Assessment Instruction

Competency: SEC-201: Data Privacy, Security, and Integrity

General Information

Competency Code:	SEC-201
Competency Name:	Data Privacy, Security, and Integrity
Semester:	-
Instructor:	Charnon Pattiyanon, Ph.D.

Competency Overview

Data is one of the most valuable assets in modern software systems, often containing sensitive or personal information that must be protected to uphold the reputation and trustworthiness of these systems. Ensuring data privacy, security, and integrity are essential principles in effective data protection.

In this competency, we explored three critical aspects of data protection. First, we will examine existing issues and the principles that should be prioritized. Then, we delve into specific techniques and methods used to safeguard data privacy, security, and integrity, equipping you with the skills to analyze and design modules that ensure robust data protection. Additionally, this competency introduced the concepts of data governance, including an overview of relevant laws and regulations for data privacy. By the end of this competency, you will have the knowledge and skills to handle data responsibly, ensuring security, integrity, and privacy in all aspects of data manipulation.

Assessing Skills

- **[SEC-201:00010] Analyze the sensitivity of data and information** – Successful students must be able to identify the sensitivity of data and information used in a software system.
- **[SEC-201:00020] Analyze the secure data and information processing** – Successful students must be able to design and evaluate secure data processing activities.
- **[SEC-201:00030] Evaluate data security in an information system** – Successful students must be able to implement data security techniques, such as encryption and secure key exchange, in a practical system.
- **[SEC-201:00040] Evaluate data integrity in an information system** – Successful students must be able to implement data integrity techniques, such as message authentication and digital signatures, in a practical system.

- **[SEC-201:00050] Evaluate data privacy preservation mechanisms in an information system** – Successful students must be able to apply data privacy preservation mechanisms, such as data anonymization and conditional privacy, in a practical system.
- **[SEC-201:00060] Analyze the compliance of data privacy laws and regulations** – Successful students must be able to understand, analyze, and suggest the compliance of a practical system to a data privacy laws and regulations.

Pre-cautions

- Please ensure that your answers to each part of the required outcomes are expressed in your own words and perspectives. **Plagiarism is strictly prohibited**. If there is evidence that content or ideas are significantly similar between two or more students without valid justification, the scores of all involved students will be deducted as a penalty for academic misconduct.
- Students are expected to demonstrate a deep understanding of the subject matter by applying **critical analysis and original insights**. Overreliance on AI-generated content without meaningful personal input will negatively affect the assessment score.
- Each response in your assessment should be written in a **"why" style**, where you provide justifications to explain the reasoning behind your answers. For example: *"I believe this privacy principle applies to the target system because …"*. There is no single "correct" solution or criticism; instead, your analytical and reasoning skills will be evaluated based on the clarity and depth of your justifications.
- You are encouraged to ask questions to satisfy your curiosity about the assessment through email or the Canvas discussion page. However, please do not submit your assessment report for feedback. According to the submission policy, feedback will only be provided on formally submitted reports.
- You are allowed to use AI tools for writing (e.g., proofreading or grammar correction), but you must provide clear evidence that you have included your own original ideas in the report. If you fail to provide reasonable evidence at the time of submission, your score will be deducted, as your skills cannot be properly assessed.

Submission Policy

- You are allowed to submit your work only once per semester. You may submit your work and then request feedback from the instructor. However, it is at the instructor's discretion whether to provide feedback.
- All submissions must be completed **through the Canvas system only**, as your scores need to be stored and transferred to the university's system. Submissions made via any other channel will not be recognized as official, and you will not receive a score for your work.

- At the end of each semester, **CMKL University** sets a deadline for students to submit their assessments for all enrolled competencies. If you fail to submit your work by the stated deadline, you will not receive any score. In such cases, you must retake the competency in future semesters. While you may submit a request for consideration of a late submission, approval is subject to the instructor's discretion and the university's operational constraints.

Assessment Instruction

1. Select **a target information-processing system** for your assessment and implement security, privacy, and integrity protection mechanisms. The chosen system must satisfy the following qualifications:
   a. The system may be either an existing application (which you can replicate as a command-line program) or a new system you intend to implement; examples include chat applications, file-sharing systems, or registration systems.
   b. The system must store, manipulate, display, and transmit data to deliver functionality to users.
   c. The system should include multiple components and support data communication among components to demonstrate protection mechanisms during transmission.
   d. For simplicity, the system must be implementable at minimum as a command-line interface (CLI) program.
2. Write a PDF report following the given template and submit it to the instructor via email (charnon@cmkl.ac.th).

Important Dates for the Assessment

- **Submission Deadline for Assessment Report to Request Feedback:** October 20, 2025, 11:59PM
- **Submission Deadline for Assessment Report:** November 28, 2025, 11:59PM

*** Note:** For this competency only, students who submit the assessment report before the first deadline will receive initial feedback on their report in around 1 week after the deadline. They will then have the opportunity to revise their report to improve their score. Submissions made after the first deadline will be graded only at the end of the semester and will not have the chance for revision.

Assessment Report

SEC-201: Data Privacy, Security, and Integrity

By

[Your First Name] [Your Last Name] ([Your Nickname])

[Your Email Address]

General Information of the Chosen System

System Name: [Put your chosen system's name here]

System Description:

Write a section (minimum of one paragraph) to describe the chosen system. This section must describe the high-level overview of the system functionality and architecture. At least this section must answer the following questions:

- What is the chosen information processing system?
- What are the main purposes and/or objectives, in term of functionality, that the chosen system should deliver?
- What are data objects being processed in the chosen system? Are they sensitive?
- What type of system architecture is being used by the chosen system? How many components distributed in the chosen system architecture?

A contextual diagram may be optionally included in this section to illustrate an overview of the system architecture.

System Development Information

Data Structure and Analysis:

Write a section (minimum of one paragraph) to describe about the data structure of the chosen system. This section must include a list of data objects with their sensitivity. The following template may be used to guide the writing of this section, but not limited to:

List of Data Objects:

Name	Description	Sensitivity?	Personal?	Justification
Username	An account identifier that each user must have.	No	Yes	It can be used to uniquely identify a person. However, I don't think it is sensitive because its sole exposure would not harm the data owner.
…	…	…	…	…

Security, Privacy, and Integrity Protection Mechanisms:

Write a section (minimum of one paragraph) describing the data security, privacy, and integrity protection mechanisms used in the implementation of the chosen system. You may select techniques discussed during the lecture or other relevant methods. Each technique must be explained in your own words, with a clear description that allows readers with no prior knowledge of these concepts to understand them easily. You may also include figures or illustrations to enhance clarity.

Source Code Implementation:

Write a section to describe each segment of the source code you implemented for the chosen system. The source code can be a simple Command-Line Interface (CLI) program demonstrating secure, privacy-preserved, and data integrity ensuring data manipulation and transmission. Each code segment must include a caption describing its purposes and how it functions.

Example:

```
import numpy as np
user_arr = np.array([“John1”, “Smith007”])
```

This code segment shows an initialization of an array for usernames using the well-known NumPy package. This will store the array in the **`user_arr`** variable.

Execution Screenshots:

Provide a collection of screenshots demonstrating the execution of the implemented system. These screenshots must provide sufficient evidence to the instructor that you have successfully and correctly implemented security, privacy, and integrity protection techniques. In addition, you must include a short description for each execution screenshot to explain it in detail.

Compliance Analysis

Compliance Target and Justification:

Choose one of the following laws, regulations, or technical standards:

- California Consumer Privacy Act (CCPA),
- EU General Data Protection Regulation (GDPR),
- Thailand’s Personal Data Protection Act (PDPA), or
- ISO/IEC 29100:2024 Information Technology – Security Techniques – Privacy Framework.

You may also choose other privacy-related laws, regulations, or technical standards if you find them more suitable for the target system. Then, write a paragraph justifying why you selected the chosen document in this case.

List of Security/Privacy Controls from the Compliance Target:

List all security and privacy controls provided by the compliance target document, including a detailed description of each control and an example of a situation where a system complies with the control. You may use the following table as a template, though you are not limited to it:

Control	Description	Example
Data Minimization	A system collects and processes only the personal data that is adequate, relevant, and limited to what is necessary for the specific, stated purposes of the processing.	An HR system collects an employee's name, home address, and email address but does not collect information about their partner or health insurance details.
…	…	…

List of Security/Privacy Requirements for Compliance:

Based on the security and privacy controls listed in the previous section, list all security and privacy requirements necessary to ensure that the chosen system you implemented complies with the compliance target document.