
	LA SALLE GREEN HILLS			
	DOCUMENT TITLE: LSGH Data Privacy Security Incident Management Policy		DOCUMENT NO:	CLASS:
	FILES SOURCE:	EFFECTIVE DATE: 2022 June 18	APPROVAL DATE: 2022 June 18	NO. OF PAGES: 7

APPROVAL HISTORY

Date (YYYY-MM-DD)	Prepared by:	Authorized by:	Approved by: (Secondary)	Approved by:
2022 June 18	Atty. Armee M. Javellana RMCO Head Administrator			 Br. Edmundo L. Fernandez FSC LSGH President

REVISION HISTORY

Revision Date (YYYY-MM-DD)	Author	Reason for Changes
2022 June 15	Atty. Maria Armee M. Javellana Mr. Niccolo Paolo M. Agcaoli Mrs. Esther D. Dollete	In pursuant to the National Privacy Commission directive dated 08 June 2022 to revise the LSGH Data Privacy Policy.

RELATED INFORMATION

Document Control No.	Document Title	File Source

TABLE OF CONTENTS

Section Title	Page Number
Introduction	2
Purpose	2
Objectives	2
Definition of Terms	2-3
Scope	3
Guideline Statements	3-5
Data Privacy Security Incident Reporting Form	6-8

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 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 recurrence is minimized;
- 3.1.2. Data incidents breaches, including incidents are immediately acted upon, investigated, assessed and responded to appropriately according to this Policy;
- 3.1.3. Serious security breaches are reported to the National Privacy Commission (NPC);
- 3.1.4. The availability, integrity, and confidentiality of the Personal Data being processed through the School's information and communication system;
- 3.1.5. Lessons learned in the course of the incident/breach are communicated to LSGH community to prevent future incidents; and
- 3.1.6. To establish a Data Breach Response Team.

4. **Definition of Terms**

- 4.1. Personal Data Breach – refers to 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. Non-critical incident - refers to an incident that would only require inquiry or advice.
- 4.4. A personal data breach may be in the nature of:
 - 4.4.1. Availability breach resulting from loss, accidental or unlawful destruction of personal data;
 - 4.4.2. Integrity breach resulting from alteration of personal data
 - 4.4.3. Confidentiality breach resulting from the unauthorized disclosure of or access to personal data
- 4.5. Personal data breach may include but is not limited to the following:
 - 4.5.1. Unauthorized access of personal data from LSGH's server or through malicious attack;
 - 4.5.2. Employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguration of a security service or device, etc.);
 - 4.5.3. 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);
 - 4.5.4. Loss through negligence, theft, robbery of hard drive disk, USB, laptop, personal computer, smart phone, any removable media containing one or more personal data;
 - 4.5.5. Accidental or unauthorized access to student or personnel database;Inadvertent exposure of personal data in the LSGH's website, social media or public document;
 - 4.5.6. Direct loss or theft of personal data (e.g. papers taken from car, post intercepted, unauthorized download);
 - 4.5.7. Accidental or unauthorized disclosure of personal data (e.g. via misaddressed correspondence or incorrect system permissions/filter failure);
 - 4.5.8. Corruption or unauthorized modification of vital records (e.g. alteration of master records);
 - 4.5.9. Computer system or equipment compromise (e.g. virus, malware, denial of service attack);
 - 4.5.10. Compromised IT user account (e.g. spoofing, hacking, shared password);

- 4.5.11. Break in at a location holding personal information or containing critical information processing equipment such as servers.

5. **Scope**

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

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 incidents 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 in 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 shall be assigned to the relevant risk owner and unacceptable risks shall be mitigated promptly in accordance with the LSGH'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. **Incident Reporting Procedure**

- 6.3.1. Within two (2) hours of the data privacy security incident or personal data breach the Data Protection Officer or the Head/supervisor of the Department or Unit involved in the incident/breach should be informed via email or phone call for initial immediate action.
- 6.3.2. The Data Protection Officer shall initially assess and categorize the report as one of the following:
 - 6.3.2.1. Data Privacy Security Incident
 - 6.3.2.2. Data Breach
 - 6.3.2.3. Non-Critical

- 6.3.3. LSGH Employee/Personnel or student shall file a Data Breach Reporting Form within 24 hours from his/her 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. **Initial Mitigation**
- 6.4.1. Mitigation action shall be implemented to contain the incident/breach to prevent further damage through actions such as: disconnecting affected devices from the internet/intranet; applying short or long term containment strategies; implementing a backup system to aid in restoration; update and patch system; review remote access protocols; change user and administrative access credentials; secure passwords.
 - 6.4.2. The Technological Management Center should undertake necessary actions to: restore system; repair or rebuild the system that was compromised; validate the problem that caused the incident to ensure it is addressed; communicate to users that the problem or issue has been fixed; disclosing the incident to the affected users if needed and recommending appropriate administrative measures to address the incident.
- 6.5. **Compliance**
- 6.5.1. 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 Development to be addressed under the relevant disciplinary code.
 - 6.5.2. 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 may constitute an actionable breach of contract.
- 6.6. **Composition of the Data Breach Response Team**
- 6.6.1. The Data Breach Response Team shall be composed of the following:
 - 6.6.1.1. Director of Administration - to ensure management's commitment to breach response planning and execution;
 - 6.6.1.2. Head Administrator of Marketing Communication Office - to ensure an accurate account of any issues is communicated to stakeholders and the press;
 - 6.6.1.3. Data Protection Officer - to ensure 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;
 - 6.6.1.4. Head Administrator of TMC - to work directly with the affected network to research the time, location, and details of a breach;
 - 6.6.1.5. Head Administrator of the Source of Breach - to ensure that there is cooperation in the investigation and securing evidence in his office, department or unit; and
 - 6.6.1.6. Head Administrator of Safety and Security - to conduct investigation in cases of physical break-in.
 - 6.6.2. The team shall be responsible for the following:
 - 6.6.2.1. 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;
 - 6.6.2.2. Coordination with the different office, department or unit of LSGH for the development of the overall incident response;
 - 6.6.2.3. Implementation of the Incident Security Incident Management Policy; and
 - 6.6.2.4. Reporting actions taken on instances of personal data breaches to the Data Protection Officer within 24 hours from discovery.
 - 6.6.3. Upon receipt of the report from the Data Breach Response Team, the Data Protection Officer shall be responsible for the following:
 - 6.6.3.1. Reporting instances of data breaches and corresponding action taken to the President's Council;
 - 6.6.3.2. Monitoring of resolution of personal data breaches; and
 - 6.6.3.3. Notifying the National Privacy Commission and affected data subjects, upon clearance by the President's Council, within 72 hours

upon knowledge, or what there is reasonable belief that a personal data breach occurred.

- 6.6.4. The notification to the National Privacy Commission shall include the following information:
 - 6.6.4.1. Description of the nature of the personal data breach;
 - 6.6.4.2. Personal data possibly involved; and
 - 6.6.4.3. Measures taken by LSGH to address the personal data breach, including measures taken to reduce harm or negative consequences of the personal data breach.
- 6.6.5. The notification to the data subjects shall include the following information:
 - 6.6.5.1. Description of the nature of the personal data breach;
 - 6.6.5.2. Personal data possibly involved;
 - 6.6.5.3. Measures taken by LSGH to address the personal data breach, including measures taken to reduce harm or negative consequence of the personal data breach;
 - 6.6.5.4. Representation of LSGH, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
 - 6.6.5.5. Any assistance to be provided on the data subjects

6.7. Mitigation action that may be taken by the Data Breach Response Team

- 6.7.1. Secure systems and fix vulnerabilities that may have caused the incident/breach.
- 6.7.2. 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.
- 6.7.3. Remove improperly posted information from the web.
 - 6.7.3.1. 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.
 - 6.7.3.2. Search for the company's exposed data to make sure that no other websites have saved a copy. Contact those sites and demand for the removal of the exposed data.
- 6.7.4. Stop additional data loss.
 - 6.7.4.1. Put in offline mode all affected equipment but do not turn any machines off until forensic experts arrive. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users.
- 6.7.5. 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.
- 6.7.6. Interview people who discovered the breach. Ensure that any individual who knows about the breach/incident knows where to forward the information that may aid the investigation of the breach. Investigation must always be documented.
- 6.7.7. Do not destroy any forensic evidence in the course of the investigation and remediation.
- 6.7.8. 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 service providers take the necessary steps to make sure another breach does not occur and verify the actions taken to remedy these vulnerabilities.
- 6.7.9. Develop a communications plan that will reach all affected audiences (i.e. students, personnels 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.
- 6.7.10. 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.
- 6.7.11. Coordinate with law enforcement agencies, if applicable.
- 6.7.12. 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.
- 6.7.13. 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. Verify the types of information compromised, the number of people affected, and the contact information of the people affected.

DATA PRIVACY SECURITY INCIDENT REPORTING FORM

This document ensures that in the event of a data privacy security incident. All needed information is gathered to understand the impact of the incident and what must be done to reduce any risk to data subject and/or the School'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 School'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.

DATA PRIVACY NOTICE

LSGH respects one's rights to data privacy. Any personal data that is provided will only be used in line with the investigation of this incident and other legitimate purposes. This includes contact information should there be need for clarifications or additional information. All collected data will be kept secure and confidential, unless otherwise authorized by law. They will be disposed of as soon as it has served its purpose. Aggregated or anonymized data may be retained for statistical or research purposes.

If there are questions or clarifications relating to privacy and data protection, you may contact the College's data protection officer at dpo@lsg.edu.ph

Reported by: _____ Name and Signature	Noted by: _____ Name and Signature of Department Head
Department/Unit: _____	Date: _____

Summary of the Incident

Date and Time of the Incident	
Date Reported	
How many individuals or records are involved?	
Department/Center/Office	
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	<brief description of the incident>

Timeline

Provide a comprehensive account of the incident.

List down the relevant events in a chronological order, starting from the time the issue was discovered until it was mitigated or resolved, if so.

Date	Time	Particulars

Personal Data Involved

Personal Information	Sensitive Personal Information

Reporting

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

Initial Assessment

Does it involve sensitive personal information or any other data that may be used to commit identity fraud?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Uncertain
Is there reason to believe that the data has been acquired by an unauthorized person?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Uncertain
Is there a real risk of serious harm to the affected individual/s?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Uncertain
What are the immediate consequences of the incident on the affected individual/s? (if known)			
Were there security measures in place to help avoid the incident or mitigate its negative impact? If yes, please describe.			

Remedial Measures Taken

Measure	Application	Date (of implementation)
What have you done to secure, recover, remove, or delete the personal data (if applicable)?		

Measure	Application	Date (of implementation)
What have you done to help mitigate the harm, damage, distress or negative consequences caused by the incident on the affected individuals?		
What have you done to inform the affected individuals? Indicate the reason if there was delay, or no notification.		
What have you done to provide assistance to affected individuals?		
What have you done to prevent or avoid similar incidents in the future?		

Impact

What are the potential adverse consequences for students, personnels, third parties, or LSGH?	
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/breach? If so, provide details.	

Management

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

Assessment (to be accomplished by Data Protection Officer)

Recommendation:
