



Alignment Guide for the Saudi Cybersecurity Higher Education Framework (SCyber-Edu)

In The Name Of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White – No Restriction

Table of Contents

Introduction	7
SCyber-Edu Objectives	9
SCyber-Edu Alignment process	9
SCyber-Edu Alignment Form	14
Steps of Filling the Alignment Form	15

Introduction:

The National Cybersecurity Authority (NCA) is mandated to “build the national cybersecurity workforce; to participate in developing education and training programs; to prepare professional standards and frameworks; and to develop and run professional assessment tests related to cybersecurity”. Therefore, and due to the importance of developing national high-quality academic programs in cybersecurity, the NCA has worked on the development of the “Saudi Cybersecurity Higher Education Framework (SCyber-Edu)” in cooperation and coordination with the Ministry of Education and the Education and Training Evaluation Commission.

The framework was developed by the NCA in cooperation and coordination with the Ministry of Education and the Education and Training Evaluation Commission.

SCyber-Edu is designed in alignment with the Unified Saudi Classification for Educational Levels and Specializations, the National Qualifications Framework (NQF) and the guidelines of the National Center for Academic Accreditation and Evaluation.

The framework can be used and applied to cybersecurity degree programs offered by public and private higher educational institutions in Saudi Arabia. It covers the program descriptors of the cybersecurity higher education degree programs, admission requirements, core knowledge units, and elective knowledge units, as illustrated in Figure 1.

	Intermediate Diploma	Bachelor (Cybersecurity Track)	Bachelor (Cybersecurity Major)	Higher Diploma for Non-IT Background	Higher Diploma for IT Background	Master	Doctoral
Admission Requirements	High school diploma or equivalent			Bachelor's degree	Bachelor's degree in cybersecurity, computer science or related fields	Master's degree in cybersecurity, computer science or related fields	
				English Proficiency			
Core Knowledge Units	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	If one or more Core KUs of the Bachelor (Cybersecurity Track) program are not completed prior to admission, they must be completed in the program of study of this degree program		Completion of a thesis or a project in a cybersecurity topic
Elective Knowledge Units	At least 3 elective KUs	At least 4 elective KUs	At least 8 elective KUs	At least 2 elective KUs	At least 8 elective KUs	At least 7 elective KUs	At least 3 elective KUs
				It is recommended that elective KUs are limited to ones that cover relatively advanced topics			

Figure 1 . Summary of Admission Requirements, Core KUs and Elective KUs for all programs

SCyber-Edu Objectives:

- 1. To be a guide that can be used for developing, evaluating and accrediting cybersecurity higher education degree programs.
- 2. To set the minimum curriculum requirements of cybersecurity higher education degree programs to assure their academic quality and ensure that higher education degree programs in Saudi Arabia develop highly qualified cybersecurity professionals.
- 3. To align cybersecurity higher education degree programs' outcomes with the national need.

SCyber-Edu Alignment Process:



Self-Assessment



Arbitration



Alignment Verdict

SCyber-Edu Alignment Process:



1. Self-Assessment



1.1 Fill

The educational institute completes the alignment form, available at <https://nca.gov.sa/en/pages/scyberedu.html>



1.2 Share

Through scyber-edu@nca.gov.sa, the educational institute sends a request to align with the Saudi Cybersecurity for Higher Education (SCyber-Edu), with the following details:

- Program Name
- Degree program
- Credit hours
- The filled alignment form
- Information of the Communication Contact



1.3 Initial assessment

- The NCA conducts a preliminary assessment for the alignment application and review the provided alignment form.
- The NCA shares the feedback on the provided form with the educational institute, and requests the supporting documents.

SCyber-Edu Alignment Process:



1. Self-Assessment



1.4 Update

The educational institute updates the alignment form according to the feedback, and share the following through scyber-edu@nca.gov.sa, with the following consideration:

- The updated alignment form
- The supporting documents, while considering the following:
 - Attachments size 10 megabytes or less, and in case the documents' size exceed 10 megabytes, they can be shared in consecutively through email.
 - Acceptable extensions are (.PDF, .docx, .xlsx and .7z).

SCyber-Edu Alignment Process:



2. Arbitration



2.1 Review

- The NCA reviews the updated alignment form along with the supporting documents.



2.2 Arbitration

- The NCA team shares the updated alignment form along with the supporting documents, with independent arbitrators, to prepare the alignment report.
- The arbitrators share the alignment report with the NCA team.
- The final alignment report for the alignment verdict is prepared based on the arbitrators' reports.

SCyber-Edu Alignment Process:



3. Alignment Verdict

The NCA team shares the alignment report with the educational institute, and the alignment verdict's levels are as follows:



3.1 “Aligned”:

- The NCA issues an alignment certificate that is valid for five years.
- The program is added as an aligned program in the NCA's website.



3.2 “Provisionally Aligned”:

- The NCA team asks the educational institute to develop a treatment plan to resolve the program's alignment shortcomings with the SCyber-Edu framework.
- The educational institute shares the shortcomings treatment plan with the NCA team, and commits to execute it within a year.
- The NCA issues an alignment certificate that is valid for a year.
- The program is added as a provisionally aligned program in the NCA's website.



3.3 “Not Aligned”:

- The NCA team asks the educational institute to resolve the shortcomings stated in the report.
- The educational institute can submit an application to align the program with the SCyber-Edu framework after a year of the previous request.

SCyber-Edu Alignment Form

Form Components:

[Cover Page](#) | [Program General Information](#) | [Program Courses](#) | [Alignment](#)

[Intermediate Diploma](#) | [Bachelors \(Cybersecurity Track\)](#) | [Bachelors \(Cybersecurity Major\)](#)

[Higher Diploma \(IT Background\)](#) | [Higher Diploma \(Non-IT Background\)](#) | [Masters](#) | [Doctoral](#)

1. Cover Page
2. Program General Information Sheet
3. Program Courses Sheet
4. Alignment Sheet
5. Cybersecurity higher education programs sheets as defined by SCyber-Edu:
 - a. Intermediate Diploma
 - b. Bachelor (Cybersecurity Track)
 - c. Bachelor (Cybersecurity Major)
 - d. Higher Diploma for IT Background
 - e. Higher Diploma for Non-IT Background
 - f. Master
 - g. Doctoral

Note: It is required to fill the alignment form independently per cybersecurity higher education program, even if these programs belong to the same educational institute.

Steps of Filling the Alignment Form:

1. Cover Page

1.1 Click on “Start” button.



2. Program General Information Sheet

- 2.1. Enter general program information (Educational Institute Name, Program Degree, Program Title, Program Period , Number of Courses, Total Credit Hours, and Program Summary).
- 2.2. Enter program admission requirements.
- 2.3. Enter program learning outcomes.
- 2.4. Click on “Next” button.

The screenshot shows a web-based application for program submission. At the top right is the National Cybersecurity Authority logo. Below it is a header bar with 'Previous' and 'Next' buttons. The main title is 'Program General Information (1 - 4)'. The first section, 'General Information about the Program', contains fields for 'University Name' (empty), 'Program' (dropdown menu showing 'Please select a program'), 'Title' (empty), 'Period (in years)' (empty), 'Number of Courses' (empty), and 'Total Credit Hours' (empty). A 'Program Summary' section is present. The second section, 'Index', lists items 1 through 5 under 'General Information about the Program' and items 1 through 8 under 'Program Learning Outcomes (PLOs)'. The third section, 'Other', is also listed under 'General Information about the Program'. A dropdown menu for the 'Program' field is open, listing the following options:

- Please select a program
- Intermediate Diploma
- Bachelors (Cybersecurity Track)
- Bachelors (Cybersecurity Major)
- Higher Diploma (IT Background)
- Higher Diploma (Non-IT Background)
- Masters
- Doctoral

3. Program Courses Sheet

- 3.1. Enter the program's courses information, per course (Course Type -Core or elective-, Course Code, Course Name, and Description)
- 3.2. Enter the course learning outcomes, per course.
- 3.3. Enter the course topics, per course.
- 3.4. Click on “Next” button.

The screenshot shows the 'Program Courses (2 - 4)' section of the alignment guide. The interface includes a header with a logo and navigation links (Previous, Next, Course Index). The main area displays a table with columns for Course Type (Core/Elective), Course Code, Course Name, Description, and CLO Number (1-20). A modal window is open over the table, prompting the user to 'Please select an answer' between 'Core' and 'Elective'. The table rows for CLO numbers 1 through 20 are visible as light gray horizontal bars.

Program Courses (2 - 4)				
Course Type (Core/Elective)	1	2	3	4
Course Code				
Course Name				
Description	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	13			
	14			
	15			
	16			
	17			
	18			
	19			
	20			
Remarks				

Course Learning Outcomes (CLOs)

CLO Number

Course Topics (CT)

CT Number

Please select an answer
Core
Elective

Cover Page | Program General Information | **ProgramCourses** | Alignment | Intermediate Diploma | Bachelors (Cybersecurity Track) | Bachelors (Cybersecurity Major) | Higher Diploma (IT Background) | HigherDiplom

4. Alignment Sheet

- 4.1. Automatically filled from step 2.1 entries in ‘Program General Information’ sheet.
- 4.2. Automatically filled from the corresponding program’s requirements in the SCyber-Edu framework.
- 4.3. Link the program’s admission requirement(s), by selecting the coverage status, and/or checking against the number(s) of the admission requirement(s), that meet the corresponding program in the SCyber-Edu framework’s admission requirements.
- 4.4. Link the program’s program learning outcomes, by selecting the coverage status, and/or checking against the number(s) of the program leaning outcome(s), that meet the corresponding program in SCyber-Edu’s program leaning outcomes.

4.1

Alignment (3 - 4)						
General Information about the Program	University Name	Program	Title	Period (in years)	Total Credit Hours	Summary
	No program was selected					

4.2

SCyber-Edu Admission Requirements		Coverage Status	Program Admission Requirements								Remarks								
			1	2	3	4	5	Other	1	2		3	4	5	6	7	8		
SCyber-Edu Program Descriptors		Coverage Status									Program Learning Outcomes (PLOs)								Remarks
Knowledge																			<input checked="" type="checkbox"/>
Skills																			<input checked="" type="checkbox"/>
Values, Autonomy and Responsibility																			<input checked="" type="checkbox"/>

4.3

Please select an answer
Covered by strict admission requirements
Not covered

4.4

Please select an answer
Covered
Not covered

Cover Page | **Program General Information** | **Program Courses** | **Alignment** | **Intermediate Diploma** | **Bachelors (Cybersecurity Track)** | **Bachelors (Cybersecurity Major)** | **Higher Diploma (IT Background)** | **Higher Diploma (Non-IT Background)**

- 4.5. Link the program's mathematics requirements, by selecting that the coverage status, and/or selecting the course code(s), that meet the corresponding program in SCyber-Edu's mathematics requirements.
- 4.6. Automatically filled from the corresponding program's core knowledge units in the SCyber-Edu framework.
- 4.7. Link the program's courses with the SCyber-Edu framework's core knowledge units, by selecting the coverage status, and/or selecting the course code(s), that meet the requirements of the core knowledge units of the corresponding program in the SCyber-Edu framework.
- 4.8. Choose the elective knowledge units from the dropdown list of the program's corresponding elective knowledge units.
- 4.9. Link the program's courses with the SCyber-Edu framework's elective knowledge units, by selecting the coverage status, and/or selecting the course code(s), that meet the requirements of the elective knowledge units of the corresponding program in the SCyber-Edu framework.
- 4.10. Click on "Next" button.

 National Cybersecurity Authority

Previous Next

Alignment (3 - 4)

Skills								
	4.10		4.11		4.12		4.13	
Values, Autonomy and Responsibility	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>							
SCyber-Edu Mathematics Requirements	Coverage Status	Course Code(s)		Remarks				
SCyber-Edu Core Knowledge Units	Coverage Status	Course Code(s)		Remarks				
SCyber-Edu Elective Knowledge Units	Coverage Status	Course Code(s)		Remarks				

4.2 → 4.5
4.6 → 4.7
4.8 → 4.9

[Cover Page](#) | [Program General Information](#) | [Program Courses](#) | **Alignment** | [Intermediate Diploma](#) | [Bachelors \(Cybersecurity Track\)](#) | [Bachelors \(Cybersecurity Major\)](#) | [Higher Diploma \(IT Background\)](#) | [Higher Diploma \(Non-IT\)](#)

5. Cybersecurity Higher Education Sheets (e.g. Intermediate Diploma)

- 5.1. Automatically filled from step 4.7 entries in ‘Alignment’ sheet.
- 5.2. Automatically filled from step 2.1 entries in ‘Program General Information’ sheet.
- 5.3. Automatically filled from step 3 entries in ‘Program Courses’ sheet, and displayed as a dropdown list of course learning outcomes and course topics.
- 5.4. Link the program’s course learning outcomes and the course topics that meet the corresponding program’s course learning outcomes and the course topics in the SCyber-Edu framework.

		Intermediate Diploma (4 - 4)		Please fill this sheet				
		Core Knowledge Units		CSF	COP	ISC	BNW	BSP
		NDF	OSC	CTH	PLE	SRA		
General Information about the Program	University Name							
	Program	Intermediate Diploma						
	Title							
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	<ol style="list-style-type: none"> Explain basic terms and concepts in the field of cybersecurity. Review cyber risks, threats and vulnerabilities. Explain the methodologies and techniques used to protect data, systems, and networks. Discuss appropriate procedures for managing cyber risks and responding to cyber incidents. <ol style="list-style-type: none"> The Importance of Cybersecurity Cyber Risks, Threats and Vulnerabilities Maintaining Confidentiality, Integrity and Availability Control Access, Authentication, Authorization and Non-Repudiation Encryption and Its Uses Governance and Cyber Risk Management Protecting Data, Systems and Networks Security Know-How and Cyber Threats Monitoring Detecting and Responding to Cyber Incidents Technologies and Solutions Used in Cybersecurity Social Engineering and the Role of the Human Element in Cybersecurity 							
Topics								
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	<ol style="list-style-type: none"> Express the secure-by-design principles. Explain the importance of cybersecurity design principles and how each principle is useful to design trusted systems. Distinguish the violated design principle for common system security weaknesses. 							

Please send your form and any questions or queries about the alignment with the Scyber-Edu framework to:

scyber-edu@nca.gov.sa



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority