UNIVERSITY OF THE PHILIPPINES
DILIMAN QUEZON CITY
VOIP TRUNKLINE: 981-8500 LOCAL: 2558, 2556
DIRECT LINE: (632) 929-5401, (632) 927-1835
FAX: (632) 928-2863
E-MAIL: chancellor.updiliman@up.edu.ph

OFFICE OF THE CHANCELLOR

25 March 2019

ADMINISTRATIVE ORDER NO. MLT 19 –072

TO: Deans, Directors, Heads of Units, Faculty, REPS and Staff Information Officers / Data Privacy Compliance Focal Persons

SUBJECT: Data Privacy Security Incident Management Policy

Timely and responsive management of data privacy incidents allows for resilience and continuity of operations of affected offices and contains adverse effects to people. To establish an efficient and effective process to handle privacy incidents and personal data breaches, the attached Security Incident Management Policy is hereby promulgated.

MICHAEL L. TAN, PhD
Chancellor

Attachment: UPD Security Incident Management Policy

University of the Philippines Diliman
Security Incident Management Policy

This Policy governs the monitoring, mitigation, investigation, response, containment, reporting and resolution of Security Incidents and Personal Data Breaches in the University of the Philippines Diliman.

PART I.
OBJECTIVE AND SCOPE

Objective

This policy is promulgated to:

- Establish data breach response team and define its roles and responsibilities
- Ensure Security Incidents, including data breach, are handled in a timely manner, properly investigated and handled in accordance with the response procedures to contain a Security Incident
- Ensure the availability, integrity and confidentiality of the Personal Data being processed through its information and communication system

Scope

This policy governs all UP Diliman academic units and administrative offices which process personal information.

Definition of Terms

For the purpose of this policy, the following terms are defined, as follows:

1. ***Data Breach Response Team or BRT*** refers to UP Diliman teams mandated to assess and evaluate Security Incidents, which includes Personal Data Breaches, restore integrity to the information and communications systems, mitigate and remedy resulting damages, and comply with reportorial requirements.
2. ***Data Subject*** refers to an individual whose personal information is processed;
3. ***Data Processor*** refers to UP People who process Personal Data pertaining to a Data Subject;
4. ***DPA*** refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
5. ***IRR*** refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
6. ***NPC*** refers to the National Privacy Commission of the Philippines as created by the Data Privacy Act of 2012;

7. ***Personal Data*** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012;
8. ***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. A Personal Data Breach may be in the nature of:
    a. An availability breach resulting from loss, accidental or unlawful destruction of Personal Data;
    b. Integrity breach resulting from alteration of Personal Data; and/or
    c. A confidentiality breach resulting from the unauthorized disclosure of or access to Personal Data.

    For the purposes of this Policy, the term "Personal Data Breach" is included in the term "Security Incident";
9. ***Privacy Concern*** refers to an inquiry, issue, risk, incident, breach or request referred to the UP Diliman Privacy Focal Person having jurisdiction over the relevant UP Diliman unit;
10. ***Privacy Focal Person or PFP*** refers to an academic unit's or administrative office's focal person for data privacy compliance acting as compliance officers for privacy. They are champions of data privacy and agents of pursuing data privacy culture in their unit. A go-to person when it comes to data security and privacy compliance;
11. ***Risk*** refers to the potential of an incident to result in harm or danger to a Data Subject or organization;
12. ***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 shall include incidents that would result to a Personal Data Breach, if not for safeguards that have been put in place. For the purposes of this Policy, the term "Security Incident" includes "Personal Data Breach";
13. ***Sensitive personal information*** refers to personal information:
    a. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    b. 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;
    c. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, and
    d. Specifically established by an executive order or an act of Congress to be kept classified.
14. ***Staff*** refers to UP Dilman staff, including Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, and retirees as well as UP Diliman Faculty, including visiting faculty;
15. ***Threat*** refers to a potential cause of an unwanted incident, which may result in harm or danger to a Data Subject, system, or organization;

16. ***UP People*** refers to Staff, researchers, alumni, subcontractors, outsourcees, agents and representatives of UP Diliman;
17. ***Vulnerability*** refers to a weakness of a data processing system that makes it susceptible to threats and other attacks.

Jurisdiction, Authority, and Oversight

The UP Diliman Data Protection Officer shall have jurisdiction, authority and oversight over endeavors, projects, actions and decisions related to the data privacy and data protection of UP Diliman and UP People.

PART II.
UP DILIMAN BREACH RESPONSE TEAMS

Data Breach Response Teams or BRTs

UP Diliman Breach Response Teams are an organized group of Staff mandated to assess and evaluate Security Incidents, which includes Personal Data Breaches, restore integrity to the information and communications systems, mitigate and remedy resulting damages, and comply with reportorial requirements. BRTs are under the jurisdiction and authority of the UP Diliman Data Protection Officer.

Composition

UP Diliman shall have a Constituent University-level Breach Response Team (the "Diliman-Level BRT") and a Breach Response Team for each academic unit and administrative office (the "Unit-Level BRT").

Responsibilities

BRTs shall be responsible of the following:

- Implementation of the Security Incident management policy of UP Diliman;
- Management of Security Incidents and Personal Data Breaches; and
- Compliance with the relevant provisions of the DPA, its IRR, and all related issuances by the Commission on Personal Data Breach management.

The team must be ready to **assess and evaluate** a Security Incident, **restore integrity** to the information and communications system, **mitigate and remedy** any resulting damage, and **comply** with reporting requirements.

Diliman-Level BRT

The Diliman-Level BRT shall be comprised of the following members:

1. UP Diliman Data Protection Officer as Chair;
2. Director of the Computer Center as Deputy Chair;
3. A representative from the School of Library and Information Sciences (SLIS);
4. A representative from the Human Resources Development Office (HRDO);
5. A representative from the Office of the University Registrar (OUR);
6. A representative from the Diliman Legal Office (DLO).

If a Security Incident involves Personal Data of a student, parent or guardian, then the Privacy Focal Person (PFP) of the Office of the Vice Chancellor for Student Affairs shall *motu proprio* become a support and resource person of the Diliman-Level BRT.

If a Security Incident involves Personal Data processed by an office under the Office of the Vice Chancellor for Administration (OVCA), then the PFP of OVCA shall *motu proprio* become a support and resource person of the Diliman-Level BRT.

If a Security Incident involves Personal Data handled of an alumnus, then the PFP of the academic unit of the alumnus shall *motu proprio* become a support and resource person of the Diliman-Level BRT.

Unit-Level BRTs

Each UP Diliman academic unit and administrative office is required to establish a BRT for its unit.

The Unit-Level BRT shall be comprised of:

1. The unit's Privacy Focal Person (PFP) who shall have authority to decide on privacy-related matters in case of a Personal Data Breach. The PFP is the leader and coordinator of the Unit-Level BRT;
2. An officer of the UP Diliman unit with authority to decide on relevant administrative matters in case there is a data breach;

3. A Data Processor or information security person with knowledge how Personal Data is processed by the unit.

For every Privacy Concern (including Security Incidents and Personal Data Breaches) the PFP shall coordinate the monitoring, mitigation, investigation, response, containment, reporting and the unit's contribution in resolving the Privacy Concern.

If the unit-level BRT reasonably believes that there is a Security Incident, PFPs must immediately inform the DPO all information on hand regarding the Security Incident details:

- Nature of the incident or breach
- Personal Data affected
- Data Subjects affected

PART III.
IMPLEMENTATION OF SECURITY MEASURES

Data privacy is a responsibility of every academic unit and administrative office of UP Diliman. Privacy Focal Persons (PFPs) are mandated to monitor, mitigate, investigate, respond to, contain, reporting and aid in resolving Privacy Concerns (including Security Incidents and Personal Data Breaches).

Acceptable Use Policy

The Acceptable Use Policy of the University of the Philippines (upd.edu.ph/aup/) shall govern use of computing facilities and network infrastructure in UP Diliman. Any part of the said policy that is inconsistent with the DPA and its IRR shall be superseded by DPA and its IRR.

Protection of information systems and assets

UP Diliman units should conduct inventories of information assets. As far as practicable, UP Diliman units should adopt information security policies that address the specific needs of their units with applicable controls and procedures. In no case shall policy specific to a unit may supersede or prevail over UP Diliman's data privacy policies.

Protection of Personal Data

Personal Data should be treated with privacy and confidentiality. Its loss or unauthorized disclosure may lead to one or more of the following consequences:

- Financial loss (e.g. the withdrawal of a research grant or donation, a fine by the government, a legal claim for breach of confidence);
- Reputational damage (e.g. adverse publicity, demonstrations, complaints about breaches of privacy); and/or
- An adverse effect on the safety or well-being of members of UP Diliman or UP People (e.g. increased threats to staff or students engaged in sensitive research, embarrassment or damage to benefactors, suppliers, staff and students).

Storage of Personal Data

All Personal Data being processed by UP Diliman shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the University.

No Personal Data should be store other than UP Diliman owned, controlled or leased properties.

Encryption of Personal Data

As far as practicable, file or disk industry-standard encryption methods should be performed in cases where sensitive personal information is regularly processed by the concerned data processing system.

Access to Personal Data

There shall be a system to regulate access to data centers owned or controlled by UP Diliman. Appropriate security clearances or access control lists should be set up for classes of administrators and uses. There should be an access control system that records when, where, and by whom the data centers are accessed. Copies of access control lists and similar records must be filed to UP Diliman Data Protection Office.

Transfer of Personal Data

Messages and Communications Policy

The University of the Philippines Diliman Message and Communication Policy (upd.edu.ph/privacy/communications/) should be followed in the creation, sending, transmittal, receipt, access, use, processing, and storage of documents, instruments, files and data in any form or medium containing personal or confidential information.

Other Policies

Relevant UP Diliman policies on Data Privacy, Information Security and Data Governance should be followed with respect to Personal Data in transit or at rest.

PART IV.
INCIDENT MANAGEMENT AND NOTIFICATION

Any person with knowledge or reason to believe that there is either:

(1) A **Security Incident**, that is, an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of Personal Data; or
(2) A **Personal Data Breach**, that 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;

should immediately report all information on hand both to the UP Diliman Data Protection Officer and the Privacy Focal Person (PFP) having jurisdiction over the UP Diliman unit or office involved.

The following eight (8) steps, divided into three (3) sections, should be followed in responding, reporting and managing Security Incidents and Personal Data Breaches:

Section A. Incident Response Procedure

Step 1 – Reporting

Within two (2) hours from discovery of the Security Incident or Personal Data Breach, any person – whether connected with UP Diliman or not – *should* report

via email *and* phone call to *both* the UP Diliman Data Protection Officer and the PFP having jurisdiction over the unit involved. The email address of the UP Diliman Data Protection Office to receive incident and breach reports is securityincident.updiliman@up.edu.ph.

Step 2 – Categorization

The Privacy Focal Person shall *categorize* the Report as one of the following:

(A) Security Incident
- Reporting of an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. This includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

(B) Personal Data Breach
- Notification on 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.

(C) Non-urgent Matter
- Inquiry or solicitation of advice.
- Request for participation or guidance from the UP Diliman Data Protection Office in projects and undertakings.
- Request for support service not included in the above classifications.

Step 3 – Investigation and Identification

If the Report is either a Security Incident or Personal Data Breach, the Unit-Level BRT led by the PFP, should investigate to discover the following information:

(A) Nature and circumstances of the incident or breach;
(B) Data processing systems involved;
(C) Persons responsible, involved and affected and their contact details.

The above information should be submitted by the Unit-Level BRT to the Diliman-Level BRT within six (6) hours from initial discovery of the incident or breach.

Security Incidents and Personal Data Breaches should be investigated, identified and profiled. Observations, indicators and deviations from normal operations may be used to discover the nature, effects and extent of a Security Incident or Personal Data Breach.

As far as practicable, the Computer Center shall endeavor to have sensor platforms (i.e., Network Perimeter, Host Perimeter, System-Level detection, Application-Level detection, etc.) to monitor malicious acts or attempts to do harm.

For Security Incidents that have come to the knowledge of the Computer Center, it shall provide an annual report to the UP Diliman Data Protection Office with assessment on the degree of risk for each incident.

Section B. Breach Notification

Step 4 – Reporting and Notification

All Personal Data Breaches should be monitored and recorded by the Diliman-Level BRT and the concerned Unit-Level BRT but not all data breaches have to be reported to the NPC. If all the following are present, a report shall be made to NPC:

- There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;
- The data is reasonably believed to have been acquired by an unauthorized person; and
- Either UP Diliman's Chancellor 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.

When there is doubt of notification to NPC, the following should be considered:

1. The likelihood of harm or negative consequences on the affected Data Subjects;
2. How notification, particularly of the Data Subjects, could reduce the risks arising from the Personal Data Breach reasonably believed to have occurred; and
3. If the data involves:
    a. Information that would likely affect national security, public safety, public order, or public health;
    b. At least one hundred (100) individuals;
    c. Information required by all applicable laws or rules to be confidential; or
    d. Personal Data of vulnerable groups.

Aside from notifying the NPC, UP Diliman, shall also notify the affected Data Subjects upon knowledge of, or when there is reasonable belief that a Personal Data Breach has occurred.

The NPC shall be notified within **seventy-two (72) hours** upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a Personal Data Breach has occurred.

Generally, there shall be no delay in notification however, the notification may **only be delayed to the extent** necessary to determine:

- the scope of the breach;
- to prevent further disclosures; or
- to restore reasonable integrity to the information and communications system.

There can be no delay in the notification if the breach involves at least one hundred (100) Data Subjects, or the disclosure of sensitive personal information will harm or adversely affect the Data Subject. In either case, the NPC must be notified within the 72-hour period based on available information.

The full report of the Personal Data Breach must be submitted within five (5) days from notification, unless the UP Diliman is granted additional time by the NPC to comply.

All Security Incidents and Personal Data Breaches must be recorded with details by the UP Diliman Data Protection Officer and reported to the NPC if required.

Section C. Mitigation Response Plan

Step 5 – Containment and Eradication

The Unit-Level BRT, in coordination with relevant UP Diliman units and UP People shall conduct steps to stop the cause of the Security Incident or Personal Data Breach and its effects. The PFPs and responsible units are responsible to contain the Security Incident or Personal Data Breach so that it does not spread and cause further damage. Steps that may be taken are:

- Disconnect the affected devices form the internet or intranet
- Commence short-term and long-term containment strategies
- Ensure that there is a back-up system to help us in the restoration process
- Update and patch the system
- Review remote access protocols
- Change user and administrative access credentials
- Secure passwords

The UP Diliman DPO shall address the Concern. The Privacy Focal Person shall facilitate all forms of resolutions by ensuring that the support provided by the UP Diliman DPO responsively and effectively addresses the Concern without causing new Concerns.

Step 6 – Recovery

The Unit-Level BRT, in coordination with relevant UP Diliman units and UP People (such as Data Processors, I.T. personnel and records managers), shall endeavor to restore the system or application to a working state and take necessary actions to recover affected records, systems and other matters affected by the Security Incident. The following tasks may be conducted:

- restoring system data to a known good state
- repairing or rebuilding the system or application that was compromised
- validating that the problem that caused the incident has been addressed
- communicating to users that the system is back online
- disclosing the incident to effected users if necessary
- taking any appropriate administrative actions related to the incident

Step 7 – Feedback

The Unit-Level BRT shall officially categorize the status of the Security Incident or Personal Data Breach as one of the following:

(A) Resolved with finality
- The matter had been sufficiently addressed.

(B) Resolved with issues
- The dangers of matter had been prevented or mitigated but certain issues remain due to factors or circumstances beyond the control of UP Diliman's University-Level and Unit-Level BRTs.

(C) Resolved with new concern
- The matter had been resolved but a new inquiry, issue, risk, incident, breach or request has arisen from the original Security Incident or from the resolution. In this case the new concern shall be handled starting with Step 2.

Compliance with the above procedure ensures that data privacy is upheld and protected in an efficient, responsive and effective manner.

As far as practicable, the Unit-Level BRT shall reach out to the affected data subjects to render a report on UP Diliman's management of the Security Incident or Personal Data Breach. Depending on the propriety of the act, the Diliman-Level BRT may also reach out to the NPC to provide updates.

Step 8 – Learning

The Diliman-Level BRT discuss lessons learned. Diliman-Level BRT may document lessons to prevent similar incidents from occurring again.

The UP Diliman Data Protection Office shall maintain records of Security Incidents and Personal Data Breaches.

The mitigation, management and resolution of Security Incidents and Personal Data Breaches requires the coordination of various UP People. All concerned should be vigilant in their responsibilities to enable an effective security incident management process.