Republic of the Philippines
Department of Education
REGION VIII
SCHOOLS DIVISION OF NORTHERN SAMAR

Office of the Schools Division Superintendent

DIVISION MEMORANDUM
No. 230, s. 2026

To: Public School District Supervisors
District-in-Charged
Elementary and Secondary School Heads
Teacher-in-Charged
School Head-in-Charged
All Other concerned

SCHOOL-LEVEL REPORTING OF PERSONAL DATA BREACHES AND SECURITY INCIDENCES FOR QUARTER SECURITY INCIDENCE REPORT (QSIR) OF THE DEPARTMENT OF EDUCATION (DEPED)

1. This refers to the quarterly submission for School-Level Reporting of Personal Data Breaches and Security Incidence Report of the Department of Education (DepEd) for Second Quarter.

2. For your guidance, security incidents and personal breaches covered by the mandatory notification requirements includes:
   a. Situations involving sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud;
   b. Situations where there is reason to believe that the information may have been acquired by an unauthorized person; and
   c. Situations where the Department or National Privacy Commission (NPC) believe that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

   For reference, please find attached a copy of the QSIR template which this Office will subsequently submit to NPC through the Data Privacy Office.

3. All concerned shall submit on or before **July 10, 2026,** for this Office will consolidate the Data on **July 15, 2026.**

4. Accomplished reports using the QSIR template shall be submitted to Data Privacy Officer, **ATTY. RISTY T. ADARAYAN,** Attorney III, Legal Unit, though https://tinyurl.com/QSIR-DEPED-NORTHERNSAMAR

   In case a school has no occurrence of a security incident and/or personal data breach, kindly indicate "No Personal Data Breach" on the form.
5. For any concerns or clarifications, you may contact the Data Privacy Office via email at legal.northernsamar@deped.gov.ph

6. Immediate and wide dissemination of this Memorandum is desired.

GAUDENCIO C. ALJIBE, Jr, PhD, CESO V
Schools Division Superintendent

DepEd Northern Samar
RELEASED
By:
Date: 02 JUL 2026

DepED DEPARTMENT OF EDUCATION
BAGONG PILIPINAS
Address: Mabini St., Brgy. Acacia, Catarman, 6400, Northern Samar
Telephone Nos: (055) 500 1020
Email Address: northernsamar@deped.gov.ph
Division Official Website: https://northernsamar.deped.gov.ph

RECOMMENDED TEMPLATE FOR INITIAL DOCUMENTATION OF SECURITY INCIDENT

In with the Department of Education's ASIR and QSIR documentation requirements, all offices are expected to properly document security incidents within their jurisdiction. All concerned offices are requested to immediately act on identified incidents, implement the appropriate response protocols, and report to the Data Privacy Office by 12:00 noon of the next day following discovery.

Initial documentation is necessary to ensure that confirmed details of the incident are promptly recorded and tracked, even while investigation is ongoing. Additional information and supporting documents may be submitted as they become available. Offices are encouraged to use the prescribed template for consistency; however, offices with existing documentation formats may continue to use their own, provided that all required details reflected in this template are sufficiently captured.

Name of Office	
Focal Person for the Incident *Indicate Name, Position, Contact Details, and Email Address*	
Date and Time of the Incident	
Date and Time of the Discovery	
Security Incident Occurred *Indicate the Nature of the Breach, Incident that Occurred, Data System involved, and its description*	
Security Incident Tag *Select one (1) security tag that is most applicable to the Security Incident.*	_____a. Theft _____b. Identify Fraud _____c. Sabotage of Physical Damage _____d. Malicious Code _____e. Hacking or Logical Infiltration Occurred _____f. Misuse of Resources _____g. Hardware Failure _____h. Software Failure _____i. Communication Failure _____j. Natural Disaster _____k. Design error _____l. User Error _____m. Operation Error _____n. Software Maintenance Error _____o. Third Party or Service Provider _____p. Others: _____

Does the Incident involve personal data?	□ **Yes** □**No** Details of the Data Involved: --- --- ---
System Involved	Select which electronic database is involved: □None □Local System □Department-wide System Name of the System:
Are there any indicators that the network and/or data processing systems were compromised?	□ **Yes** □**No** Details of the System Involved: --- --- ---
Was the internal investigation conducted to validate the alleged breach? *Please provide the timeline, investigation action taken, and initial findings.*	□ **Yes** □**No** **I. Incident Overview** **II. Discovery and Immediate Response** **III. Technical Findings and Scope of Impact** **IV. Precautionary Actions and Data Subject Notification (If Applicable)** **V. Conclusion and Recovery**
Security measures implemented both before and after breach *For Security Measures, you may refer the DICT Playbook or the National Privacy Toolkit.*	**I. Precautionary Measure implemented prior to the security incident** **II. Action Taken during the Security Incident** **III. Recommendations and Ways Forward after the Security Incident**
Other Relevant Details	

Republic of the Philippines

Department of Education

REGION VIII

SCHOOLS DIVISION OF NORTHERN SAMAR

ANNEX A

Annual Security Incident Report for PICs

SUMMARY

Annual Security Incident Reports

January – December 2025

Sector: _____ **City/Municipality:** _____ **Province:** _____

PIC (Individual and Organization) _____

Name of DPO _____

PERSONAL INFORMATION CONTROLLER

A. Personal Data Breach, Mandatory Notification	
B. Personal Data Breach, not covered by mandatory notification requirements	
C. Other Security Incidents	
D. Total Security Incidents (D=A+B+C)	

How Security Incidents Occurred

Types	***Number***	**Types**	***Number***
Theft	<_____>	Communication Failure	<_____>
Fraud	<_____>	Fire	<_____>
Sabotage/Physical Damage	<_____>	Flood	<_____>
Malicious Code	<_____>	Design Error	<_____>
Hacking/Logical Infiltration	<_____>	User Error	<_____>
Misuse of Resources	<_____>	Operating Error	<_____>
Hardware Failure	<_____>	Software Maintenance Error	<_____>
Software Failure	<_____>	Third Party Services	<_____>
Hardware Maintenance Error	<_____>	Others	<_____>

Personal Data Breach

	Confidentiality	**Integrity**	**Availability**
Mandatory Notification Required	<_____>	<_____>	<_____>
Mandatory Notification Not Required	<_____>	<_____>	<_____>

PREPARED BY: _____ EMAIL: _____

DESIGNATION: _____ CONTACT NO.: _____

DATE: _____

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 Departments compliance with the Data Privacy Act of (RA 10173) and related National Privacy commission (NPC) issuances.

Specifically, the implementation of QSIR aims to:

a. **Ensure prompt, consistent, 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 NPCC or affected data subject becomes necessary.;
b. **Promote accountability and awareness among offices and personnel** by reinforcing the shared responsibility of recognizing, reporting, and managing security incidents involving personnel 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 trend, 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.

1. **What is a Security Incident?**
   A Security Incident is an event or occurrence that effects or tends to affects data protection, or may compliments 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, or otherwise processed.

All personal data breaches are essentially security incidents. A security incidents 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 unlawful destruction to personal data.

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

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

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 refers to security incident 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 whether notification is indeed necessary, consider:

1.) The likelihood of harm or negative consequences on the affected data subject;
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 that type of incident or resulting impact, not the underlying cause. All security incident must be assigned the tag that the best describes the incidents.

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 component 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 transaction, registration, or identity misuse are detected
c. Sabotage or Physical Damage	• Systems, servers, or facilities were deliberately damage • 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 misconfiguration happened
f. Misuse of Resources	• Authorized users used systems or data outside their permitted purpose

	• Insider misuse, excessive privilege abuse, or policy violation 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 occurred • Affected access to or transmission of personal data
j. Natural Disaster	• Incident 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	• Incident resulted from unintentional actions of user • No malicious intent
m. Operation Error	• Errors occurred during routine operations • Procedural lapses or mis-execution occurred
n. Software Maintenance Error	• Incident 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/*