REPORTING A BREACH OR INCIDENT REPORT

DATA BREACH/INCIDENT REPORT NO. 2021 - ____

In the event of personal data breach or security incident occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimize the impact of the breach and prevent a recurrence.

If an employee/staff/subcontractor/intern of CIBI becomes aware of an actual, potential or suspected breach of personal data security, he/she must report the incident to its Unit Head and the Unit had to report such an incident to databreach@cibi.com.ph

Please refer to the Personal Data Breach Management Procedure Manual in filling out this report, herein attached as Appendix 2.

Section 1: Notification of Data Security Breach (To be completed by Unit Head of the person reporting incident)	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information breached or lost:	
Number of Data Subjects affected, if known:	

Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	

FOR DATA PRIVACY MANAGEMENT TEAM USE	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity (To be completed by the Lead Investigator in consultation with Supervisor/Unit head of area affected by the breach and Data Privacy Management Team)	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the Information lost?	
How much data has been lost? If laptop was lost/stolen: how recently was the laptop backed up onto central IT systems?	

Is the information unique? Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for CIBI or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data - Sensitive personal data (as defined in Data Privacy Act of 2012) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings	
- Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as government issued IDs and copies of passports and visas;	
- Detailed profiles of individuals including information about work performance, salaries or personal life	

that would cause significant damage or distress to that person if disclosed;	
Security information that would compromise the safety of individuals if disclosed.	
Category of incident (1, 2a, 2b or 3):	
Reported to Data Protection Officer on:	
If level 2b or level 3, must be escalated by Lead Investigator to CIBI's Data Privacy Critical Response Team	

Section 3: Action Taken To be completed by Data Protection Officer	
Breach/Incident number	
Report received by:	
Action taken by responsible officer/s:	
Was the incident reported to NPC?	Yes/No If yes, notified on (date):
Follow up action required/recommended:	
Reported to Data Protection Officer on (date):	
Reported to other internal stakeholders (details, dates):	

FOR USE OF DATA PROTECTION OFFICER:	
Notification to National Privacy Commission	Yes/NO. If Yes, notified on: Details:
Notification to data subjects	Yes/NO. If Yes, notified on: Details:
Notification to other external, regulator/stakeholder	Yes/NO. If Yes, notified on: Details:

Reviewed and Updated January 2021
Version 2

APPENDIX 1 – CHECKLIST FOR ASSESSING SEVERITY OF THE INCIDENT

How serious is the incident?

Level 1: Local Incident:

- Is this a local incident?
  - Local incident = limited disruption to services; no serious threat to the privacy of individuals; no threat to CIBI being sued by data subject or client for data privacy breach
- Can the consequences of the privacy breach, loss or unavailability of the asset be managed locally within normal operating procedures?
- If so, manage the incident according to the Data Security Breach Management Procedure

Level 2.a: Minor Emergency Type A – Unlikely to Escalate into a Major Emergency:

- Is this a Minor Emergency (type A)?
  - Minor Emergency (type A) = Disruption to the functioning capacity of a key service. Situation or incident (actual or potential) which poses a threat to the privacy of an individual/s at a minor level but may escalate to Type B.
- Do containment and recovery require assistance from other members of staff within CIBI or support teams outside CIBI?

- Does the breach require a notification to the CIBI's senior managers?

- If so, the Lead Investigator (liaising with the Data Privacy Management Team) will decide who else needs to assist or be made aware of the breach e.g. Chief Financial Officer, President and CEO & Head of Information Security and so on.

Level 2.b: Minor Emergency Type B or Level 3: Major Emergency

- Is this a major incident?
- Does this involve a breach where personal data has been put at risk for identity fraud, acquired by unauthorized person; and there is reason to believe that the unauthorized acquisition is likely to give rise to a real risk of serious harm;
- Does containment and recovery, or the consequences of the loss or unavailability of the asset, data privacy impact to individuals require significant CIBI resources beyond normal operating procedures?
- If so, escalate the incident to the Critical Response Team to email address: criticalbreach@cibi.com.ph

The incident level is defined by:

- Does the incident need to be reported immediately to the NPC? It falls under the criteria for reporting under NPC Circular 16-03 (Personal Data Breach Management), all incidents in which personal data has been put at risk for identity fraud, acquired by unauthorized person; and there is reason to believe that the unauthorized acquisition is likely to give rise to a real risk of serious harm?

- How important an information asset is to the CIBI business process or function
- Whether the asset is a vital record. Is it unique – once lost, lost forever? Will its loss have adverse financial legal, liability or reputational consequences to CIBI?
- Is it business-critical? Do you rely on access to this particular information asset or you can turn to reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable.
- How urgently access would need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service
- Does the loss or breach of data security involve high risk personal data, i.e.:

    - Sensitive personal data (as defined in the Data Privacy Act) relating to an identifiable individual's
        a) racial or ethnic origin;
        b) sex or gender
        c) political opinions or religious or philosophical beliefs;
        d) Medical condition/ physical or mental health or condition
        e) sexual life;
        f) commission or alleged commission of any offence, or
        g) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
    - Information that could be used to commit identity fraud such as personal bank account and other financial information and Government Issued IDs and copies of passports and visas;
    - Personal information relating to vulnerable adults and children;
    - Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;
    - Security information that would compromise the safety of individuals if disclosed.

Reviewed and Updated January 2021
Version 2

APPENDIX 2 – PERSONAL DATA MANAGEMENT BREACH PROCEDURE GUIDELINES

1. INTRODUCTION

CIBI Information, Inc. ("CIBI") is obliged under the Data Privacy Act of 2012 and its Implementing Rules and Regulations to keep personal data safe and secure and to respond promptly and appropriately to data security breaches (including reporting such breaches to the National Privacy Commissioner in certain cases). It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to CIBI.

2. PURPOSE

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data (defined below) held by CIBI. These procedures are a supplement to the CIBI's Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

3. WHAT IS A PERSONAL DATA SECURITY BREACH?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by CIBI in any format. Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorized individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorized use of information;
- suspected breach of the CIBI's IT security and Acceptable Use policies;
- attempts to gain unauthorized access to computer systems, e.g. hacking;
- records altered or deleted without authorization by the data "owner";
- viruses or other security attacks on IT equipment systems or networks;'
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive information sent in error to the wrong recipient.

4. WHO DO THESE PROCEDURES APPLY TO?

These procedures apply to all users of CIBI data, including:

- any person who is employed by CIBI or is engaged by CIBI who has access to CIBI data in the course of their employment or engagement for administrative, research and/or any other purpose;
- Management Committee

- any student/intern/trainee of CIBI who has access to CIBI/Client data in the course of their internship for administrative, research and/or any other purpose;
- individuals who are not directly employed by CIBI, but who are employed by contractors (or subcontractors) and who have access to CIBI/Client data in the course of their duties

hereinafter, collectively referred to as "Members".

5. WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?

These procedures apply to:

- all personal data created or received by CIBI in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;

- personal data held on all CIBI IT systems managed centrally by the IT Department, and locally by the individual CIBI Sites;

- personal data accessed by CIBI Members as part of the service provided to its clients;

- any other IT systems on which CIBI data including Client data accessed by CIBI members is held or processed.

6. WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES?

Personal data security breaches are managed by the Data Privacy Management Team composed of the Information Security Officer, Data Protection Officer, Legal Compliance Officer and HR Employee Relationship Officer. In emergency situations, CIBI's Critical Response Team will take over responsibility for managing the incident. The Critical Response Team is composed of the President and CEO, Chief Financial Officer, and VP for Sales.

	Data Privacy Organizations	Members
1	Data Privacy Management Team	• Information Security Officer • Data Protection Officer • Legal Compliance Officer • HR Employee Relationship Officer
2	Critical Response Team	• President and CEO • Chief Financial Officer • VP for Sales
3	Lead Investigator	• To be appointed by the Data Privacy Management Team

7. PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimize the impact of the breach and prevent a recurrence.

If a member of CIBI becomes aware of an actual, potential or suspected breach of personal data security, he/she must report the incident to its Unit Head and the Unit had to report such an incident to databreach@cibi.com.ph

8. PROCEDURE FOR MANAGING DATA SECURITY BREACHES

In line with best practice, the following five steps should be followed in responding to a data security breach:

Step 1: Identification and initial assessment
Step 2: Containment and Recovery
Step 3: Risk Assessment
Step 4: Notification
Step 5: Evaluation and Response

STEP 1: Identification and Initial Assessment of the Incident
If a member of CIBI considers that a data security breach has occurred, this must be reported immediately to the Unit Head. The Unit Head must inform the Data Privacy Management Team about the incident by sending an email: databreach@cibi.com.ph. The Unit Head should submit a Data Security Breach Report Form (Appendix 1) without delay. The Report Form will assist the Data Privacy Management Team in conducting an initial assessment of the incident by establishing:

- if a personal data security breach has taken place; if so:
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected);
- the harms to affected individuals that could potentially be caused by the breach;
- how the breach can be contained.

Following this initial assessment of the incident, the Data Privacy Management Team will investigate the incident or appoint an investigator (e.g. IT Head for IT-related incidents, etc.) and will decide if it is also necessary to appoint a group of relevant CIBI stakeholders to assist with the investigation. Any records relating directly to an investigation will be retained by the Data Privacy Management Team The Lead Investigator (if appointed), liaising with the Data Privacy Management Team will determine the severity of the incident using the checklist in Appendix 2 and by completing Section 2 of the Data Security Breach Report Form (Appendix 1) (i.e. s/he will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to CIBI's Critical Response Team to email address: criticalbreach@cibi.com.ph.

The severity of the incident will be categorized as level 1, 2a, 2b or 3.

Level 1 classed as a Local Site Incident	Both managed and controlled by the Data Privacy Management Team
Level 2 (a) classed as a Minor Emergency Type (A)	
Level 2 (b) classed as Minor Emergency Type (B)	
Level 3 classed as a Major Emergency	Escalated to Critical Response Team which is responsible for the management and close out of the incident

Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, CIBI needs to take immediate and appropriate action to limit the breach.

The Lead Investigator, liaising with the Data Privacy Management Team and relevant CIBI members/managers, will:

- Establish who within the CIBI needs to be made aware of the breach (e.g. IT Services, Operations, Legal, Sales Office) and inform them of what they are expected to do to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.)
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).
- Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of serious harm to individuals).
- Where appropriate (e.g. in cases involving theft or other criminal activity), inform the National Privacy Commission.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant CIBI stakeholders are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialize and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage.

The Lead Investigator and Data Protection Officer in conjunction with the head of unit/function/CIBI site in which the incident occurred will review the incident report to:

- Assess the risks and consequences of the breach:
  - Risks for individuals:
    - What are the potential adverse consequences for individuals?
    - How serious or substantial are these consequences?
    - How likely are they to happen?

- Risks for CIBI:
  - Strategic & Operational
  - Compliance/Legal
  - Financial
  - Reputational
  - Continuity of Service Levels

- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The Lead Investigator and Data Protection Officer will prepare an incident report setting out (where applicable):

- a summary of the security breach;
- the people involved in the security breach, (such as employees, contractors, external clients, vendors);
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;
- unrealized, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action;
- recommendations for future actions and improvements in data protection as relevant to the incident.

The incident report will then be furnished to the Head of the Unit (as appropriate) affected by the breach. Such Head will request relevant employee to update the risk registers at the appropriate levels where necessary. Any significant risks will be reported to the Data Privacy Management Team.

Step 4: Notification

On the basis of the evaluation of risks and consequences, the Data Protection Officer and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside CIBI. For example:

- individuals (data subjects) affected by the breach;
- the National Privacy Commission;
- other bodies such as regulatory bodies
- corporate counsel.

As well as deciding who to notify, the Data Protection Officer must consider:

- What is the message that needs to be put across?

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved;
- what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the Data Protection Officer should give specific and clear advice on what steps they can take to protect themselves, what CIBI is willing to do to assist them and should provide details of how they can contact CIBI for further information (e.g. contact information details of the DPO in the CIBI website).

- How to communicate the message?

What is the most appropriate method of notification (e.g. are there large numbers of people involved? Does the breach involve sensitive data? Is it necessary to write to each individual affected? Is it necessary to seek legal advice on the wording of the communication?).

- Why are we notifying?

Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

In accordance with National Privacy Commission Circular 16-03 (Personal Data Breach Management), all incidents in which personal data has been put at risk for identity fraud, acquired by unauthorized person; and there is reason to believe that the unauthorized acquisition is likely to give rise to a real risk of serious harm must be reported to the National Privacy Commission within 72 hours from knowledge of the personal data breach, based on available information. Follow up report should be submitted within five (5) days from knowledge of the breach, unless allowed a longer period by the Commission

Any contact with the National Privacy Commission should be made through the Data Protection Officer. Initial contact with the Commission should be made by the Data Protection Officer within two working days of becoming aware of the breach, outlining the circumstances surrounding the incident. This initial contact may be by e-mail and must not involve the communication of personal data. In cases where the decision is made by the Lead Investigator and Data Protection Officer/ not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the Commissioner will be retained by the Data Protection Officer.

Step 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the Data Privacy Management Team in consultation with the relevant stakeholders in CIBI will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved. All data security breach reports should be sent to the Data Privacy Management Team who will use these to compile a central record (log) of incidents. The Data Protection Officer will report on incidents to Management Committee at least on a quarterly basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed. For each serious incident, the Data Privacy Management Team and Data Protection Officer will conduct a review to consider and report to the Board on the following:

- What action needs to be taken to reduce the risk of future breaches and minimize their impact?
- Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are employees and users of data aware of their responsibilities for information security and adequately trained?
- Is additional investment required to reduce exposure and if so what are the resource implications?

CIBI reserves the right to amend or revoke these procedures at any time without notice and in any manner in which CIBI sees fit at the absolute discretion of CIBI.