



Republic of the Philippines  
**Department of Education**  
REGION VIII - EASTERN VISAYAS

**Advisory No. 29**, s. 2026  
**February 9, 2026**

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/region8.deped.gov.ph](http://deped.in/region8.deped.gov.ph))

**ONLINE WORKSHOP ON BREACH RESPONSE AND CYBERSECURITY THREATS & ATTACKS**

Attached is a communication from Rebecca M. Santos, CEO/President, Yisrael Solutions and Training Center, Inc., regarding the **Online Workshop on Breach Response and Cybersecurity Threats & Attacks** on **February 11-13, 2026**, via **Zoom**.

This activity is designed to minimize the risk of employees falling victim to phishing or social engineering tactics, which could result in data breaches compromising the organization's systems.

Yisrael Solutions and Training Center, Inc. invites interested teachers and school leaders to join the activity.

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.

More information may be inquired from:

**REBECCA M. SANTOS**

CEO/President

Yisrael Solutions and Training Center, Inc.

09685959169

[yisrael.solutions@gmail.com](mailto:yisrael.solutions@gmail.com)/[bonn@yisraelsolutions.com](mailto:bonn@yisraelsolutions.com)

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

HRDD-RVR



Address: Government Center, Candahug, Palo, Leyte  
Telephone No.: (053) 832-5738  
Email Address: [region8@deped.gov.ph](mailto:region8@deped.gov.ph)  
Website: [region8.deped.gov.ph](http://region8.deped.gov.ph)

Page 1 of 1



YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

DEPARTMENT OF EDUCATION

**RECEIVED**

RECORDS SECTION REGIONAL OFFICE NO. VIII

DATE: 2/6/24

TRACKING #: 1853

TIME: 9:15 am

SIGNATURE: [Signature]



**Subject: Invitation to Online Breach Response and Cyber Security Workshop**

Dear Sir/Madam,

Greetings!

We are pleased to invite you to our online workshop on "**Breach Response and Cybersecurity Threats & Attacks.**"

Our cybersecurity expert will provide a comprehensive discussion and live demonstration on cyber threats and attacks. The workshop will be held on the proposed dates listed below.

This training aims to reduce the risk of employees falling victim to phishing or social engineering tactics, which could lead to data breaches affecting your organization's systems. It will also help your agency or company prepare for and respond to security breaches in compliance with the notification requirements under the Philippine Data Privacy Act (RA 10173).

The program focuses on educating participants about their role in protecting the **confidentiality, availability, and integrity** of organizational information. Topics include cybersecurity best practices and key threat phases such as system hacking, malware, sniffing, social engineering, and DDoS attacks—along with appropriate response strategies.

The session will include:

- A breach simulation briefing and attack demo
- Discussion on breach notification requirements under RA 10173 and NPC Circular 16-03
- Overview of RA 10175 (Cybercrime Prevention Act)

As part of the simulation, participants will prepare technical and compliance reports based on a mock breach incident. We highly encourage the formation of a **Breach Response Team** (minimum of three members), headed by your **Data Protection Officer (DPO)**, to take part in the **Breach Response Team Report** activity.

Our registration/workshop fee is aligned with the allowable budget under National Budget Circular No. 596 dated January 20, 2025. Please see the attached guidelines issued by the Department of Budget and Management (DBM) for reference.

Below are the online workshop class programs/modules:

[yisrael.solutions@gmail.com](mailto:yisrael.solutions@gmail.com) or [bonn@yisraelsolutions.com](mailto:bonn@yisraelsolutions.com)

DRD Email 2/6/24



## YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

MODULE	TOPIC	PERIOD	OBJECTIVES
1	INTRODUCTION TO CYBER SECURITY	9:00 AM	Know the state-of-the-art information about Cyber Security, its importance, good practices, and benefits to the organization
2	KNOWING THE ATTACK VECTORS (PART I)	TO 4:30 PM	Participants can have a view of different phases of security threats: System Hacking, Malware Threats, Sniffing, Social Engineering, DDOS attacks, and How can they respond to them.
3	KNOWING THE ATTACK VECTORS (PART II)	9:00 AM	Continuation of discussion on phases of security threats: Hacking web servers, SQL Injection, Hacking Wireless Networks, and Mobile Platforms
4	BREACH AND LIVE-ATTACK SIMULATION	TO 4:30 PM	Breach simulation briefing and simulation of an attack
6	MANAGEMENT APPROACH: INCIDENT RESPONSE FRAMEWORK	9:00 AM	The session will provide guidance and additional information on the security incident response framework
7	CONTINUATION OF DATA BREACH HANDS-ON EXERCISE  BREACH RESPONSE TEAM REPORT (PRESENTATION OF REPORTS)	TO 4:30 PM	Participants will take their time to report the results of their investigation on the given breach simulation, both technical and compliance reports.

### ZOOM ONLINE SCHEDULES FOR THE YEAR 2025

January 21 – 23, 2026

February 11 – 13, 2026

**PROMO ALERT! PROMO ALERT! PROMO ALERT!**

#### REGISTRATION FEE:

1 - 2 Participants

6,500.00 per Participant for three (3) days.

3 & more Participants

6,000.00 per Participant for three (3) days.

Kindly fill up the attached Confirmation Form, which requires a list of your participants and email at [yisrael.solutions@gmail.com](mailto:yisrael.solutions@gmail.com) or [bonn@yisraelsolutions.com](mailto:bonn@yisraelsolutions.com) for your workshop schedule. Please deposit the

---

[yisrael.solutions@gmail.com](mailto:yisrael.solutions@gmail.com) or [bonn@yisraelsolutions.com](mailto:bonn@yisraelsolutions.com)



## YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

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 TRAINING CENTER INC.**

**We also conduct an In-house workshop wherein your office can organize its region 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 [yisrael.solutions@gmail.com](mailto:yisrael.solutions@gmail.com) or [bonn@yisraelsolutions.com](mailto:bonn@yisraelsolutions.com) attention to Bonn Marc Pecson); or through text at mobile number 0968-595-9169(Smart).

We look forward to your participation.

A handwritten signature in black ink, appearing to read "forwards" or "forwarded" in a cursive script.

REBECCA M. SANTOS  
CEO/President

YISRAEL SOLUTIONS AND TRAINING CENTER 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.

*We are also attaching the updated guidelines under National Budget Circular No. 596 dated January 20, 2025, which states that the allowable registration or participation fee for government officials and employees attending seminars or workshops is ₱2,800 per day, per participant. This means that the cost of attending the workshop is reimbursable for government officials and employees, subject to agency rules and availability of funds*

**IMPORTANT REMINDER:** After completing your reservation and payment, please wait for further updates regarding the finalization of your workshop schedule before booking any flights, transportation, or accommodation. We will provide confirmation and final details no later than one week before the scheduled workshop.

### 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).