



Republic of the Philippines
Department of Education
REGION VII – CENTRAL VISAYAS
DIVISION OF CITY SCHOOLS – TAGBILARAN CITY

**Office of the Schools Division
Superintendent**

DIVISION MEMORANDUM
No. 499 s.2026

JUNE 25, 2026

TO : **All Public Elementary and Secondary School Heads**
All Section/Unit Heads
All Others Concerned

**SAFEGUARDING PERSONAL INFORMATION BY IMMEDIATE
REPORTING OF ANY SECURITY INCIDENT RELATIVE TO DATA BREACHES
THROUGH SUBMISSION OF THE SECURITY
INCIDENT REPORT**

1. In line with the Department of Education's (DepEd) commitment to safeguard personal information, sensitive personal information, and privilege information protected under the Data Privacy Law, the DepEd Tagbilaran City Division through the designated Compliance Officer for Privacy is mandated to comply and submit the Annual Security Incident Report (ASIR) to which compliance thereof shall be done quarterly to be submitted to the Department of Education-Data Privacy Office, pursuant further to the reportorial requirements of the Data Privacy Act, its IRR, and all related issuances by the NPC pertaining to personal data breach notification.
2. Relative to such mandate, the above-mentioned concerned offices, officers and personnel shall be duty bound to report and submit a **Security Incident Report** to the office of the **Compliance Officer for Privacy** relative to any security incidents either classified according to their causes and as to whether they are considered mandatory or voluntary data breach notifications or other security incidents. (See Annex A).
3. 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.
4. 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. A personal data breach may be in the nature of:



Republic of the Philippines
Department of Education
REGION VII – CENTRAL VISAYAS
DIVISION OF CITY SCHOOLS – TAGBILARAN CITY

**Office of the Schools Division
Superintendent**

- I. **Confidentiality** breach resulting from the unauthorized disclosure of or access to personal data.
 - II. **Integrity** breach resulting from alteration of personal data; and/or
 - III. **Availability** breach resulting from loss, accidental or unlawful destruction of personal data.
5. An **Annual Security Incident Report (ASIR)** is a report to the Commission containing all security incidents and personal data breaches in a calendar year, including those not covered by the mandatory notification requirements. ASIRs shall be submitted to the Commission annually and contain the following information: number of incidents and breach encountered; and number of incidents classified according to their causes and as to whether they are considered mandatory or voluntary data breach notifications or as other security incidents.
6. **Rights as a data subject.** Under the Data Privacy Act of 2012, you have the right to be informed, to access, to object to the processing of your data, to rectify errors, to suspend or withdraw your data, to data portability, and to lodge a complaint before the National Privacy Commission.
7. For further inquiries and concerns, visit the office of Atty. Tammy I. Relampagos the designated Compliance Officer for Privacy.
8. Immediate and wide dissemination of this Memorandum is desired.

WILFRERDA D. BONGALOS PhD, CESO V
Schools Division Superintendent



Republic of the Philippines
Department of Education
REGION VII – CENTRAL VISAYAS
DIVISION OF CITY SCHOOLS – TAGBILARAN CITY

ANNEX "A"

SECURITY INCIDENT REPORT	
Incident Overview	
Reported By: [Name and Signature]	
Date & Time of Incident:	
Date & Time of Discovery:	
Department/Unit:	
Type of Incident:	
Confidentiality (e.g., unauthorized access, data leak)	
Integrity (e.g., unauthorized alteration or modification)	
Availability (e.g., ransomware, accidental deletion, system crash)	
Description of How it Happened: [Provide a detailed narrative of the event, including the root cause and circumstances of discovery.]	
Systems/Assets Affected: [e.g., Servers, physical documents, laptops, databases]	
Impact & Scope	
Data Subjects Involved: [Number of individuals affected, e.g., employees, clients, students]	
Personal Data Involved: [List exact data categories, e.g., names, medical records, financial details, government IDs]	
Are sensitive personal data exposed? [Yes/No - if yes, this usually triggers mandatory notification] [	
Response & Actions Taken	
Containment Measures: [What immediate steps were taken to stop the breach or recover data?]	
Root Cause Analysis: [Why did this happen? (e.g., physical theft, phishing, system misconfiguration, lost device)]	
Compliance & Notifications	
Has the Data Protection Officer (DPO) been notified? [Yes/No, Date/Time]	



H. Zamora St., Dampas, Tagbilaran City, Bohol
(038)427-1702; (038)427-2506
tagbilarancity.division@deped.gov.ph



Republic of the Philippines
Department of Education
REGION VII – CENTRAL VISAYAS
DIVISION OF CITY SCHOOLS – TAGBILARAN CITY

ANNEX "A"

Are affected data subjects notified? [Yes/No - Required within 72 hours under NPC regulations if there is a real risk of harm]	
Has the National Privacy Commission (NPC) been notified? [Yes/No]	
Recommendations & Prevention	
Preventative Measures: [Actions to prevent recurrence, e.g., revised access policies, additional employee training, system patching]	