Republic of the Philippines
Department of Education
NEGROS ISLAND REGION

REGIONAL MEMORANDUM
No. 583, s. 2026

JUN 15 2026

DISSEMINATION OF MEMORANDUM DPO-2026-051 TITLED "ORIENTATION ON SUBMISSIONS FOR THE ANNUAL SECURITY INCIDENT REPORT (ASIR)"

To: OIC-Assistant Regional Director
Schools Division Superintendents
All Others Concerned

1. Attached is Memorandum DPO-2026-051 dated May 26, 2026, titled "Orientation on Submissions for the Annual Security Incident Report (ASIR)," which is self-explanatory.

2. Immediate dissemination of and compliance with this Memorandum are desired.

RAMIR B. UYTICO EdD, CESO III
Regional Director

Encl.: As stated
Reference: As stated

To be indicated in the Perpetual Index
under the following subjects:

DATA POLICY REPORTS

Address: Batinguel, Dumaguete City, 6200
Telephone Nos: (035) 527-5297
Email Address: nir@deped.gov.ph
Website: https://depednir.net/

Republika ng Pilipinas
Department of Education
DATA PRIVACY OFFICE

MEMORANDUM
DPO-2026-051

FOR : **UNDERSECRETARIES**
ASSISTANT SECRETARIES
BUREAU AND SERVICE DIRECTORS
REGIONAL DIRECTORS
SCHOOL DIVISION SUPERINTENDENTS
DIVISION CHIEFS
ALL OTHERS CONCERNED

FROM : **ROGER B. MASAPOL**
Data Protection Officer
Data Privacy Office

ATTY. HONEYLETTE T. SANCHEZ
Attorney V
Data Privacy Office

SUBJECT : **ORIENTATION ON SUBMISSIONS FOR THE ANNUAL SECURITY INCIDENT REPORT (ASIR)**

DATE : 26 May 2026

Pursuant to this directive, the Department, through the Data Privacy Office, consolidated all reported security incidents and personal data breaches that occurred from 01 January to 31 December 2025. This was done in compliance with the National Privacy Commission's (NPC) directive on the submission of the 2025 Annual Security Incident Report (ASIR).

This Office extends its sincere appreciation to all offices that timely and diligently submitted their reports. Your cooperation significantly contributed to the Department's continuing commitment to upholding the data privacy rights of learners, personnel, and other stakeholders.

To ensure better information collection and accurate data capture moving forward, **this Office shall conduct an online orientation for all concerned offices** to introduce new mechanics in the collection of security incident reports, clarify the scope and classification of security incidents and personal data breaches, discuss proper documentation standards, share updates on the reportorial requirements issued by the NPC, and outline the end-to-end reporting and consolidation process. Concerned offices shall be required to send **one (1) representative** (preferably the Data Privacy Focal Person or the Compliance Office for Privacy) and confirm their

attendance through the designated sign-up sheet. Further details are provided in Annex A.

To allow sufficient time for questions and discussion during the orientation, offices have been grouped into clusters, each with a corresponding scheduled date of attendance.

ONLINE ORIENTATION ON ASIR SUBMISSIONS SCHEDULE	
Date of Roll Out:	**Cluster 1: 16 June 2026 (Tue), 09:00 AM to 12:00 NN** • Region I Office and Schools Division Offices • Region II Office and Schools Division Offices • CAR Office and Schools Division Offices • CALABARZON Office and Schools Division Offices • MIMAROPA Office and Schools Division Offices • Region V Office and Schools Division Offices • National Capital Region Office and Schools Division Offices
	Cluster 2: 17 June 2026 (Wed), 09:00 AM to 12:00 NN • Department of Education Central Office • Region VI Office and Schools Division Offices • Negros Island Region (NIR) Office and Schools Division Offices • Region VII Office and Schools Division Offices • Region VIII Office and Schools Division Offices
	Cluster 3: 18 June 2026 (Thu), 09:00 AM to 12:00 NN • Region IX Office and Schools Division Offices • Region X Office and Schools Division Offices • Region XI Office and Schools Division Offices • SOCCSKARGEN Regional Office and Scholls Division Offices • CARAGA Regional Office and Scholls Division Offices

For context, this Office identified several challenges in the reportorial process, which include the following:

a. **Confusion in the Classification of Security Incidents**
Several offices submitted security incident reports wherein multiple or inconsistent classifications were assigned to a single incident. This resulted in inaccurate incident counts and made it difficult to clearly determine the actual number of incidents per classification. These inconsistencies affected the integrity of the aggregated data and limited the Office's ability to conduct meaningful analysis of incident trends and types.

b. **Non-compliance with Prescribed Guidelines**
Certain offices reported the existence of security incidents without properly tagging or identifying the specific nature of the incident. In some cases, the reporting form was disseminated to schools, resulting in school-level submission of incidents, which is inconsistent with the prescribed reporting

structure. Under the established guidelines, Schools Division Offices (SDOs) were required to consolidate all security incidents from schools under their jurisdiction prior to submission to the Data Privacy Office.

c. **Lack of Documentation Leading to Reporting Issues**
Some reported incidents were submitted without sufficient supporting documentation, particularly those originating at the school level. Field offices also relayed that certain incidents occurred long ago and were not formally documented in either physical or electronic records. Additionally, deviations from the prescribed reporting structure persisted in some submissions, further constraining validation efforts and reducing the overall reliability and credibility of the reported data.

Collectively, these challenges resulted in ambiguous and inconsistent reporting, which required multiple follow-ups with Data Privacy Focal Persons (DPFPs) and Compliance Officers for Privacy (COPs) to verify the accuracy and completeness of submissions from their respective offices.

To address recurring issues and to promote accuracy, consistency, and timeliness in reporting, the Data Privacy Office shall institutionalize the **Quarterly Security Incident Report (QSIR).**

All offices in the Central, Regional, School Division-level are required to submit consolidated reports on security incidents and personal data breaches handled by their respective offices on or before the fifteenth (15th) day of the month immediately following the end of each reporting quarter, in accordance with the timetable set forth below:

Reporting Quarter	Inclusive Coverage Period	Deadline for Submission
Quarter 1	January 1 to March 31	[July 15 for CY 2026]; April 15 for the following CYs
Quarter 2	April 1 to June 30	July 15
Quarter 3	July 1 to September 30	October 15
Quarter 4	October 1 to December 31	January 15 of the succeeding year

For offices with no recorded security incidents and/or personal data breaches during the reporting period, please select **"No, our office did not handle any security incidents and/or personal data breaches"** in the submission form. For detailed guidance on which incidents fall under Mandatory, Non-Mandatory, and Other Security Incidents, including the applicable tagging mechanics, please refer to Annex B.

Further details on the matter shall be discussed during the online orientation.

For your guidance and appropriate action.

ANNEX A: ORIENTATION ON THE QUARTERLY SECURITY INCIDENT REPORTING

Program:	**Orientation on the Quarterly Security Incident Reporting in the Department of Education's Central, Regional, and School's Division Offices**
Agenda:	This conference aims to: a. Explain the background, scope, and requirements of the Quarterly Security Incident Report (QSIR), including the classification of security incidents and personal data breaches and relevant updates from the National Privacy Commission (NPC); b. Demonstrate the proper documentation and completion of the QSIR, including correct tagging, reporting mechanics, and applicable documentation standards; and c. Align understanding and address queries on the end-to-end incident reporting, consolidation, and submission process.
Target Attendees:	• Data Privacy Focal Persons; • Compliance Officers for Privacy; and • Other Relevant DepEd Employees who is the Focal of their Office in Data Privacy Matters (i.e. Information Technology Officers, Administrative Officers, etc.)
Date of Roll Out:	**Cluster 1: 16 June 2026 (Tue), 09:00 AM to 12:00 NN** • Region I Office and Schools Division Offices • Region II Office and Schools Division Offices • CAR Office and Schools Division Offices • CALABARZON Office and Schools Division Offices • MIMAROPA Office and Schools Division Offices • Region V Office and Schools Division Offices • National Capital Region Office and Schools Division Offices Link: **https://tinyurl.com/QSIR-Confe-C1**
	Cluster 2: 17 June 2026 (Wed), 09:00 AM to 12:00 NN • Department of Education Central Office • Region VI Office and Schools Division Offices • Negros Island Region (NIR) Office and Schools Division Offices • Region VII Office and Schools Division Offices • Region VIII Office and Schools Division Offices Link: **https://tinyurl.com/QSIR-Confe-C2**
	Cluster 3: 18 June 2026 (Thu), 09:00 AM to 12:00 NN • Region IX Office and Schools Division Offices • Region X Office and Schools Division Offices • Region XI Office and Schools Division Offices • SOCCSKARGEN Regional Office and Scholls Division Offices • CARAGA Regional Office and Scholls Division Offices Link: **https://tinyurl.com/QSIR-Confe-C3**
Sign-up sheet:	**https://tinyurl.com/QSIR-Confe-Sign-Up**

ANNEX B: QUARTERLY SECURITY INCIDENT FORM GUIDELINES ON SECURITY INCIDENT TAGGING

The Data Privacy Office (DPO) of the Department of Education enforces the submission of the **Quarterly Security Incident Report (QSIR)** as a proactive governance and risk-management measure to strengthen the Department's compliance with the Data Privacy Act of 2012 (RA 10173) and related National Privacy Commission (NPC) issuances.

Specifically, the implementation of QSIR aims to:

a. **Ensure prompt, consistent, and quality incident response**, supported by complete and standardized documentation, which facilitates accurate assessment of risks, informed decision-making, and appropriate escalation when notification to the NPC or affected data subjects becomes necessary;
b. **Promote accountability and awareness among offices and personnel** by reinforcing the shared responsibility of recognizing, reporting, and managing security incidents involving personal data, in line with the accountability principle under the Data Privacy Act; and
c. **Strengthen institutional risk management and planning**, as aggregated QSIR data allows the Department to analyze trends, prioritize resources, and enhance policies, controls, and capacity-building initiatives related to data protection and information security.

Overall, the QSIR serves not only as a reporting mechanism but also as a preventive, oversight, and capacity-building tool, reinforcing a culture of privacy and security across the Department.

To better understand, below are the details in what the report covers.

I. What is a Security Incident?

A 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.

II. What is a Personal Data Breach?

A 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.

All personal data breaches are essentially security incidents. A security incident will result in a personal data breach if there are no existing safeguards to remedy the situation.

III. What are the Natures of Personal Data Breach?

All Personal Data Breach incidents reported must be designated **one (1)** of the three natures below.

a. A **Confidentiality** breach resulting from the unauthorized disclosure of or access to personal data.
b. An **Integrity** breach resulting from alteration of personal data; and/or

c. An **Availability** breach resulting from loss, accidental or unlawful destruction of personal data.

In cases where more than one nature exists, the most imminent nature shall be reflected in the tagging, while other applicable natures shall be disclosed in the report as supplementary information.

IV. What are the Types of Breach Notification?

All data breach and/or security incident must fall under **one (1)** of the notification classifications below:

a. Mandatory Notification

These refer to personal data breaches that involves **ALL** elements:

- The personal data involves sensitive personal information or any other information that may be used to enable identity fraud;
- Other information includes, but is not limited to, the following:
    - 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.
- There is reason to believe that the information may have been acquired by an unauthorized person; and
- The personal information controller believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

b. Non-mandatory Notification

These refer to personal data breaches involving personal data that do not meet any of the criteria for mandatory notification. Specifically, the breach:

- does not involve sensitive personal information or privileged information,
- does not pose a reasonable risk of harm to data subjects, and
- does not affect a significant number of individuals.

While notification to the National Privacy Commission and affected data subjects is not required, the incident must still be properly documented, assessed, and addressed internally, and may be subject to notification should subsequent findings elevate the risk.

c. Other Security Incidents

These refer to security incidents involving the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that did not involve personal information or sensitive personal information.

If there is doubt as to whether notification is indeed necessary, consider:

1) The likelihood of harm or negative consequences on the affected data subjects;
2) How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and
3) If the data involves:
   - Information that would likely affect national security, public safety, public order, or public health;
   - At least one hundred (100) individuals;
   - Information required by all applicable laws or rules to be confidential; or
   - Personal data of vulnerable groups.

V. What is Security Incident Tagging?

These tags are descriptors that indicate the type of incident or resulting impact, not the underlying cause. All security incidents must be assigned the tag that best describes the incident.

Each data breach and security incident reported must indicate **one (1) from the following**:

Security Incident Tag	Use this Tag when
a. Theft	• Personal data, devices, media, or system components were unlawfully taken, with or without confirmed data access • Theft resulted in actual or potential loss of confidentiality
b. Identity Fraud	• Stolen or exposed personal data was used or reasonably likely to be used to impersonate a data subject • Fraudulent transactions, registrations, or identity misuse are detected
c. Sabotage or Physical Damage	• Systems, servers, or facilities were deliberately damaged • Data availability or integrity was compromised due to physical destruction
d. Malicious Code	• Malware, ransomware, spyware, worms, or trojans were detected • Code execution posed a threat to system integrity or data confidentiality
e. Hacking or Logical Infiltration Occurred	• Unauthorized access successfully occurred through logical means • Exploitation of vulnerabilities, credentials, or misconfigurations happened
f. Misuse of Resources	• Authorized users used systems or data outside their permitted purpose • Insider misuse, excessive privilege abuse, or policy violations occurred

g. Hardware Failure	• Physical components failed unexpectedly • Resulted in data unavailability, corruption, or loss
h. Software Failure	• Application or system software malfunctioned • Errors caused data loss, corruption, or service disruption
i. Communication Failure	• Network outages, transmission failures, or connectivity losses occurred • Affected access to or transmission of personal data
j. Natural Disaster	• Incidents were caused by natural events such as fires, floods, earthquakes, or storms.
k. Design Error	• System or process design flaws existed from inception • Privacy or security risks arose from poor architectural decisions
l. User Error	• Incidents resulted from unintentional actions of users • No malicious intent
m. Operation Error	• Errors occurred during routine operations • Procedural lapses or mis-execution occurred
n. Software Maintenance Error	• Incidents were caused by faulty patching, updates, or system changes
o. Third Party or Service Provider	• Incident originated from vendors, contractors, hosting providers • Data processing was outsourced or shared
p. Others	• Other causes or impact that are not listed

If more than one cause applies, the most imminent shall be used for tagging, with other applicable causes noted as supplementary information.

VI. References

- **National Privacy Commission**. (2016, December 15). NPC Circular 16-03, Personal Data Breach Management. From *https://privacy.gov.ph/wp-content/uploads/2022/01/sgd-npc-circular-16-03-personal-data-breach-management.pdf*
- **Report a Breach**. (n.d.). National Privacy Commission (NPC). From *https://privacy.gov.ph/pips-and-pics/breach-reporting/*