Ateneo de Manila University
University Data Protection Office

Security Incident Management Policy

This policy aims to guide all University offices and personnel in the proper handling of data breaches and other security incidents that involve personal data under the control of the University.

ATENEO DE MANILA UNIVERSITY
UNIVERSITY DATA PROTECTION OFFICE

Security Incident Management Policy

Background

Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA), governs the processing of personal data in the Philippines. The law calls for the adoption of appropriate and necessary security measures that prevent or minimize the risks posed by data breaches and other security incidents. They include mechanisms to notify the National Privacy Commission (NPC) and affected individuals of data breaches under certain circumstances. The NPC has also developed policies that elaborate on said measures and their implementation.

Within the Ateneo de Manila University, the responsibility for developing these security measures lies primarily with the University Data Protection Office (UDPO).

The UDPO recognizes that no data processing system can ever be completely secure. Data breaches and other security incidents are bound to occur, regardless of the type and amount of security tools one puts in place. This makes it important for every organization to be prepared and have the necessary protocols that would facilitate the proper handling of such incidents in order to minimize their impact and ensure compliance with all applicable laws and policies.

For these reasons, the UDPO issues this Policy that provides for the security incident management protocols of the University.

1. Scope

This Policy shall cover all security incidents involving any data processing system of the University and/or personal data under its control or custody.

2. Definition of Terms

Whenever used in this Policy, the following terms shall have their corresponding meanings as provided below:

2.1. "Data Breach" refers to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. It may be in the nature of:

- 2.1.1. availability breach - loss, accidental or unlawful destruction of personal data;
- 2.1.2. integrity breach - alteration of personal data; or
- 2.1.3. confidentiality breach - unauthorized disclosure of or access to personal data.

2.2. "Data processing system" refers to a system or procedure by which personal data is collected and processed in an information and communications system, or a relevant filing system.

2.3. "Data subject" refers to an individual whose personal data is processed.

2.4. "Incident Report" refers to a document that provides a detailed account of a suspected security incident. It is not an acknowledgment of guilt or wrongdoing on the part of the person who prepares it. It shall be treated primarily as a statement of facts, which also includes an initial assessment of the incident.

2.5. "Office" refers to a basic component or working unit of the University, including offices, centers, institutes, departments, and laboratories.

2.6. "Personal Data" pertains to the collective term used to refer to personal information, sensitive personal information, and privileged information.

2.7. "Personal Information" refers to any information, on its own or when combined with other information, from which the identity of an individual is apparent or can be reasonably and directly ascertained.

2.8. "Personal Information Controller" or "PIC" refers to a natural or juridical person that controls the processing or use of personal data. It includes a person who instructs another person to process personal data on its behalf.

2.9. "Personal Information Processor" or "PIP" refers to a natural or juridical person to whom a personal information controller may outsource the processing of personal data under the latter's control or custody.

2.10. "Privacy Impact Assessment" refers to a process meant to evaluate and manage the impact on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP.

2.11. "Privileged Information" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

2.12. "Process Owner" refers to the office that owns, administers, and/or manages a data processing system, or is the principal custodian of a particular personal data under the control or custody of the University. It excludes offices or units of service providers.

2.13. "Reported Incident" refers to an event or incident suspected of being a data breach or some other type of security incident that is subsequently relayed to the UDPO.

2.14. "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 shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place. A data breach is a type of security incident.

2.15. "Sensitive Personal Information" refers to personal information:

- 2.15.1. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- 2.15.2. about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- 2.15.3. issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- 2.15.4. specifically established by an executive order or an act of Congress to be kept classified. "University" or "ADMU" shall pertain to Ateneo de Manila

University including its units and offices.

2.16. "Service Provider" refers to any authorized person, organization, or body performing a function or providing a service to or on behalf of the University. A PIP is a specific type of service provider.

2.17. "University" refers to Ateneo de Manila University.

2.18. "University personnel" refers to all individuals who perform services for or on behalf of the University. They shall include, but are not limited to, administrators, faculty members, employees, and consultants[1].

3. Security Incident Response Team

There shall be a Security Incident Response Team (SIRT), which shall be responsible for investigating a suspected security incident.

Headed by the Director of the UDPO, the Team shall have two (2) other permanent members appointed by the University President. Other University personnel may be called on to join the Team on a per incident basis when their expertise or background is appropriate and necessary to adequately address the incident, as recommended by the permanent members and approved by the University President. All members must have the rank of administrator.

Where a permanent member of the Team is the Process Owner involved in a reported incident, the University President will designate a competent alternate. A service provider or external party may also be considered.

A Team member may delegate his or her functions to another member of his or her Office, provided that he or she shall remain the signatory in all related documents accomplished or generated by the Team.

4. Assignment of Duties and Responsibilities

To ensure the effective implementation of this Policy, the following offices and individuals shall perform their respective functions and responsibilities:

4.1. *SIRT*

- 4.1.1. Investigate and assess suspected security incidents in coordination with all concerned units and offices of the University.
- 4.1.2. Recommend remedial measures to be performed by the Process Owner and other concerned units or offices of the University in relation to a suspected security incident.
- 4.1.3. Accomplish an Assessment Report (SIRTAR), as prescribed by the UDPO.

4.2. *UDPO*

- 4.2.1. Serve as the main point of contact for all reports of a suspected security incident.
- 4.2.2. Act as custodian of all reports and documents generated or prepared in relation to each suspected security incident.
- 4.2.3. Review and revise this Policy in accordance with the provisions hereof.
- 4.2.4. Assist the University President, the SIRT, and Process Owners in the performance of their functions under this Policy.

[1] *May include employees of University service providers*

4.3. *University President*

4.3.1. Approve, reject, or otherwise take action on the findings or recommendations of the SIRT.
4.3.2. Appoint the permanent members of the SIRT.
4.3.3. Approve the designation of additional members of the SIRT as the circumstances may require.
4.3.4. Designate the alternate of any permanent member of the SIRT, when necessary.
4.3.5. Notify the NPC and/or affected data subjects when required by DPA.
4.3.6. Approve, reject, or otherwise comment on proposed revisions to this Policy.

4.4. *Process Owners*

4.4.1. Where a reported incident involves its data processing system or any personal data under its control or custody, including those being processed by a service provider or an authorized third party, submit an Incident Report to the UDPO in accordance with this policy.
4.4.2. Implement security measures that aim to:
   a. avoid or minimize the risk of experiencing security incidents
   b. stop an ongoing security incident
   c. contain, limit, or mitigate the impact of a security incident
4.4.3. Where they share, disclose, or transfer to authorized third parties any personal data under their control or custody, require such third parties to report any security incident that affects or involves the shared, disclosed, or transferred data.
4.4.4. Cooperate with and extend assistance to the UDPO and the SIRT in resolving each reported incident.

Unless otherwise prevented by more pressing matters, the foregoing offices and individuals shall prioritize their functions and responsibilities under this Section to ensure a prompt and effective resolution of all reported incidents, and to enable the University to meet its obligations under the DPA.

5. Notification of the UDPO

Incident notification shall be carried out in accordance with the provisions of this Section:

5.1. *Subject of a Notification.* An incident must involve a data processing system of the University or personal data under the control or custody of the University. It includes those being processed by a service provider or any other authorized third party.

5.2. *Notifying Party and Recipient of Notification*. Any person who becomes aware of or has reason to believe that an incident described by the previous subsection has occurred must notify the UDPO using any of the latter's contact information. If a notification is sent to or received by a different office of the University, it shall be immediately referred to the UDPO.

5.3. *Method of Notification*. A person who wishes to notify the UDPO of an incident shall submit a Contact Form, as prescribed by the UDPO. In the absence of a Contact Form, the Notifying Party must be able to provide the following information:

5.3.1. Name
5.3.2. Contact details
   5.3.2.1. Email Address
   5.3.2.2. Contact Number
5.3.3. Details of the incident (if known)

5.3.3.1. Date and Time of Incident
5.3.3.2. Number of persons affected
5.3.3.3. Name of office processing the information

If the incident involves the office of the Notifying Party (i.e., the office is the concerned Process Owner), he or she shall instead accomplish an Incident Report in accordance with Section 6.2 of this Policy.

All forms are available at the UDPO website.

6. Investigation of Incidents

Investigations of incidents shall be carried out in accordance with the provisions of this Section:

6.1. The UDPO shall refer a reported incident to the concerned Process Owner. It shall also give advance notice to the SIRT about the reported incident.

6.2. Once informed by the UDPO, the Process Owner shall accomplish an Incident Report and submit the same to the UDPO within twenty-four (24) hours. The Process Owner must inform the UDPO before the expiration of such period if it requires additional time. However, in no case shall such additional time exceed five (5) calendar days.

Whenever possible, the person/s who may be involved in the reported incident should not be made to accomplish the Incident Report to minimize any conflict of interest.

The UDPO shall not accept Incident Reports that are incomplete or improperly accomplished.

6.3. The UDPO shall refer the Incident Report to the members of the SIRT for their evaluation. At this point, the SIRT will determine if additional members are necessary to investigate the reported incident.

If so deemed necessary, the SIRT shall recommend the designation of additional members to the University President.

6.4. The SIRT shall conduct its investigation of the incident based primarily on the Incident Report. However, it is not bound by such report and can perform any of the following tasks:

6.4.1. direct clarificatory or follow-up questions to the Process Owner
6.4.2. require additional submissions from the Process Owner
6.4.3. request for a meeting with the Process Owner and other concerned offices of the University, including individuals affected by the suspected security incident
6.4.4. perform other actions to obtain information critical to the investigation

The SIRT shall complete its investigation within forty-eight (48) hours after it has obtained all information it needs to carry out its investigation. If it requires additional time, it must at least determine within this period whether or not a data breach has occurred, and if notification of the NPC is necessary. This initial assessment shall be relayed to the University President by the UDPO.

6.5. The results of the investigation by the SIRT shall be consolidated by the UDPO into an SIRT Assessment Report. The UDPO may already advise the Process Owner regarding any initial or urgent recommendations by the SIRT.

6.6. The SIRT Assessment Report, together with the Incident Report and other relevant attachments, shall be recorded and stored in accordance with this Policy. However, if it

contains recommendations and/or other matters that require the attention of or action from the University President, it shall be transmitted immediately to the latter for appropriate action.

7. Data Breach Notification of the NPC and Data Subjects

Notification of the NPC and affected data subjects shall be carried out in accordance with the provisions of this Section:

7.1. A confirmed data breach shall be reported to the NPC if the University President, after being informed of the advice of the SIRT, has determined that it is attended by all of the following conditions:

7.1.1. it involves sensitive personal information or any other information that may be used to enable identity fraud;
7.1.2. there is reason to believe that the information may have been acquired by an unauthorized person; and
7.1.3. there is reason to believe that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

7.2. If there is uncertainty regarding the need to notify the NPC, the following additional factors shall be considered by the University President and the SIRT:

7.2.1. Notification could reduce the risks arising from the data breach.
7.2.2. The data breach would likely affect national security, public safety, public order, or public health.
7.2.3. The personal data involved is required by applicable laws or rules to be confidential.
7.2.4. The personal data involved belongs or refers to vulnerable groups.
7.2.5. The data breach affects at least one hundred (100) individuals.

7.3. The University President, with the assistance of the UDPO, shall notify the NPC within seventy-two (72) hours after he has determined that a confirmed data breach meets the conditions set out in Subsections 7.1 and/or 7.2 hereof.

For this purpose, the UDPO shall send a notification letter to the NPC via email, as signed by University President. The UDPO shall make sure to obtain a confirmation from the NPC that it has received the notification letter. If online access is not available, the UDPO shall personally deliver the notification letter to the NPC and maintain a receiving copy.

7.4. There shall be no delay in notifying the NPC except in instances expressly allowed or recognized by the Commission through its Circular 16-03 and other applicable policies.

7.5. The University must also notify affected individuals within the same period, unless there are grounds recognized by law that allow the University to forego with such notification.

In determining whether a valid reason exists for not notifying affected individuals, the University, through the University President, may consult with the NPC.

7.6. Whenever possible, the University, through the concerned Process Owner, shall coordinate with all affected data subjects and provide appropriate guidance or assistance.

8. Reports and Documentation

All reported incidents shall be properly documented. The UDPO shall develop forms for this purpose, facilitate their accomplishment by the responsible parties, and see to their secure storage and disposal. As a basic security measure, soft copies of all reports and related documents must be password-protected. Only those directly involved in their preparation and use shall have access to these documents.

A Summary Report shall be submitted by the UDPO to the President's Council on a quarterly basis. A separate Annual Security Incident Report shall also be submitted by the UDPO to the President's Council and the NPC.

All documents shall be made available to the NPC, upon request. However, the UDPO shall anonymize all personal data within two (2) years after their filing.

9. Undertaking of Confidentiality

All information generated by or involved in the handling of security incidents shall be kept confidential by all concerned Parties. For this purpose, all University Personnel involved must have accomplished the Non-Disclosure Agreement prescribed by the UDPO before they assume their functions under this Policy.

Any public pronouncements involving such incidents must be coordinated with the UDPO and shall be subject to the approval of the University President.

10. Remedial and Prevention Measures

To help prevent or avoid the same type of security incident from occurring, the following measures may be undertaken:

10.1. The UDPO may facilitate a debriefing session with the concerned Process Owner to ensure that remedial or preventive measures are properly implemented. It may also conduct an orientation regarding data privacy and compliance with the DPA.

10.2. The SIRT may recommend the conduct of a Privacy Impact Assessment (PIA) on the data processing system involved in a security incident, or on the entire office of the Process Owner. The UDPO shall issue the necessary guidelines for the proper conduct of a PIA.

10.3. The concerned Process Owner shall implement new security measures, and/or make changes to existing ones.

11. Penalties

Failure to comply with this Policy may result in disciplinary action, in accordance with the applicable Code of Discipline/Conduct of the University, and other relevant rules and regulations. This is without prejudice to other legal remedies available to the University and/or any aggrieved or injured party under all applicable laws and policies.

12. Review

Unless circumstances require a shorter period, the UDPO shall review this Policy every two (2) years in consultation with relevant units and offices of the University. Amendments must also be approved by the University President.

13. Effectivity

Upon the approval by the University President, this Policy and any subsequent amendments shall take effect within fifteen (15) calendar days after it has been posted in the UDPO website.

Noted by:

(sgd.) JOSE RAMON T. VILLARIN, S.J.
President

Date approved: 01 May 2019