Training Guide
Generative AI and Developing a Cybersecurity Curriculum Based on NIST NICE Framework and JNSA SecBok

---

1. Background

The rapid advancement of digital technologies has created new demands for both cybersecurity professionals and higher education institutions. **Generative AI** is becoming an important tool for improving cybersecurity-related tasks, while the growing demand for skilled cybersecurity professionals requires universities to develop curricula aligned with international standards.
This five-day training consists of two independent modules. The first module provides practical knowledge and hands-on experience in applying **Generative AI** to cybersecurity. The second module introduces a practical methodology for developing cybersecurity curricula based on **National Institute of Standards and Technology (NIST) NICE Framework** and **Japan Network Security Association (JNSA) SecBok**.

---

2. Objective

Participants will learn how to:

[Generative AI Module]

- Understand **Generative AI** and Large Language Models.
- Utilize AI platforms for cybersecurity tasks.
- Compare general purpose and security focused AI platforms.
- Apply AI to documentation, awareness, and planning.

[Cybersecurity Curriculum Development Module]

- Confirm the general process of university curriculum development.
- Apply **NICE Framework v2** to identify cybersecurity workforce roles and their associated Tasks, Knowledge, and Skills (TKS).
- Apply **SecBok 2025** to identify cybersecurity knowledge areas.
- Design a cybersecurity curriculum structure.
- Develop individual course specifications.

---

3. Target Participants

This training is intended for:

- University faculty members
- Curriculum developers
- Academic program coordinators
- Government officials responsible for higher education
- Cybersecurity education managers

---

4. Training Information

Item	Description
Training Title	Generative AI and Developing a Cybersecurity Curriculum Based on NIST NICE Framework and JNSA SecBok
Date	July 09, 10, 13, 14, 15 (5 Days)
Time	09:00–17:00 (Registration begins at 08:30)
Organizer	**Japan International Cooperation Agency (JICA)** and **Department of Information and Communications Technology – Cybersecurity Bureau (DICT-CSB)**, Republic of the Philippines

Item	Description
Venue	B Hotel Quezon City
Meeting Mode	Hybrid (Offline + Online)
Online Meeting Link	https://meet.google.com/tax-mbgg-yfb
Language	English

5. Training Agenda

[Generative AI Module] 2 Days

DAY1: July 09, Thursday: Understanding Generative AI and AI-Assisted Cybersecurity

Start	End	Topic
09:00	9:15	Opening & Welcome
09:15	9:25	Why This Matters
09:25	9:40	Roadmap & Pre-Survey
09:40	10:20	**Module 1 - Intro to GenAI & LLMs**
10:20	10:55	Exercise 1 - Infographic
10:55	11:25	Exercise 2 - Audio Overview
11:25	11:40	Coffee Break
11:40	12:20	**Module 2 - AI Platform Landscape**
12:20	1:20	Lunch Break
13:20	13:55	Exercise 3 - Frontier Platforms
13:55	15:00	Exercise 4 - Local AI (Hermes)
15:00	15:15	Coffee Break
15:15	16:00	**Module 3 - Real Cyber Threats from AI**
16:00	16:30	Exercise 5 - Gandalf
16:30	17:00	Exercise 6 - Awareness Video

DAY2: July 10, Friday: Practical Applications of Generative AI in Cybersecurity

Start	End	Topic
09:00	9:05	Day 2 Opening
09:05	9:50	**Module 4 - Red Team with AI**
09:50	10:30	Exercise 7 - AI VAPT (online)
10:30	10:45	Coffee Break
10:45	12:00	Exercise 8 - AI VAPT (Hermes)
12:00	13:00	Lunch Break
13:00	13:45	**Module 5 - Blue Team with AI**
13:45	14:25	Exercise 9 - Install XORCISM
14:25	15:05	Exercise 10 - CISO for a Day
15:05	15:20	Coffee Break
15:20	16:00	**Module 6 - Build Your Career with Ikigai**
16:00	16:25	Exercise 11 - Ikigai Diagram
16:25	16:50	Exercise 12 - Profile Website
16:50	17:00	Post-Survey & Close

[Curriculum Development Module] 3 Days

DAY3: July 13, Monday: Introduction to Curriculum Development and Designing the Curriculum Structure

Start	End	Topic
9:15	9:30	Overview of University Curriculum Development Process **(Including Common Pitfalls to Avoid)**
9:30	9:45	Overview of Curriculum Development Best Practices — Outcome-Based Education (OBE), Bloom's Taxonomy, and Constructive Alignment **(Aligning ILOs, TLAs, and ATs)**
9:45	10:05	Case Study: ACM/IEEE Computer Science Curricula (CS2023) — Purpose, Structure, Knowledge Areas, **Competency Model**, and Curriculum Development Example
10:05	10:15	Discussion: Applying International Curriculum Guidelines to Cybersecurity Education
10:15	10:30	Coffee Break
10:30	11:00	Introduction to NICE Framework v2 — Cybersecurity Workforce Roles and Tasks, Knowledge, and Skills (TKS)
11:00	11:30	Introduction to SecBok 2025 — Organizing Cybersecurity Knowledge Areas
11:30	12:00	Exercise 1: **Needs Analysis Refresher** & Defining the Graduate Profile, Program Educational Objectives (PEOs), and Program Learning Outcomes (PLOs)
12:00	13:00	Lunch Break
13:00	13:30	Identifying Target Workforce Requirements Using NICE Work Roles
13:30	14:00	Identifying Required Cybersecurity Knowledge Areas Using SecBok 2025
14:00	14:30	Selecting Core Courses and Elective Courses
14:30	15:15	Exercise 2: Designing the Curriculum Structure
15:15	15:30	Coffee Break
15:30	16:30	Group Presentations and Discussion
16:30	17:00	Summary of Day 1 and Preparation for Course Development

DAY4: July 14, Tuesday: Individual Course Development and Curriculum Integration

Start	End	Topic
9:00	9:30	Methodology for Developing Role-Oriented Cybersecurity Courses
9:30	10:00	Using NICE Work Roles and TKS as References for Course Design
10:00	10:30	Using SecBok Knowledge Areas to Define Course Contents
10:30	10:45	Coffee Break
10:45	12:00	Exercise 3: Developing a Course Specification
12:00	13:00	Lunch Break
13:00	13:30	Reviewing Workforce Alignment Using NICE Framework v2
13:30	14:00	Reviewing Curriculum Coverage Using SecBok 2025
14:00	15:00	Exercise 4: Curriculum Review and Gap Analysis
15:00	15:15	Coffee Break
15:15	16:15	Group Presentations
16:15	16:45	Instructor Feedback and Discussion
16:45	17:00	Post-Survey and Closing Remarks

DAY5: July 15, Wednesday: Discussion on Philippine Cybersecurity Curriculum and Education

Start	End	Topic
9:00	10:30	Philippine Cybersecurity Curriculum Discussion
10:30	10:45	Coffee Break
10:45	12:00	Continuation of the Discussion
12:00	13:00	Lunch Break
13:00	15:00	Drafting Recommendations for the Philippine Cybersecurity Curriculum
15:00	15:15	Coffee Break
15:15	16:15	Summary of Key Recommendations and Way Forward
16:15	16:45	Closing Remarks (DICT / JICA / Experts)
16:45	17:00	Certificate Distribution and Photo Session

6. Others

(1) Participants must join the online meeting using the designated link.
(2) Participants are requested to bring a laptop computer to be used for:
- Generative AI hands-on exercises
- Curriculum design exercises
- Preparing presentation materials
- Group discussions
- Group presentations

(3) Participants who achieve an attendance rate of 75% or higher across the five-day schedule will be awarded a **certificate of completion** issued by the **Department of Information and Communications Technology (DICT)** and the **Japan International Cooperation Agency (JICA)**. Attendance is calculated based on 10 total units across the five days, with the morning and afternoon sessions each counting as one unit; therefore, attendance of at least seven units is mandatory.