



Republic of the Philippines
Department of Education

REGION I

SCHOOLS DIVISION OF THE CITY OF BATAC

Advisory No. **138** s. 2025

19 JUN 2025

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 www.deped.gov.ph)

**INVITATION TO ATTEND ONLINE WORKSHOP ON BREACH RESPONSE AND
CYBERSECURITY THREATS & ATTACKS**

The Yisrael Solutions and Training Center, Inc. is offering an online workshop
on Breach Response and Cybersecurity Threats 87 Attacks on June 18-20, July 16-
18 and August 13-15, 2025 via zoom Meeting

School heads and teachers of public and private elementary and secondary
schools are invited to participate in the activity on a voluntary basis.

Participation of public and private school 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.

Attached is the letter of invitation for reference.

For more information and other concerns please contact:

BONN MARC PECSON

Ysrael Training Coordinator

Email: yisrael.solutions@gmail.com or bonn@yisraelsolutions.com

Cellphone No. 0968-595-9169

For information.

SGOD/impd/DA-WorkshopBreachResponseCybersecurity
00025/June 18, 2025
2508855

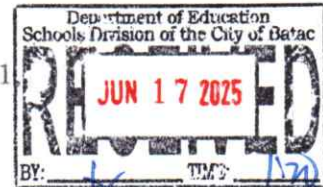


Republic of the Philippines
Department of Education
REGION I



Advisory No. 97, s. 2025

In compliance with DepEd Order (D.O) No. 8, s. 2013
this advisory is issued not for endorsement per D.O No. 28, s. 2001
but only for the information of DepEd Officials,
personnel/staff, as well as the concerned public.
(Visit www.deped.gov.ph)



**INVITATION TO ATTEND ONLINE WORKSHOP ON BREACH RESPONSE AND
CYBERSECURITY THREATS & ATTACKS**

The Yisrael Solutions and Training Center, Inc. is offering a online workshop
on Breach Response and Cybersecurity Threats 87 Attacks on **June 18-20, July
16-18 and August 13-15, 2025** via Zoom Meeting.

Personnel who have access to private data and information of persons of the
School's Division Offices and public and private elementary and secondary
schools are invited to participate on a voluntary basis.

Participation of 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.

Attached is a copy of the invitation for information.

For inquiries and/or clarification, kindly contact:

Bonn Marc Pecson

Yisrael Training Coordinator

Email: yisrael.solutions@gmail.com or bonn@yisraelsolutions.com

Mobile No.: 0968-595-9169

Landline: (02) 616-3086

Facebook Page: <https://www.facebook.com/Yiscon/>

ORD-LU/sam/Breach Response and
Cybersecurity Threats & Attack 2025

*Order for
posting.*



DepEd RO1



Document E



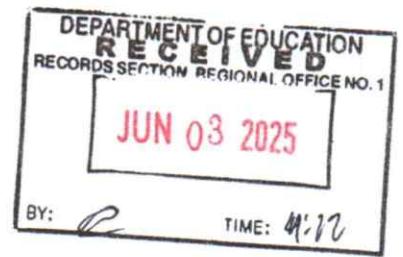
Flores St., Catbangen, City of San Fernando, La Union
Telephone Nos.: (072) 607-8137/682-2324

DepEd Region I region1@deped.gov.ph

www.depedro1.com

Doc. Ref. Code	RO-CLMD- F045	Rev	00
Effectivity	11.07.2024	Page	1 of 1





YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

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 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

JUNE 18-20 JULY 16-18 AUGUST 13-15

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.



YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

Kindly fill up the attached Confirmation Form, which requires a list of your participants and email at visrael.solutions@gmail.com or bonn@visraelsolutions.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 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 visrael.solutions@gmail.com or bonn@visraelsolutions.com attention to Bonn Marc Pecson); or through text at mobile number 0968-595-9169(Smart).

We look forward to your participation.

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).

S. No 2796

H. No 5808

Republic of the Philippines
Congress of the Philippines
Metro Manila

Fifteenth Congress

Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT No. 10175]

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I

PRELIMINARY PROVISIONS

SECTION 1. *Title.* — This Act shall be known as the “Cybercrime Prevention Act of 2012”.

SEC. 2. *Declaration of Policy.* — The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting,

electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

SEC. 3. Definition of Terms. – For purposes of this Act, the following terms are hereby defined as follows:

(a) *Access* refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.

(b) *Alteration* refers to the modification or change, in form or substance, of an existing computer data or program.

(c) *Communication* refers to the transmission of information through ICT media, including voice, video and other forms of data.

(d) *Computer* refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.

(e) *Computer data* refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

(f) *Computer program* refers to a set of instructions executed by the computer to achieve intended results.

(g) *Computer system* refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media.

(h) *Without right* refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law.

(i) *Cyber* refers to a computer or a computer network, the electronic medium in which online communication takes place.

(j) *Critical infrastructure* refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

(k) *Cybersecurity* refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

(l) *Database* refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system.

(m) *Interception* refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

(n) *Service provider* refers to:

(1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

(o) *Subscriber's information* refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established:

(1) The type of communication service used, the technical provisions taken thereto and the period of service;

(2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and

(3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

(p) *Traffic data or non-content data* refers to any computer data other than the content of the communication including, but not limited to, the communication's origin,

destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II

PUNISHABLE ACTS

SEC. 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) *Illegal Access.* — The access to the whole or any part of a computer system without right.

(2) *Illegal Interception.* — The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

(3) *Data Interference.* — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

(4) *System Interference.* — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(5) *Misuse of Devices.* —

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the

(bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(6) Cyber-squatting. — The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

(i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(iii) Acquired without right or with intellectual property interests in it.

(b) Computer-related Offenses:

(1) Computer-related Forgery. —

(i) The input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or

(ii) The act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

(2) Computer-related Fraud. — The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent. Provided That if no

damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided*, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(c) Content-related Offenses:

(1) Cybersex. – The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) Child Pornography. – The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: *Provided*, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

(3) Unsolicited Commercial Communications. – The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

(i) There is prior affirmative consent from the recipient;
or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(4) Libel. - The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

SEC. 5. *Other Offenses.* - The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. - Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. - Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

SEC. 7. *Liability under Other Laws.* - A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

CHAPTER III

PENALTIES

SEC. 8. *Penalties.* - Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (P200,000.00) up to a maximum amount commensurate to

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(1) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": *Provided, That* the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

SEC. 9. *Corporate Liability.* - When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on:

the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00).

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (PhP5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

CHAPTER IV

ENFORCEMENT AND IMPLEMENTATION

SEC. 10. *Law Enforcement Authorities.* – The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

SEC. 11. *Duties of Law Enforcement Authorities.* – To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the

SEC. 12. *Real-Time Collection of Traffic Data.* - Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed; (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

SEC. 13. *Preservation of Computer Data.* - The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension for another six (6) months: *Provided*, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the preservation

Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

SEC. 14. *Disclosure of Computer Data.* - Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

SEC. 15. *Search, Seizure and Examination of Computer Data.* - Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and;

(a) To secure a computer system or a computer data storage medium;

(b) To make and retain a copy of those computer data secured;

(c) To maintain the integrity of the relevant stored computer data;

(d) To conduct forensic analysis or examination of the computer data storage medium; and

(e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve

necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

SEC. 16. *Custody of Computer Data.* - All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

SEC. 17. *Destruction of Computer Data.* - Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination.

SEC. 18. *Exclusionary Rule.* - Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

SEC. 19. *Restricting or Blocking Access to Computer Data.* - When a computer data is *prima facie* found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

SEC. 20. *Noncompliance.* - Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of *prision correccional* in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.

CHAPTER V

JURISDICTION

SEC. 21. *Jurisdiction.* - The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

CHAPTER VI

INTERNATIONAL COOPERATION

SEC. 22. *General Principles Relating to International Cooperation.* - All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense shall be given full force and effect.

CHAPTER VII

COMPETENT AUTHORITIES

SEC. 23. *Department of Justice (DOJ).* – There is hereby created an Office of Cybercrime within the DOJ designated as the central authority in all matters related to international mutual assistance and extradition.

SEC. 24. *Cybercrime Investigation and Coordinating Center.* – There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, for policy coordination among concerned agencies and for the formulation and enforcement of the national cybersecurity plan.

SEC. 25. *Composition.* – The CICC shall be headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson with the Director of the NBI as Vice Chairperson; the Chief of the PNP; Head of the DOJ Office of Cybercrime; and one (1) representative from the private sector and academe, as members. The CICC shall be manned by a secretariat of selected existing personnel and representatives from the different participating agencies.

SEC. 26. *Powers and Functions.* – The CICC shall have the following powers and functions:

(a) To formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);

(b) To coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in this Act;

(c) To monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;

(d) To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;

(e) To coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other related projects;

(f) To recommend the enactment of appropriate laws, issuances, measures and policies;

(g) To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions; and

(h) To perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of this Act.

CHAPTER VIII

FINAL PROVISIONS

SEC. 27. *Appropriations.* - The amount of Fifty million pesos (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

SEC. 28. *Implementing Rules and Regulations.* - The ICTO-DOST, the DOJ and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act, for its effective implementation.

SEC. 29. *Separability Clause.* - If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 30. *Repealing Clause.* - All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly. Section 33(a) of Republic Act No. 8792 or the

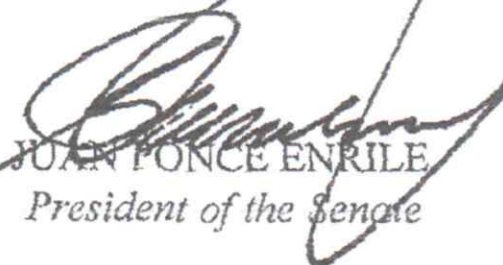
SEC. 31. *Effectivity.* — This Act shall take effect fifteen (15) days after the completion of its publication in the *Official Gazette* or in at least two (2) newspapers of general circulation.

Approved,



FELICIANO BELMONTE JR.

*Speaker of the House
of Representatives*



JOAN PONCE ENRILE

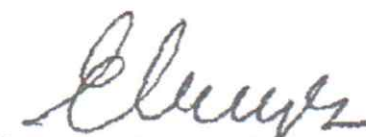
President of the Senate

This Act which is a consolidation of Senate Bill No. 2796 and House Bill No. 5808 was finally passed by the Senate and the House of Representatives on June 5, 2012 and June 4, 2012, respectively.



MARILYN B. BARUA YAP

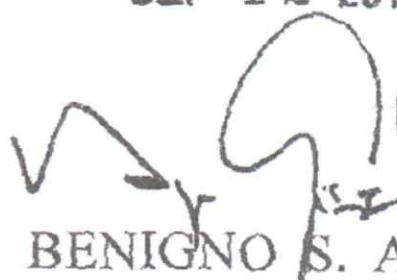
*Secretary General
House of Representatives*



EMMA LIRIO-REYES

Secretary of the Senate

Approved: **SEP 12 2012**



BENIGNO S. AQUINO III

President of the Philippines



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular 16-03

DATE : 15 December 2016
SUBJECT : PERSONAL DATA BREACH MANAGEMENT

WHEREAS, the Philippine Constitution guarantees respect for the right to privacy, including information privacy, accorded recognition as inherent in the freedoms enjoyed by every Filipino, and at the same time, Article II, Section 11 of the Constitution emphasizes that the State values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, Article II, Section 24, of the Constitution provides that the State recognizes the vital role of communication and information in nation-building, and Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012, provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth;

WHEREAS, there are increasing incidents of personal data breaches that impact both public and private entities, entailing significant economic and legal costs for those involved in processing of personal data and putting at risk data subjects for identity theft, crimes and other harm, and that in order to afford protection of personal data, reasonable and appropriate organizational, physical and technical measures should be implemented;

WHEREAS, Section 20(f) of the Act requires prompt notification of the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, which may likely give rise to a real risk of serious harm to any affected data subject;

WHEREAS, in order to ensure compliance of the country and all personal information controllers and personal information processors with the law and international standards set for data protections, and to safeguard against accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing, the management of personal data breach should include prevention, incident response, mitigation and compliance with notification requirements;

WHEREFORE, in consideration of these premises, the National Privacy Commission hereby issues this Circular governing personal data breach management.

RULE I.
GENERAL PROVISIONS

SECTION 1. Scope. These Rules apply to any natural and juridical person in the government or private sector processing personal data in outside of the Philippines, subject to the relevant provisions of the Act and its Implementing Rules and Regulations.

SECTION 2. Purpose. These Rules provide the framework for personal data breach management and the procedure for personal data breach notification and other requirements.

SECTION 3. Definition of Terms. For the purpose of this Circular, the following terms are defined, as follows:

- A. "Act" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- B. "Commission" refers to the National Privacy Commission;
- C. "Data Protection Officer" refers to an individual designated by the head of agency to be accountable for the agency's compliance with the Act: *Provided*, that the individual must be an organic employee of the government agency: *Provided further*, that a government agency may have more than one data protection officer;
- D. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- E. "Personal data" refers to all types of personal information;
- F. "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:
 - 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
 - 2. Integrity breach resulting from alteration of personal data; and/or
 - 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.
- G. "Personal information controller" refers to a natural or juridical person, or any other body that controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:
 - 1. A natural or juridical person, or any other body that performs such functions as instructed by another person or organization; or
 - 2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person, or any other body, decides on what information is collected, or the purpose or extent of its processing;
- H. "Personal information processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;
- I. "Privacy Impact Assessment" is a process undertaken and used by a government agency to evaluate and manage privacy impacts.
- J. "Security incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place;
- K. "Security Incident Management Policy" refer to policies and procedures implemented by a personal information controller or personal information processor to govern the actions to be taken in case of a security incident or personal data breach;
- L. "Sensitive personal information" refers to personal information:
 - 1. About an individual's race, ethnic origin, marital status, age, color, and religious,

2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, and
4. Specifically established by an executive order or an act of Congress to be kept classified.

RULE II. GUIDELINES FOR PERSONAL DATA BREACH MANAGEMENT

SECTION 4. *Security Incident Management Policy.* A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

- A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
- B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
- C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
- D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
- E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.

SECTION 5. *Data Breach Response Team.* A personal information controller or personal information processor shall constitute a data breach response team, which shall have at least one (1) member with the authority to make immediate decisions regarding critical action, if necessary. The team may include the Data Protection Officer.

The team shall be responsible for the following:

- A. Implementation of the security incident management policy of the personal information controller or personal information processor;
- B. Management of security incidents and personal data breaches; and
- C. Compliance by the personal information controller or personal information processor with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

The team must be ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements.

The functions of the Data Breach Response Team may be outsourced. Such outsourcing shall not reduce the requirements found in the Act, the IRR or related issuance. The Data Protection Officer shall remain accountable for compliance with applicable laws and regulations.

In cases where the Data Protection Officer is not part of the Data Breach Response Team, the Data Breach Response Team shall submit a written report addressed to the Data Protection Officer detailing the actions taken in compliance with these Rules.

RULE III.

GUIDELINES FOR THE PREVENTION OF PERSONAL DATA BREACH

SECTION 6. *Preventive or Minimization Measures.* A security incident management policy shall include measures intended to prevent or minimize the occurrence of a personal data breach. Such safeguards may include:

- A. Conduct of a privacy impact assessment to identify attendant risks in the processing of personal data. It shall take into account the size and sensitivity of the personal data being processed, and impact and likely harm of a personal data breach;
- B. Data governance policy that ensures adherence to the principles of transparency, legitimate purpose, and proportionality;
- C. Implementation of appropriate security measures that protect the availability, integrity and confidentiality of personal data being processed;
- D. Regular monitoring for security breaches and vulnerability scanning of computer networks;
- E. Capacity building of personnel to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents;
- F. Procedure for the regular review of policies and procedures, including the testing, assessment, and evaluation of the effectiveness of the security measures.

SECTION 7. *Availability, Integrity and Confidentiality of Personal Data.* The implementation of security measures shall be in accordance with the Act, its IRR, and other issuances of the Commission. The security measures should be directed to ensuring the availability, integrity, and confidentiality of the personal data being processed, and may include:

- A. Implementation of back-up solutions;
- B. Access control and secure log files;
- C. Encryption;
- D. Data disposal and return of assets policy.

RULE IV.

GUIDELINES FOR INCIDENT RESPONSE POLICY AND PROCEDURE

SECTION 8. *Policies and Procedures.* The personal information controller or personal information processor shall implement policies and procedures for guidance of its data breach

- A. A procedure for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;
- B. Clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure, and who shall be immediately contacted in the event of a possible or confirmed personal data breach;
- C. Conduct of a preliminary assessment for purpose of:
 - 1. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage
 - 2. Determining the need for notification of law enforcement or external expertise; and
 - 3. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;
- D. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects;
- E. Procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;
- F. Conduct of investigations that will evaluate fully the security incident or personal data breach;
- G. Procedures for notifying the Commission and data subjects when the breach is subject to notification requirements, in the case of personal information controllers, and procedures for notifying personal information controllers in accordance with a contract or agreement, in the case of personal information processors; and
- H. Policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The personal information controller must be ready to provide assistance to data subjects whose personal data may have been compromised.

SECTION 9. Documentation. All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:

- A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
- B. Actions and decisions of the incident response team;
- C. Outcome of the breach management, and difficulties encountered; and
- D. Compliance with notification requirements and assistance provided to affected data subjects.

A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

SECTION 10. Regular Review. The incident response policy and procedure shall be subject to regular revision and review, at least annually, by the Data Protection Officer, or any other person designated by the Chief Executive Officer or the Head of Agency, as the case may be. The date of the last review and the schedule for the next succeeding review must always be indicated in the documentation of the incident response policy and procedure.

RULE V. PROCEDURE FOR PERSONAL DATA BREACH NOTIFICATION AND OTHER REQUIREMENTS

SECTION 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

- A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

- B. There is reason to believe that the information may have been acquired by an unauthorized person; and
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

SECTION 12. Public Information. A claim that the data involved in a breach is public information will not automatically exempt a personal information controller from the notification requirements provided herein. When the level of availability or publicity of the personal data is altered by a personal data breach, it shall be considered as a personal data breach requiring notification, subject to the preceding paragraphs.

SECTION 13. Determination of the Need to Notify. Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred.

The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:

- A. Information that would likely affect national security, public safety, public order, or public health;
- B. At least one hundred (100) individuals;
- C. Information required by applicable laws or rules to be confidential; or
- D. Personal data of vulnerable groups.

SECTION 14. *Discovery of Vulnerability.* A discovery of a vulnerability in the data processing system that would allow access to personal data shall prompt the personal information controller or the personal information processor, as the case may be, to conduct an assessment and determine if a personal data breach has occurred.

SECTION 15. *Who should Notify.* The personal information controller shall notify the Commission and the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the personal information controller even if the processing of information is outsourced or subcontracted to a personal information processor.

The personal information controller shall identify the designated data protection officer or other individual responsible for ensuring its compliance with the notification requirements provided in this Circular.

SECTION 16. *Reporting by Personal Information Processors.* To facilitate the timely reporting of a personal data breach, the personal information controller shall use contractual or other reasonable means to ensure that it is provided a report by the personal information processor upon the knowledge of, or reasonable belief that a personal data breach has occurred.

SECTION 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

- A. *When Notification Should be Done.* The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.
- B. *Delay in Notification.* Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

The personal information controller need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects.

Delay in notification shall not be excused if it is used to perpetuate fraud or to conceal the personal data breach.

- C. *When delay is prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply.
- D. *Content of Notification.* The notification shall include, but not be limited to:
 - 1. Nature of the Breach
 - a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
 - b. a chronology of the events leading up to the loss of control over the personal data;
 - c. approximate number of data subjects or records involved;
 - d. description or nature of the personal data breach;
 - e. description of the likely consequences of the personal data breach; and

- f. name and contact details of the data protection officer or any other accountable persons.
2. Personal Data Possibly Involved
 - a. description of sensitive personal information involved; and
 - b. description of other information involved that may be used to enable identity fraud.
3. Measures Taken to Address the Breach
 - a. description of the measures taken or proposed to be taken to address the breach;
 - b. actions being taken to secure or recover the personal data that were compromised;
 - c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
 - d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
 - e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.

- E. *Form.* Notification shall be in the form of a report, whether written or electronic, containing the required contents of notification: *Provided*, that the report shall also include the name and contact details of the data protection officer and a designated representative of the personal information controller: *Provided further*, that, where applicable, the manner of notification of the data subjects shall also be included in the report.

Where notification is transmitted by electronic mail, the personal information controller shall ensure the secure transmission thereof.

Upon receipt of the notification, the Commission shall send a confirmation to the personal information controller. A report is not deemed filed without such confirmation. Where the notification is through a written report, the received copy retained by the personal information controller shall constitute proof of such confirmation.

SECTION 18. Notification of Data Subjects. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

- A. *When should notification be done.* The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

- B. *Exemption or Postponement of Notification.* If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.

A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.

The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.

C. *Content of Notification.* The notification shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.

The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

SECTION 19. Exemption from Notification Requirements. The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:

- A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;
- B. Subsequent measures that have been taken by the personal information controller or personal information processor to ensure that the risk of harm or negative consequence to the data subjects will not materialize;
- C. Age or legal capacity of affected data subjects: *Provided*, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.

In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.

SECTION 20. *Failure to Notify.* In case the personal information controller fails to notify the Commission or data subjects, or there is unreasonable delay to the notification, the Commission shall determine if such failure or delay is justified. Failure to notify shall be presumed if the Commission does not receive notification from the personal information controller within five (5) days from knowledge of or upon a reasonable belief that a personal data breach occurred.

SECTION 21. *Investigation of a Breach or a Security Incident.* Depending on the nature of the incident, or if there is failure or delay in the notification, the Commission may investigate the circumstances surrounding a personal data breach. Investigations may include on-site examination of systems and procedures.

If necessary, the Commission shall require the cooperation of concerned parties, or compel appropriate action therefrom to protect the interests of data subjects.

The investigation under this Section shall be governed by the Rules of Procedure of the Commission.

Section 22. *Reportorial requirements.* All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the event of a personal data breach, a report shall include the facts surrounding the incident, the effects of such incident, and the remedial action taken by the personal information controller. For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation.

Any or all reports shall be made available when requested by the Commission: *Provided*, that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

Section 23. *Notification and Reporting to the National Privacy Commission.* The requirements pertaining to notification and the submission of reports shall be complied with through the appropriate submissions to the office of the National Privacy Commission or by electronic mail (complaints@privacy.gov.ph). The foregoing details may be amended, subject to a public announcement made through the Commission's website or other comparable means.

SECTION 24. *Separability Clause.* If any portion or provision of this Circular is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 25. *Effectivity.* This Order shall take effect fifteen (15) days after publication in the Official Gazette or two newspapers of general circulation.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Summary	
What is subject to the notification requirements.	<p>A security breach that:</p> <ol style="list-style-type: none"> 1. Involves sensitive personal information, or information that may be used to enable identity fraud 2. There is reason to believe that information have been acquired by an unauthorized person 3. The unauthorized acquisition is likely to give rise to a real risk of serious harm
Who should notify.	The personal information controller, which controls the processing of information, even if processing is outsourced or subcontracted to a third party.
When should notification of Commission be done.	<p>Within 72 hours from knowledge of the personal data breach, based on available information.</p> <p>Follow up report should be submitted within five (5) days from knowledge of the breach, unless allowed a longer period by the Commission.</p>
When should data subjects or individuals be notified.	Within seventy-two (72) hours from knowledge of the breach, unless there is a reason to postpone or omit notification, subject to approval of the Commission.
What are the contents of notification to Commission	<p>In general-</p> <ol style="list-style-type: none"> 1. nature of the breach 2. sensitive personal information possibly involved 3. measures taken by the entity to address the breach 4. details of contact person for more information
What are the contents of notification to data subject	In general, same contents as notification of Commission but must include instructions on how data subject will get further information and recommendations to minimize risks resulting from breach.
How will notification be done?	<p>Commission may be notified by written or electronic means but the personal information controller must have confirmation that the notification has been received.</p> <p>Data subjects or affected individuals shall be notified individually, by written or electronic means, unless allowed by the Commission to use alternative means.</p>
Other requirements	<p>Cooperate with the Commission where there is an investigation related to the breach.</p> <p>Documentation of all security incidents and the submission of an annual report to the Commission.</p>

ATTENTION TO: Bonn Marc Pecson

Confirmation Date: _____

MESSAGE: Please fill-out the form below (readable and correct name spelling of participants) and fax to Yisrad Training Secretariat at (02) 956-2025; or email to: yisrael.solutions@gmail.com

CONFIRMATION FORM
(Breach Response and Cyber Security
Workshop)

Please take note that Confirmation/Reservation is on First Come First Serve Basis)

Name of Company:					
Address: (For LBC)				Region:	
Type of Organization:					
Contact Person:			Tel. No.	Mobile No.	Fax No.
Participants Details:					
First Name	Middle Initial	Last Name	Gender	Mobile No	Position
Email Address:					

Please reserve me/us on this workshop schedule:

A M O U N T

SCHEDULE	Time	No. of Slot Reserve	Total Amount PROMO (Php 6,500 per pax for 3-days)

PAYMENT METHOD

All payments shall be made in Philippine Pesos.

☐ Cash

☐ Check payment

Please make check payable to:

YISRAEL SOLUTIONS AND TRAINING CENTER INC.

Pls deposit your payment to our Landbank Account
BANK DETAILS:

Account Name: YISRAEL SOLUTIONS AND TRAINING
CENTER INC

Account Number: 1641-1087-11

Pasig-C. Raymundo Ave. Branch

REGISTRATION POLICY:

GUARANTEED SEATS

Please fill up the confirmation form to guarantee your slots. Those who confirmed will be given "priority status" contingent upon availability of seats.

CANCELLATION POLICY

NO cancellation will be made upon confirmation; however, substitutes are allowed only when there is a written notice to the Yisrael Solutions and Training Center Inc. at least five (5) working days prior to the seminar.

Please take note that there is a **LATE-CANCELLATION** and **NON-ATTENDANCE CHARGE of Php 750.00/day per** participant to cover training costs.

OR SEND YOUR PAYMENT THRU OUR GCASH ACCOUNT:
09175127230

Marissa Pecson

(Please email payment to us thru
yisrael.solutions@gmail.com)

Requested by:

Signature over printed Name

PRIVACY NOTICE:

"We from Yisrael Solutions and Consulting (YISCON), Inc. will make sure that all of the personal informations you have provided will be secured and remain confidential as much as possible. We collect informations with your proper consent and that necessary personal in information with the intent to fulfil the purpose in transacting with us."