risks, threats and vulnerabilities.							
	3. Explain the methodologies and techniques used to protect data, systems, and networks.							
	4. Discuss appropriate procedures for managing cyber risks and responding to cyber incidents.							
Topics	1. The Importance of Cybersecurity							
	2. Cyber Risks, Threats and Vulnerabilities							
	3. Maintaining Confidentiality, Integrity and Availability							
	4. Control Access, Authentication, Authorization and Non-Repudiation							
	5. Encryption and Its Uses							
	6. Governance and Cyber Risk Management							
	7. Protecting Data, Systems and Networks							
	8. Security Know-How and Cyber Threats Monitoring							
	9. Detecting and Responding to Cyber Incidents							
	10. Technologies and Solutions Used in Cybersecurity							
	11. Social Engineering and the Role of the Human Element in Cybersecurity							

5.3

5.4

Knowledge Unit:	Cybersecurity Design Principles (CDP)	Course# 1	Course# 2	Course# 3	Course# 4	Course# 5	Course# 6	Course# 7
Description	This KU includes the knowledge and skills of the fundamentals of secure-by-design for designing secure and reliable cyber systems.							
Learning Outcomes	1. Express the secure-by-design principles.							
	2. Explain the importance of cybersecurity design principles and how each principle is useful to design trusted systems.							
	3. Distinguish the violated design principle for common system security weaknesses.							

الرجاء إرسال النموذج وأسئلتكم واستفساراتكم حول المواءمة مع إطار «سايبر-التعليم» إلى:

scyber-edu@nca.gov.sa


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority