Deped Regional Advisory No. 020, s. 2022
February 2, 2022

In compliance with DepEd Order (DO) No. 8, s. 2013
This advisory is issued not for endorsement per DO 28, s. 2001,
but only for the information of DepEd officials,
personnel/staff, as well as the concerned public.
(Visit deped.in/ro8issuances)

ONLINE WORKSHOP FOR BREACH RESPONSE AND CYBER SECURITY

Attached is an invitation from the YISRAEL Solutions and Training Center, Inc. regarding the conduct of an Online Workshop for Breach Response and Cyber Security.

The primary objective of this workshop is to educate users on their responsibility to help protect the confidentiality, availability, and integrity of their organization's information and information assets.

Participation of both public and private schools shall be subject to the *no-disruption-of-classes policy* stipulated in DepEd Order No. 9, s. 2005 entitled *Instituting Measures to Increase Engaged Time-on-Task and Ensuring Compliance Therewith and the policy on off-campus stated in DepEd order No. 66, s. 2017*

More information may be inquired from:

YISRAEL Solutions and Training Center, Inc.
Mobile No.: 0915-3683-777/
Landline: (027) 616-3086
Telefax (027) 956-2025
Email Add.: hashien@yisraelsolutions.com

Considering that this is an Advisory, Schools Division Superintendents are given the discretion to act on this matter.

HRDD-RTV
DepEd RO8 ATA-**F21** (CY2018-v03-r00)

DEPARTMENT OF EDUCATION
RECORDS SECTION, REGIONAL OFFICE NO. VIII
RELEASED
020
By: Date: 2/2/22

YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

RECEIVED
RECORDS SECTION REGIONAL OFFICE NO. VIII
JAN 31 2022
BY: TIME: 3:36

499

OFFICE OF THE DIRECTOR IV
31 JAN 2022 4:01
02 FEB 2022 9:15

EVELYN R. FETALVERO, CESO IV
Regional Director
Department of Education Regional Office VIII
Email: region8@deped.gov.ph;
veronicaliza.bautista@gmail.com

SUBJECT: "INVITATION TO ATTEND TO AN ONLINE WORKSHOP FOR BREACH RESPONSE AND CYBER SECURITY"

Dear Sir/Madam,
Greetings!

Yisrael Solutions and Training Center Inc is committed to the welfare of the country and the people. In line with the recent pandemic or the amid spread of COVID 19, the conduct of training classes or seminars/workshops all over the country had been temporarily postponed indefinitely until further notice to ensure the security, health, and safety of our countrymen. However, we have decided to continue our operations with virtual classrooms and remote work through the use of digital communication technology.

As an alternative option for face-to-face, we would like to offer you our online workshop, the online equivalent of being in a training room and learning together as a group through collaborative activities which will be conducted over the internet.

Cybersecurity awareness training is essential to reduce the risk that employees are 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 training could also help the company/agency to respond to 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 to know the state-of-the-art information about Cyber Security, its 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 training, 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

DRD
1/31/22

YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

Our online workshop will be held for three (3) days and the Online Workshop Fee is Php **1,800/day per pax total of Php 5,400 for 3-days (inclusive of tax)**. Kindly fill up the attached Confirmation Form which requires a list of your participants and fax it to (027) 956-2025 or email at hashien@yisraelsolutions.com for your workshop schedule. Please deposit the payment and email the deposit slip then a meeting ID and a password will be sent to your email. Payment should be made on the account of **YISRAEL SOLUTIONS AND CONSULTING (YISCON) INC.**

We also conduct an In-house workshop wherein a central office can organize its regions to attend an online workshop. If you are interested, please inform us at the contact numbers stated below.
For inquiries and/or clarification, please contact us by email at hashien@yisraelsolutions.com (attention to Hashien Grace M. Pecson); or thru text at mobile number 0915 3683 777; landline (027) 616-3086; telefax at (027) 956-2025.
Our team, though working from our own homes, would like to remind you to sanitize your gadgets, aside from washing hands frequently, as an added precautionary measure to prevent the spread of the virus

We hope to see you in our online workshops!

YISRAEL SOLUTIONS AND CONSULTING (YISCON) INC

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.

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).

OKD annual
1/31/22

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.

While we are staying at home to help to control the spread of COVID 19, we are inviting you to attend our online workshop classes for Breach Response and Cyber Security Threat and Attacks. Our cybersecurity expert will give a discussion and demo about Cyber Threats and Attacks.

Below are the online workshop class programs/modules:

MODULE	TOPIC	TIME PERIOD	OBJECTIVES
	DAY 1:		
1	INTRODUCTION TO CYBER SECURITY	9:00AM	Know the state-of-the art information about Cyber Security, it's importance, good practices and benefits to the organization
2	KNOWING THE ATTACK VECTORS (PART I)	TO 4:30PM	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:		
3	KNOWING THE ATTACK VECTORS (PART II	9:00AM	Continuation of discussion on phases of security threats: Hacking web servers, SQL Injection, Hacking Wireless Networks and Mobile Platforms
4	MANAGEMENT APPROACH: INCIDENT RESPONSE FRAMEWORK	TO 4:30PM	The session will provide guidance and additional information on security incident response framework
5	BREACH AND LIVE-ATTACK SIMULATION		Breach simulation briefing and simulation of attack
	DAY 3:		
6	BREACH NOTIFICATION REQUIREMENTS OF RA 10173	9:00AM TO	A deep discussion on breach notification requirements under the DPA and Circular 16-03 and additional information on RA 10175 "Cybercrime Act"
7	BREACH RESPONSE TEAM REPORT (PRESENTATION OF REPORTS)	4:30PM	Participants will take their time to report the results of their investigation on the given breach simulation, both technical and compliance report.

SCHEDULES: (2022)

FEBRUARY 21-23 APRIL 27-29 JUNE 20-22