HOW TO MAKE GENERAL EMPLOYEES AWARE OF CYBERSECURITY

Course Syllabus

Cyber Security Professional Program

Subject Code: COM0020a / Version: 1.0

Updated on 29/09/2021

Official content of **idCARE.UI**
Indonesia Cyber Awareness and Resilience Center

Supported by **JICA**
Japan International Cooperation Agency

Course Syllabus

As of 29 Sept 2021

Course Title	**How to Make General Employees Aware of Cybersecurity**
Course goals	1. Describe the importance of information security and cybersecurity. 2. Identify common threats to information security and cybersecurity. 3. Plan and implement a comprehensive information security program.
Course Objective	1. Module 1: Able to explain the basic concepts of information security and international standards that are used as references in information security. 2. Module 2: Able to explain the basic concepts of cybersecurity and their relationship to information security. 3. Module 3: Able to explain the fundamentals of risks and vulnerabilities related to cybersecurity and information security. 4. Module 4: Able to explain the fundamentals of the incident response framework Able to explain how to identify and report incidents to the appropriate team/party. 5. Module 5: Able to explain the fundamentals of the cybersecurity awareness program. 6. Module 6: Able to explain how to design and develop an effective cybersecurity awareness program. 7. Module 7: Able to demonstrate the process of building and implementing an effective cybersecurity awareness program. 8. Module 8: Able to evaluate a cybersecurity awareness program.
Participants	1. Employees who are involved in the information security and cybersecurity awareness program. 2. Leaders or managers who are responsible to build and implement information security and cybersecurity awareness programs. 3. Consultants or IT professionals who are required to have a basic understanding of information security and cybersecurity awareness programs.
Prerequisites	The participants should have basic knowledge of Information Technology terminology.

Course contents and schedule 16 sessions (1session = 50min)	***Pretest*** **1. Module 1: Fundamentals of Information Security** (*Lecture, 90 minutes*) 1.1. Information: Definition, formats, lifecycle and risk 1.2. Introduction to information security 1.3. Importance of Cyber Security awareness 1.4. Information Security Management System (ISMS): Based on ISO/IEC 27001:2013 This module provides a basic introduction to information security. Starting from the understanding of information, its formats, life cycle, and risks related to the information cycle. The concept of information security and international standards related to information security, namely ISO 27001, will also be presented in this module. Course participants are expected to get an initial overview of the basic concepts of information security and understand international standards that are used as references in information security. ***Module 1 Test*** **2. Module 2: Fundamentals of Cybersecurity** (*Lecture, 95 minutes*) 2.1. Introduction to cybersecurity 2.2. Cybersecurity principles This module provides a basic introduction to cybersecurity. Starting from the understanding of cybersecurity, cybersecurity principles, cyber security-related infrastructure, and the risks associated with it. Course participants are expected to get an initial overview of the basic concepts of cybersecurity and their relationship to information security. Presentation and discussion (*hands-on, 45 minutes*) (Groups of participants will perform presentations and discussion for the subjects in Module 1 & Module 2) ***Module 2 Test*** **3. Module 3: Risks and Vulnerabilities** (*Lecture, 90 minutes*) 3.1. Basics of risk management 3.2. Threats and vulnerabilities 3.3. Cyber Attack 3.4. Case of Study

	This module will provide a basic introduction to the risk management process, especially those related to information security and cybersecurity. Types and examples of weaknesses and threats such as Phishing Scams, Viruses and Malware, Password managements, and how to deal with them are discussed in this module. Course participants are expected to gain an understanding of the risk management process, as well as to understand the weaknesses and threats that can occur related to cybersecurity and information security. ***Module 3 Test*** **4. Module 4: Incident Response** (*Lecture, 115 minutes*) 4.1. Incident response framework based on NIST.SP.800-61 Rev.2 4.2. How to Respond to a Cyber Security Incident for Employee 4.3. Disaster recovery and business continuity This module will discuss the incident management process, especially those related to information security and cybersecurity. The framework and examples of implementing incident management are also discussed in this module. In addition, it will also discuss material on disaster recovery and business continuity as a preventive measure for possible incidents that occur. Course participants are expected to gain an understanding of the incident management process, as well as to understand how to overcome it through a disaster recovery and business continuity framework. Presentation and discussion (*hands-on, 45 minutes*) (Groups of participants will perform presentations and discussion for the subjects in Module 3 & Module 4). ***Module 4 Test*** **5. Module 5: Introduction to Security Awareness Program** (*Lecture, 45 minutes*) 5.1. Background. 5.2. IT Security Learning Continuum. 5.3. Security Awareness Program Stages. This module will provide an introduction to the types of security awareness programs (awareness, training, education and professional development), as well as the stages starting from planning, implementing, monitoring and evaluating the effectiveness of the security awareness program. Course participants are expected to get an initial description of the steps that must be taken to implement a good security awareness program so that

	employee awareness of information security and cybersecurity can be increased. ***Module 5 Test*** **6. Module 6: Designing & Developing Security Awareness Program** (*Lecture, 135 minutes*) 6.1. Introduction Best practices of awareness on the threats learnt in Module 6 will be introduced. 6.2. Developing security awareness program ● Basics of teaching method and approaches ● High-tech and student-centered approach ● Instructor-led and simulation-based delivery method 6.3. Developing security awareness program ● How to find/modify/develop/utilize materials for raising CS awareness in accordance with PDCA cycle This module provides detailed steps for planning and developing an information security awareness program. In this module, a workshop will be held to design a security awareness program such as whether to conduct training, make posters, and so on. If training is to be carried out, it is also planned how the teaching methods will be delivered. Then it will also be explained how to find and develop the materials needed in this security awareness program. Course participants are expected to understand the process of planning and developing an information security awareness program, including trying to build simple security awareness materials. Presentation and discussion (*hands-on, 90 minutes*) (Groups of participants will perform presentations and discussion for the subject in Module 6). ***Module 6 Practice*** ***Module 6 Test*** **7. Module 7: Implementing Security Awareness Program** (*Lecture, 105 minutes*) 7.1. Implementing security awareness program This module will present the planning and implementation process of an information security awareness program that was designed and developed in the previous stage. Risk identification and anticipation steps during the implementation process also need to be prepared.

	Course participants are expected to understand the implementation process of an information security awareness program, including identifying and anticipating possible risks during the implementation process. Presentation and discussion (*hands-on, 90 minutes*) (Groups of participants will perform presentations and discussion for the subject in Module 7). ***module 7 Practice*** ***Module 7 Test*** **8. Module 8: Evaluating Security Awareness Program** (*Lecture, 105 minutes*) 8.1. Evaluating security awareness program This module will present the monitoring and evaluation process of the security awareness program being implemented, including plans for future improvements. The subject of evaluation includes measuring program effectiveness as well as measuring employee awareness of information security and cyber security based on NIST.SP.800-50. From this module course participants are expected to be able to understand the monitoring and evaluation process to measure the effectiveness of information security awareness and cybersecurity awareness programs Presentation and discussion (*hands-on, 90 minutes*) (Groups of participants will perform presentations and discussion for the subject in Module 8). ***Module 8 Test*** ***Post Test***
Scheme of Instructions	Lecture: 70 % hands-on training: 30 %
Keywords	Cybersecurity awareness, security awareness, security awareness training
Tools (software) required for hands-on training	Tools for hands-on training refer to website link such as: https://heimdalsecurity.com/blog/free-cyber-security-tools-list/
Reference	1. Eric C. Thompson, "Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents", Apress, 2018

2. Mark Ciampa, Ph.D., "Security Awareness: Applying Practical Security in Your World", Cengage Learning, 2017
3. Douglas Landoll, "The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments", RC Press, 2011
4. Nipon Nachin, Chatpong Tangmanee, Ph.D., Krerk Piromsopa, Ph.D., “How to Increase Cybersecurity Awareness”, ISACA Journal, 2019
5. ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary
6. ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements
7. ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls
8. NIST.SP.800-50 “Building an Information Technology Security Awareness and Training Program”, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
9. NIST.SP.800-61 Rev. 2 “Computer Security Incident Handling Guide”, URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
10. SANS Institute, ”Security Awareness Planning Toolkit”, URL: https://www.sans.org/security-awareness-training/demo/security-awareness-planning-kit
11. Security awareness free materials developed by:
    - 11.1. Id-SIRTII/CC, URL: https://idsirtii.or.id/index.html
    - 11.2. SANS Institute, URL: https://www.sans.org/security-resources/posters/
    - 11.3. Cybersecurity & Infrastructure Security Agency (CISA), URL: https://www.cisa.gov/national-cybersecurity-awareness-month-resources
    - 11.4. Cyber Safe Work, URL: https://cybersafework.com/free-security-posters/
    - 11.5. The University of California Santa Cruz, URL: https://its.ucsc.edu/security/poster.html
    - 11.6. Phising.org from KnowBe4, URL: https://www.phishing.org/phishing-posters