



**SHAKEY'S PIZZA ASIA VENTURES INC.**  
 15KM East Service Road, Brgy. San Martin de Porres, Paranaque City 1700  
 www.shakeyspizza.ph

# BREACH REPORTING GUIDELINES For EMPLOYEES

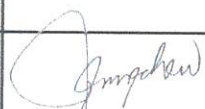
Version 01.2024

## Document History:

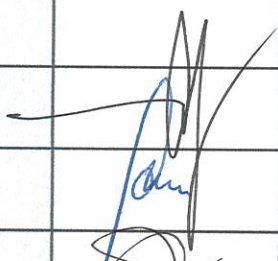



- Revision Number 00 always means Official Release
- For Revision Number 01 onwards, Description of Change must indicate which Section Numbers have been revised.

Revision Number	Description of Change	Author	Signature	Issued Date
00	Official Release			

## Reviewed by:

Department	Name	Designation	Signature	Date
Legal	Atty. James Earl Chew	DPO		

## Approved by:

Designation	Name	Signature	Date
President and Chief Executive Officer	Vicente L. Gregorio		
Chief Finance Officer	Manuel T. Del Barrio		
Chief Operating Officer	Jorge Ma. Q. Concepcion		5/20
Chief Human Resource Officer	Ma. Elma C. Santos		5/20

---

## 1. Purpose

The purpose of these Guidelines is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g. to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

---

## 2. Scope

This document applies to all possible and identified security events, incidents and breaches which involve processing of personal data through electronic or non-electronic means across Shakey's Pizza Asia Ventures, Inc. and its subsidiaries (hereafter referred to as "the Group"). The procedures provided in this document is intended to apply to all staff and service providers of the Group. The Group has the following subsidiaries:

- Shakey's Pizza Commerce Inc.
- Shakey's Seacrest Inc.
- Wow Brand Holdings Inc.

---

## 3. Audience

This policy applies to all employees who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle the personal data in addition to the Breach Response Team and other teams involved in supporting the Security Incident / Breach response process.

---

## 4. Policy

These Guidelines are intended to complement the Group's Breach Management and Reporting Policy. This policy requires employees who suspect that a theft, breach, or exposure of Personal Information has occurred in connection with the Group's processing of Personal Data, must report such incident **within 24 hours** from knowledge of the said incident or breach and provide a description of what occurred to the Breach Response Team (BRT). This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the BRT will follow the appropriate procedure in place.

An overview of the breach reporting process is provided in Annex 01.

---

## 5. Definitions

Data Subject	Employees, customers, suppliers, or other external parties whose personal data are processed by the Group.
Personal Data	Collective term for personal information and sensitive personal information, including privileged information

Personal Data Breach	Any 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
Personal Information	Any information from which the identity of an individual can be reasonably and directly ascertained, or when put together with other information would certainly and directly identify an individual
Personal Information Controller or PIC	Any natural or juridical person, including the Group, who/which controls the collection, holding, processing and use of Personal Data, or instructs another person to process Personal Data on its behalf
Personal Information Processor or PIP	Any natural or juridical person, or any other body, to whom a PIC, which may include the Group, outsources, or gives instructions as regards the Processing of Personal Data of a Data Subject or group of Data Subjects
Processing	Any operation performed on personal data including, but not limited to, collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data
Security Incident	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
Sensitive Personal Information	Personal information that is: <ol style="list-style-type: none"> <li>1. About an individual's race, ethnic origin, marital status, age, color, religious, philosophical or political affiliations;</li> <li>2. About an individual's health, education, genetic or sexual life, any proceeding for any offense committed or alleged to have been committed by such individual, disposal of such proceedings, or sentence of any court in such proceedings;</li> <li>3. Issued by government agencies peculiar to an individual which includes, but not limited to, SSS numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; or</li> <li>4. Specifically established by an Executive Order or an act of Congress to be kept classified</li> </ol>

---

## 6. Data Breaches and Security Incidents

**Data breach** is 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.

Under the Data Privacy Act of 2012, 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.

Examples of Data Breaches:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information;
- unauthorized access to personal information by an employee;
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person; and

- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

**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 includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

Examples of Security Incidents:

- malicious code;
- hacking/logical infiltration;
- misuse of resources
- hardware failure
- software failure
- hardware maintenance error
- software maintenance error
- Theft;
- Identity Fraud;
- Sabotage/ Physical Damage;
- Malicious Code;
- Hacking;
- Communication Failure;
- Natural Disaster;
- Design Error;
- User Error;
- Operations Error;
- Software Maintenance Error;
- Third Party/Service Provider; and
- Others.

Examples of Data Breaches and Notification and Communication Requirements are provided in Annex 02.

---

## **7. Detecting a Data Breach**

Personal Data Breaches can be detected through:

1. Reporting by an employee, agent or Personal Information Processor (PIP) of the Group;
2. Reporting by clients, customers of the public;
3. Reporting or alert by third parties including Law Enforcement, Government Regulatory Authorities (e.g., the NPC) or through social media posts; OR
4. Internal detection as a result of monitoring by the IT/Cybersecurity team.

---

## **8. Reporting a Security Incident or Suspected Data Breach**

**Responsibility of Employees.** All employees and agents of the Group involved in the processing of Personal Data are tasked with regularly monitoring for signs of security incidents or a potential data breach. In case of doubt as to whether an incident is a Security Incident or a Data Breach, report the incident as soon as possible.

**Who to Report to.** Reports of Security Incidents or (potential) Data Breaches may be reported to:

1. DPO
2. COP of your Business Unit or department
3. Immediate superior or Department Head
4. IT Department

**How to Report.** Reports of Security Incidents or (potential) Data Breaches may initially be made by a Data Subject in two ways:

Report to the head of the relevant BU/department or directly to the DPO or COPs. Reporting Party shall fill out the Security Incident Report Form. The form may be obtained from the DPO.

Report the Security Incident or suspected Data Breach by clicking the link to the Security Incident Report form in the *Contact Us* portion in the Privacy Policy page on the SPAVI Website.

Report a Security Incident or suspected Data Breach to the Information Security Department. Reports to the InfoSec Department will usually involve IT or system-related incidents. Upon reporting, the InfoSec Department will interview the Reporting Party and assess whether Personal Data is involved.

If Personal Data is involved, the InfoSec team shall report the matter to the DPO within twenty-four (24) hours from the initial report. The DPO shall then inform the Breach Response Team to conduct assessment on whether there is an actual data breach.

**What to Report.** The report or Security Incident Report form (see Annex 03) must contain the following information:

- a. Name of individual reporting the incident or event
- b. Contact information of individual
- c. Summary of the reported incident
- d. Date and time of receipt of report
- e. Date and time of detection of incident or suspected data breach

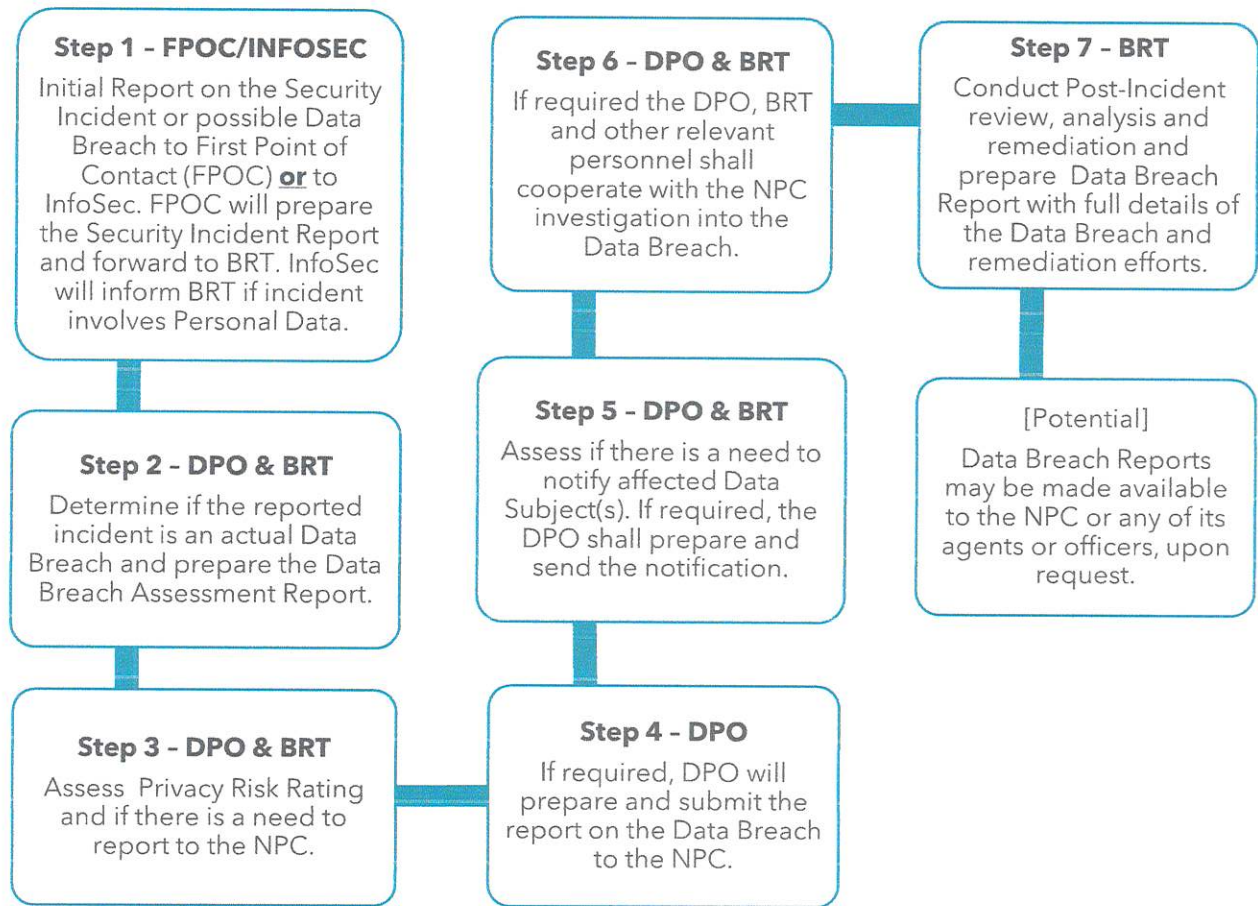
If necessary, you may be required to provide further assistance or information.

**When to Report.** The Security Incident or suspected Data Breach must be reported as soon as possible after discovery or within 24 hours upon knowledge of, or receipt of information on, any suspected security incident involving personal data.

**Why is there a need to report as soon as possible.** Under the DPA, serious breaches, especially those involving sensitive personal information, must be reported to the *National Privacy Commission* (the regulator) within 72 hours from knowledge

or discovery. The DPA penalizes the concealment of security breaches involving sensitive personal information or information subject of notification requirements (Sec. 30, DPA)

**ANNEX 01 – Procedure for Data Breach Reporting**





## ANNEX 02- Examples of Security Incidents and Data Breaches and the Notification & Communication Requirements

Example	Notify the COP/DPO	Notes/recommendations
An employee stored a backup of an archive of personal data encrypted on a USB Drive. The USB Drive is stolen during a break-in.	No.	As long as the data are encrypted, backups of the data exist, and the unique key is not compromised, this is not a reportable breach. However, if the employee suspects that there has been unauthorized access or if it is later compromised, notification is required.
Personal data of individuals are ex-filtrated from a secure website managed by the controller during a cyber-attack.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high.	If the risk of harm or damage to data subjects is not high, the data subject may need to be notified, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed.
A brief power outage lasting several minutes meaning personal information controllers and custodians are unable to access the personal information records.	Yes.	This is not a notifiable personal data breach, but still a recordable security incident. Electronic records and files should be checked to verify that no data was lost or corrupted. Appropriate records should be maintained by the BU/Department concerned.
An employee suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data and that there was no other malware present in the system.	Yes, report the IT Department.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, the IT Team may consider an investigation to assess compliance with the broader security requirements under existing Group policies.
A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients.	Yes.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.



**ANNEX 03 - List of DPO and COPS**

DPO Business Unit	DPO email
Group DPO; DPO for SPAVI	<a href="mailto:dpo@shakeys.biz">dpo@shakeys.biz</a>
WBHI	<a href="mailto:dpo@periperichicken.biz">dpo@periperichicken.biz</a>
SPCI	<a href="mailto:dpo@shakeys.biz">dpo@shakeys.biz</a>

**ANNEX 04- SECURITY INCIDENT REPORT FORM**

Ref. No. 001

**SECURITY INCIDENT REPORT**

Shakey's Pizza Asia Ventures, Inc.

This form should be used to report events or occurrences that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place. Such events include, but are not limited to:

- malicious code;
- hacking/logical infiltration;
- misuse of resources
- hardware and/or software failure
- hardware maintenance error
- loss of personal information or sensitive personal information
- suspected breach of IT security policies

<b>Details of Reporting Party</b>	
Employee ID (if SPAVI employee)	
Full Name	
Phone /Mobile number	
Email	
Department/Division	
If SPAVI Vendor:	
Name of Vendor	
Address of Vendor	

<b>Details of Incident</b>		
Date of Incident		
Time of Incident		
Location of Incident		
What personal data is involved?		
Is the incident arising internally or externally (at a vendor)?		
Is the incident still in progress?	Yes	No
Do you need immediate assistance from IT Security?	Yes	No
Has this incident already been reported to the IT Service Desk?	Yes	No
If yes, provide ticket number		
Date and time of report		

<b>Brief Description of the Incident</b>
Include details on what type of personal information is affected (or suspected to be affected) and number of individuals that could be affected)

<b>Comments</b>

<b>Prepared By:</b>	
First Point of Contact:	
Department:	Position:
Telephone/Mobile number:	Email:
Date:	Signature:

**Please forward to COP / DPO for evaluation and recording.**