DATA PROTECTION COMMISSION

www.dataprotection.org.gh

INCIDENT / DATA BREACH REPORT FORM

Where there are reasonable grounds to believe that the personal data of a Data Subject has been lost, damaged or accessed or acquired by an unauthorized person, the Data Controller or a Third Party who processes data under the authority of the Data Controller shall notify the Commission. Section 31, Data Protection Act, 2012 (**ACT 843**).

Please fill out the template below by providing adequate responses. The completed template must be forwarded to incidents@dataprotection.org.gh without any delay.

Note: Kindly proceed to www.dataprotection.org.gh to register/ renew with the Data Protection Commission (DPC) if you have not already registered.

1. OVERVIEW	
Name of Institution	
Industry/Sector:	
Date of Incident (Date & Time discovered)	
Date of Reporting to the Commission	
Report type (Initial / Follow-up)	
Reported By: (Name & Role)	
Correspondence channel (e-mail, contact no.& office address)	
Priority / Risk Level	
2. DESCRIPTION OF INCIDENT	
How did the incident occur?	
How was the incident discovered / identified?	
Did this incident result in a data breach?	
What is the extent/ impact of the breach?	
Was the breach caused by a manual or cyber incident?	
What was the volume of Data involved?	
What category (ies) of Personal Data was breached/compromised? (financial, academia, etc.)	
Was there any sensitive/ special category of data involved? (child data, medical records, ethnic record, religious, etc.)	

Was the incident / breach caused by an unauthorized access or a privileged user?	
Has the unauthorized / privileged user been identified?	
3. DATA SUBJECTS AFFECTED	
How many Data Subjects were affected?	
What category of Data Subjects were affected?	
Have Data Subjects been informed of this breach?	
Is this breach likely to result in a high risk to the privacy rights to data subjects?	
4. SECURITY SAFEGUARD ACTIONS	
What were the Security Measures in place prior to the breach?	
Has the breach been contained? (if yes, how?)	
Has your institution undergone any Data Protection Audit?	
5. MITIGATION MEASURES	
Has the lost / damaged/ breached data been recovered?	
What is the Recovery & Business Continuity Plan?	
What future measures have been put in place to prevent further occurrence of this breach? (indicate timelines where necessary)	
Has there been any staff training on data protection & security safeguards?	

Has any other Agency or Organization been notified of this breach	
6. SUBMISSION OF RELEVANT DOCUMENTS	
List documents attached & submitted to report. (Evidence of all actions taken i.e. notification of data subjects, reports of investigation, assessments, etc.)	
7. REMARKS (FOR DPC USE ONLY)	