# Introduction to Smart Data Security Module

***Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)***

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.

***The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)***

- #7: Information Hiding

***Description:***

This module presents an easy-to-understand introduction to fundamentals of information security by utilizing a case study. Participants will learn about key information security concepts such as those listed below:

Smart Data (SD) analyzes data for a global market. Up to this point it has never had an information security department. They are hiring you as their first Information Security Manager. You must set up the department and make sure that SD is prepared to deal with the risks and challenges faced by the company. Please work in teams of two or three and look your answers up on the Internet. There may not be a "right" answer but as a manager you will face numerous options. Be prepared to justify your solution and explain why it is the best choice.

1. What are the immediate challenges that the company faces?
2. What are the challenges that you will face in your role as Security Manager?
3. Use the AIC triad and list some important security considerations that the company faces.
4. How important is Senior Management Support and why?
5. In your security plan, what should be addressed in the initial security statement?
6. How can you create a new security culture within SD?
7. What cultural problems are you going to face in establishing a security program?
8. What security concepts may be violated at SD currently that should be addressed?
9. There are many different operating systems being utilized; how will you address this problem?
10. What are the advantages and disadvantages of solving the multiple OS problem?
11. Define a procedure from a security perspective and describe the main intent.
12. What is a policy and how is it implemented?
13. From a HR perspective list some good practices related to hiring and firing.
14. What is the role of an information custodian?
15. What are the primary risks that you see as facing SD?
16. What are some sources of threats to SD?

17. What areas should be included in the ethics statement for SD, from a security perspective?

SD recently acquired a small company and their network has been pieced together from several initiatives. As security manager you must prepare a security review and recommend initiatives.

1. What is the primary security requirement of a network?
2. What are the main network security requirements?
3. What would be the benefits and security risks of a VOIP system to SD?
4. Why would SD decide to install Wireless Access Points (WAP)?
5. What precautions should be taken before installing WAP?
6. Define jitter, latency and Quality of Service (QoS).
7. If SD sets up a website to make payments directly, then what precautions need to be taken?
8. What is MLPS and what benefits and risks does it offer compared to a leased line solution?
9. How can SD obtain a QoS level that is better than a packet-switched network?
10. What are the two things that an analog signal varies?
11. How do you indicate the beginning and end of asynchronous communications?
12. What is the most reliable network structure?
13. What is radius and how is it used?
14. What is the most common method of providing secure communications?
15. What is the threat associated with DNS?
16. What are the major parts of SSL and TCP setups?
17. What are the three parts of Security Association?

***learner-centered classroom:***

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include basics of Internet and IUP Library research on cybersecurity issues.

***Assessment:***

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive answers to the case questions. For example, a carefully chosen set of questions on the covered topics can form a case quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contributes to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

***Suitability to various groups:***

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how these security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as advanced operating systems use. The contents will also advance in the level of difficulty when being presented to the Middle school group compared to when being presented to the High school students.

***How the Teachers and Students groups will be interacting:***

This module will not have explicit interacting among the three groups. But, the contents covered in the teachers group will primarily focus of how to integrating these security concepts in the K-12 curriculum. Also, input from the teachers will be sought on how to better deliver the module contents to the other two students groups. We also are planning a culminating competition-based activity among all three groups towards the end of the camp.