	LA SALLE GREEN HILLS			
	DOCUMENT TITLE: LSGH Data Privacy Security Incident Management Policy		DOCUMENT NO:	CLASS:
	FILES SOURCE:	EFFECTIVE DATE:	APPROVAL DATE:	NO. OF PAGES: 7

APPROVAL HISTORY

Date (YYYY-MM-DD)	Prepared by:	Authorized by:	Approved by: (Secondary)	Approved by:
	Atty. Armee M. Javellana			

REVISION HISTORY

Revision Date (YYYY-MM-DD)	Author	Reason for Changes
		Initial Documentation

RELATED INFORMATION

Document Control No.	Document Title	File Source

TABLE OF CONTENTS

Section Title	Page Number
Introduction	1
Purpose	1
Objectives	1
Definition of Terms	1-2
Scope	2
Guideline Statements	2-7
References	

CONTROL STAMP

FOR CIAD USE ONLY

1. Introduction

   La Salle Green Hills (LSGH) is obliged under the Data Privacy Act of 2012 (RA 10173), to implement measures and procedures to guarantee to safety and security against unauthorized processing and against accidental loss, destruction or damage to personal information/data.

2. Purpose

The purpose of this policy is to ensure a consistent and effective approach to the management of Information Security Incidents and establishing a structure for the reporting and management of such incidents as required by NPC Circular No. 16-03 dated December 15, 2016.

3. Objectives

   3.1 To ensure that:

      3.1.1 Data lost, stolen, and inappropriately accessed or damaged is properly identified, reported, investigated, resolved and the risk of re-occurrence is minimized;

      3.1.2 Data breaches are assessed and responded to appropriately;

      3.1.3 Serious security breaches are reported to the National Privacy Commission (NPC)

      3.1.4 Lessons learned in the course of the incident/breach are communicated to the College community to prevent future incidents.

4. Definition of Terms

   4.1 Personal Data Breach – refers a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

   4.2 Security Incident – refers to 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 the safeguard that have been put in place

   4.3 A personal data breach may be in the nature of:

4.3.1 Availability breach resulting from loss, accidental or unlawful destruction of personal data

4.3.2 Integrity breach resulting from alteration of personal data

4.3.3 Confidentiality breach resulting form the unauthorized disclosure of or access to personal data

4.4. Personal data breach may include but is not limited to the following:

4.4.1 Unauthorized access of personal data from the College's server or through malicious attack;

4.4.2 Employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.)

4.4.3 Policy and/or systems failure (e.g., a policy that does not require multiple overlapping security measures – if back-up security measures are absent, failure of a single protective system can leave data vulnerable)

4.4.4 Loss through negligence, theft, robbery of hard drive disk, USB, laptop, personal computer, smart phone, any removable media containing one or more personal data.

4.4.5 Accidental or unauthorized access to student or associate data base

4.4.6 Inadvertent exposure of personal data in the College website, social media or public document

4.4.7 Direct loss or theft of personal data (e.g. papers taken from car, post intercepted, unauthorized download)

4.4.8 Accidental or unauthorized disclosure of personal data (e.g. via misaddressed correspondence or incorrect system permissions/filter failure)

4.4.9 Corruption or unauthorized modification of vital records (e.g. alteration of master records)

4.4.10 Computer system or equipment compromise (e.g. virus, malware, denial of service attack)

4.4.11 Compromised IT user account (e.g. spoofing, hacking, shared password)

4.4.12 Break in at a location holding personal Information or containing critical information processing equipment such as servers

5. Scope

This policy covers all associates, students or third party contractors of the College who have any type of access in the in information and communication system of the College. They must comply with the terms set out in this policy.

but posts added to private forums can also be shared publically by others.

6. Guideline Statements

6.1 Security Incident/Personal Data Breach Reporting

6.1.1 The severity of the incident shall be assessed and the management response shall be proportionate to the threat. Security incident will vary in impact and risk depending on the content and quantity of the data involved, the circumstances surrounding the incident, and the speed of response to the incident. Breaches, depending on its nature, can result to a penalty of imprisonment and fine.

6.1.2 All Information Security Incidents shall be managed in accordance with the Information Security Incident Management Response Procedure.

6.1.3 Key information about serious Information Security incidents, including the impact of the incident (financial or otherwise), shall be formally recorded and the records shall be analyzed in order to assess the effectiveness of information security controls.

6.1.4 New risks identified as a result of an incident and shall be assigned to the relevant risk owner and unacceptable risks shall be mitigated promptly in accordance with the College's risk management processes.

6.1.5 Not all data breaches have to be reported to the NPC. Only when these are all present:

6.1.5.1 There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;

6.1.5.2 The data is reasonably believed to have been acquired by an unauthorized person; and

6.1.5.3 Either the personal information controller or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

6.1.6 If there is doubt as to whether notification is indeed necessary, consider:

6.1.6.1 The likelihood of harm or negative consequences on the affected data subjects;

6.1.6.2 How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and

6.1.6.3 If the data involves:

6.1.6.3.1 Information that would likely affect national security, public safety, public order, or public health;

6.1.6.3.2 At least one hundred (100) individuals;

6.1.6.3.3 Information required by all applicable laws or rules to be confidential; or

6.1.6.3.4 Personal data of vulnerable groups.

6.2 Responsibilities

6.2.1 All members of LSGH are responsible for reporting actual or suspected Information Security Incidents to the TMC Help Desk or Data Protection Officer (DPO) in accordance with the Information Security Incident Reporting Procedure

6.2.2 Third-party contractors using LSGH's information systems and services shall be required to note and report any significant information security weaknesses in those systems or services.

6.3 Compliance

6.3.1 Failure to report an Information Security Incident and any other breach of this policy shall be considered to be a disciplinary matter and shall be reported to the Senior Information Risk Owner, Data Protection Officer and Human Resource Department to be addressed under the relevant disciplinary code.

6.3.2 Compliance with this policy should form part of any contract with a third party that may involve access to LSGH networks, computer systems or data. Failure by contractors to comply and may constitute an actionable breach of contract.

6.3.3 Immediately upon knowledge and discovery of the Security Incident/Personal Data Breach, the Employee or Student shall file a Data Breach Reporting Form within 24 hours from knowledge or discovery of personal data breach.

6.3.4 Based on the Data Breach Reporting Form, the Data Protection Officer (DPO) shall assess the reported incident and if verified that a breach has occurred, the DPO shall convene the Data Breach Response Team.

6.4 Composition of the Data Breach Response Team

6.4.1 The Data Breach Response Team shall be composed of the following:

6.4.1.1 Director for Administration (to ensure management's commitment to breach response planning and execution)

6.4.1.2 Head of Marketing and Communication or representative (to ensure an accurate account of any issues is communicated to stakeholders and the press)

6.4.1.3 Data Protection Officer (ensures that any evidence collected maintains its value in the event that the company chooses to take legal action and also provide advice regarding liability issues when an incident affects data subjects and/or the general public)

6.4.1.4 Head of Technological Management Center or representative (works directly with the affected network to research the time, location, and details of a breach)

6.4.1.5 Head of Safety and Security

6.4.1.6 Head of Department which was the source of breach or representative

6.4.2 The team shall be responsible for the following:

6.4.2.1 Evaluation of the security Incident and deciding on action to be taken including but not limited to restoration of integrity of the information and communication system, mitigation and remediation of any result damage, and compliance with the reporting requirements.

6.4.2.2 Coordination with the different departments/units of the College for the development of the overall incident response

6.4.2.3 Implementation of the Incident Security Incident Management Policy

6.4.2.4 Reporting actions taken on instances of personal data breaches to the Data Protection Officer within 24 hours from discovery

6.4.3 Upon receipt of the report from the Data Breach Response Team, the Data Protection Officer shall be responsible for the following:

6.4.3.1 Reporting instances of data breaches and corresponding action taken to the College Senior Management

6.4.3.2 Monitoring of resolution of personal data breaches

6.4.3.3 Notifying the National Privacy Commission and affected data subjects, upon clearance by the College Senior Management, within 72 hours upon knowledge, or what there is reasonable belief that a personal data breach occurred

6.4.4 The notification to the National Privacy Commission shall include the following information:

6.4.4.1 Description of the nature of the personal data breach

6.4.4.2 Personal data possibly involved

6.4.4.3 Measures taken by the College to address the personal data breach, including measures taken to reduce harm or negative consequence of the personal data breach

6.4.5 The notification to the data subjects shall include the following information:

6.4.5.1 Description of the nature of the personal data breach

6.4.5.2 Personal data possibly involved

6.4.5.3 Measures taken by the College to address the personal data breach, including measures taken to reduce harm or negative consequence of the personal data breach

6.4.5.4 Representation of College, including his or her contact details, from whom the data subject can obtain additional information regarding the breach

6.4.5.5 Any assistance to be provided on the data subjects

6.5 Action that may be taken by the Data Breach Response Team

6.5.1 Secure systems and fix vulnerabilities that may have cause the incident/breach.

6.5.2 Check network segmentation. Work with forensic experts to analyze whether the segmentation plan was effective in containing the breach and make the necessary changes if there is a need.

6.5.3 Remove improperly posted information form the web.

6.5.3.1 Immediately remove any involved personal information improperly posted on the website. Contact the search engines to ensure that personal information posted in error is not archived.

6.5.3.2 Search for the company's exposed data to make sure that no other websites have saved a copy. Contact those sites and request for the removal of the exposed data.

6.5.4 Hire independent forensic investigators to determine the source and scope of the breach through forensic images of affected systems, collection and analysis of evidence, and determination of remediation steps.

6.5.4.1 Work with forensic experts. Find out measures such as encryption were enabled when the breach happened. Analyze back-up or preserved data. Review logs to determine who had access to the data at the time of the breach. Analyze who currently has access, determine whether that access is needed and restrict access if it is not. Verifying the types of information compromised, the number of people affected, and the contact information of the people affected.

6.5.5 Stop additional data loss.

6.5.5.1 Put in offline mode all affected equipment but do not turn any machines off until forensic experts arrive. If possible, put clean machines on line in place of affected ones. In addition, update credentials and passwords of authorized users.

6.5.6 Do not destroy any forensic evidence in the course of the investigation and remediation.

6.5.7 Secure physical areas potentially related to the breach. Closely monitor all entry and exit points, especially those involved in the breach. Lock them and change access codes, if needed.

6.5.8 Interview people who discovered the breach. Ensure that the Contact Center knows where to forward the information that may aid the investigation of the breach. Document your investigation.

6.5.9 If service providers were involved examine what personal information they can access and decide if there is a need to change their access privileges. Ensure that the services providers take the necessary steps to make sure another breach does not occur and verify the actions taken to remedy these vulnerabilities.

6.5.10 Develop a communications plan that will reach all affected audiences (i.e. students, associates and stakeholders). Avoid misleading statements about the incident/breach. Do not withhold key details that might help data subjects protect themselves and their information. Do not publicly share information that might put data subjects at further risk.

6.5.11 Coordinate with the units responsible for the release of advisories/bulletins containing information on persons who committed the personal data breach, the modus operandi of the perpetrator and the steps for reporting the incident.

6.5.12 Coordinate with law enforcement agencies, if applicable.

Annex A

Data Privacy Security Incident Reporting Form

This document ensures that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to data subject and/or the College's data and information.

The checklist can be accomplished by an individual with knowledge of the incident. It will also require the review by the College's Data Protection Officer who will determine the implications of the Data Privacy Act of 2012, its Implementing Rules and Regulations and/or relevant order and other guidelines issued by the National Privacy Commission and address changes required to the existing processes.

Name of individual reporting: ___________________________

Department/Unit: ________________________________

Date: ________________________________+

Summary of the Incident

Data and Time of the Incident	
How many individuals or records are involved?	
Department/Division	
Nature of the breach: Confidentiality/Integrity/Availability This should be as detailed as possible (e.g. unauthorized access/processing)	

Description of how the breach happened	
What type of data is involved? (The individual data fields should be identified, e.g. name, address, bank account number, etc.)	
What happened to the data?	

Reporting

When was the breach reported?	
Were there any controls in place? (e.g. encryption, etc.)	
Who detected the breach?	
When was the breach isolated?	

Impact

What are the potential adverse consequences for students, associates, third parties, or DLS-CSB?	
What processes/systems are affected and how? (e.g. website taken off line, access to data base restricted, etc.)	
Have you received a formal complaint from any individual affected by this incident? If so, provide details.	

Management

What further action has been taken to minimize the possibility of a repeat of such an incident?	