
	Department of Education Region III DIVISION OF CITY SCHOOLS Angeles City Jesus Street, Pulungbulu, Angeles City		Document Code: SDO-QF-OSDS-SDS-005 Revision: 00 Effectivity date: 10/31/2018
	DIVISION ADVISORY		Name of Office: OSDS-SDS

DIVISION ADVISORY

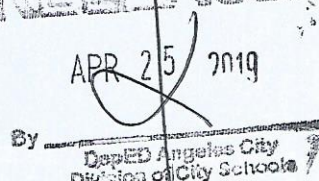
No. 112, S. 2019

To : Heads of Public Elementary and Secondary Schools

From : Schools Division Superintendent

Subject : Cyber Security Awareness and Breach Response Workshop


Date : April 25, 2019

RELEASED
 APR 25 2019
 By 
 DepEd Angeles City
 Division of City Schools

Please be informed that Yisrael Solutions and Consulting (YISCON) Inc. will conduct a training entitled Cyber Security Awareness and Breach Response Workshop to be held on the workshop schedules stated in the attached letter of invite.

Target participants to the training are the personnel in MIS, Web Developer, Technical Support, Network Admin, I.T., Technical Working Group and those who have access to personal data.

For information.


LEILANI S. CUNANAN, CESO V
 Schools Division Superintendent

lv/chiefsod

CH # 2019-118

"SMILES BRIGHT, SERVES RIGHT"

April 17, 2019

Leilani S. Cunanan, CESO VI
School Division Superintendent
Department of Education - Angeles City Division
Tel/Fax no. (045) 322-4106F / (045)322-5722 ; (045)322-4702
angeles.city@deped.gov.ph

SUBJECT: "CYBER SECURITY AWARENESS AND BREACH RESPONSE WORKSHOP"

Dear Mam/Sir:

Greetings!

We are pleased to invite you and your personnel in MIS, Web Developer, Technical Support, Network Admin, I.T., Technical Working Group and those who have access to personal data to attend to the Cyber Security Awareness and Breach Response Workshop to be held on the workshop schedules stated below.

With the evolving hacking events around us, we can see the news regarding organizations being hacked around the world. Despite investing millions of dollars on technology, many of them avoid human factor that is the weakest link in Cyber security. Organizations recruit employees in different departments, but they cannot assume that they have enough knowledge about to secure official and personal data. Hackers are using sophisticated techniques to breach the network & server to steal confidential information. At that point, security training seems helpful to create awareness in employees as well users/customers. It is the duty of an organization to make their customers aware about basic security precautions for a safe browsing experience.

Cyber security awareness workshop is essential to reduce the risk that employees exposed and tricked by sophisticated phishing or social engineering methods into serving unknowingly as entry points or worst, breach incidents that can affect organization information and data systems. This workshop could also help the company/agency to respond in a security breach and comply with the necessary notification requirements under the Philippine Data Privacy Act.

The primary objective of the security awareness program is to educate users on their responsibility to help protect the confidentiality, availability and integrity of their organization's information and information assets. The participants will be able know the state-of-the art information about Cyber Security, it's importance, good practices and benefits to the organization. Participants can have a view on different phases of security threats: System Hacking, Malware Threat, Sniffing, Social Engineering, DDOS Attack and How can they respond to them.

During the workshop, the speakers will also confer on Breach simulation briefing and simulation of attack and a Breach Notification Requirements of RA 10173, a deep discussion on breach notification requirements under the DPA and Circular 16-03 and additional information on RA 10175 "Cybercrime Act"

Participants will take their time to report the results of their investigation on the given breach simulation, both technical and compliance report that is why we encourage you to form or create a Breach Response team (minimum number or three (3) or more participants) to be headed by the Data Protection Officer (DPO) to attend and participate on the "Breach Response Team Report.

Below are the workshop schedules: (please choose your workshop options)

SESSION MODULES	LOCATION	TENTATIVE WORKSHOP SCHEDULES	Workshop Fee (Live-out)	Workshop Fee (Live-in)
DAY 1: <ul style="list-style-type: none"> MODULE 1 – INTRODUCTION TO CYBER SECURITY (Know the state-of-the art information about Cyber Security, it's importance, good practices and benefits to the organization). MODULE 2 – KNOWING THE ATTACK VECTORS (PART I) (Participants can have a view on different phases of security threats: System Hacking, Malware Threat, Sniffing, Social Engineering, DDOS Attack and How can they respond to them). DAY 2: <ul style="list-style-type: none"> MODULE 3 – KNOWING THE ATTACK VECTORS (PART II) (Continuation of discussion on phases of security threats: Hacking web servers, SQL Injection, Hacking Wireless Networks and Mobile Platforms) MODULE 4 – MANAGEMENT APPROACH: INCIDENT RESPONSE FRAMEWORK (The session will provide guidance and additional information on security incident response framework) MODULE 5 – BREACH AND LIVE-ATTACK SIMULATION (Breach simulation briefing and simulation of attack) DAY 3: <ul style="list-style-type: none"> MODULE 6 – BREACH NOTIFICATION REQUIREMENTS OF RA 10173 (A deep discussion on breach notification requirements under the DPA and Circular 16-03 and additional information on RA 10175 "Cybercrime Act") MODULE 7 – BREACH RESPONSE TEAM REPORT (PRESENTATION OF REPORTS) (Participants will take their time to report the results of their investigation on the given breach simulation, both technical and compliance report). 	MANILA (One San Miguel Ave. Building)	JUNE 05, 2019 (DAY1)	Php 2,000.00 per pax/day	Php 3,500.00 per pax/day
		JUNE 06, 2019 (DAY2)	Php 2,000.00 per pax/day	Php 3,500.00 per pax/day
		JUNE 07, 2019 (DAY3)	Php 2,000.00 per pax/day	Php 2,000.00 per pax/day ((Check-in) 2pm at June 05 (Check-out) 12noon at June 07
	MANILA (One San Miguel Ave. Building)	AUG 07, 2019 (DAY1)	Php 2,000.00 per pax/day	Php 3,500.00 per pax/day
		AUG 08, 2019 (DAY2)	Php 2,000.00 per pax/day	Php 3,500.00 per pax/day
		AUG 09, 2019 (DAY3)	Php 2,000.00 per pax/day	Php 2,000.00 per pax/day (Check-in) 2pm at Aug 07 (Check-out) 12noon at Aug 09ssss

Our training will be held for three (3) days at the designated venues. Training Fee is Php 2,000/day per pax for live-out (inclusive of training kit, lunch, am/pm snacks and certificate of participation). Payment should be made on the account of YISRAEL SOLUTIONS AND CONSULTING (YISCON) INC. Kindly fill up the attached Confirmation Form which requires a list of your participants and fax to (02) 956-2025 or email at eman.limos@visrael.com.ph for your training schedule.

We also conduct in-house trainings. If you are interested, please inform us at the contact numbers stated below.

For inquiries and/or clarification, please contact us by email at eman.limos@visrael.com.ph (attention to: Emmanuel Limos); or thru text at mobile number 0909-719-3289; landline (632) 949-1495; telefax at (02) 956-2025.

Enclosed herewith are Implementing Rules and Regulations of Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012 and NPC Circular 16-03 for your reference. The said Republic Act and circular are accessible to the public, hence, should not be regarded as an endorsement to the person or entity affixing it.

IMPORTANT REMINDER: After accomplishing your reservation and payment, please wait for further updates regarding the finalization of your training schedule before booking a flight or any mode of transportation and accommodation. We will keep in touch as soon as the schedule is finalized not later than a week before the training schedule.

Looking forward to seeing you at this important event.



YISRAEL SOLUTIONS AND CONSULTING (YISCON) INC

NOTE: PLEASE BRING YOUR LAPTOP (at least 4GB Ram) AND USB (at least 8GB storage with no important files).

PRIVACY STATEMENT

We are committed to maintaining the accuracy, confidentiality, and security of your personally identifiable information ("Personal Information"). As part of this commitment, our privacy policy governs our actions as they relate to the collection, use and disclosure of Personal Information.

We are responsible for maintaining and protecting the Personal Information under our control. We have designated an individual or individuals who is/are responsible for compliance with our privacy policy.

Personal information will generally be collected directly from you through the use of any of our standard forms, over the internet, via email, or through a telephone conversation with you. We may also collect personal information about you from third parties acting on your behalf (for instance, agents or contact person).

We also collect information from subscribers (persons registering their details with us through the website) or website visitors for the purpose of improving our quality and effectiveness and to provide you with information. We will not publish your name in connection with any information you provide without your permission.