ATENEO DE DAVAO UNIVERSITY

Tel +63 (82) 221.2411 local 8251 · 8203 · Fax +63 (82) 221-2411 local 8277
email: registrar@addu.edu.ph · website www.addu.edu.ph
PO Box 80113 · 8000 · Davao City, Philippines

ACCREDITED and a member of the Philippine Accrediting Association of Schools Colleges and Universities (PAASCU)

Office of the University Registrar
Atty. Edgar B. Pascua II

In consortium with
Xavier University (Ateneo de Cagayan)
Ateneo De Zamboanga University

December 19, 2017

RECEIVED
Ateneo de Davao University
DEC 19 2017
OFFICE OF THE EXECUTIVE VICE PRESIDENT

FR. JOEL E. TABORA, S.J. PH.D
University President

Dear Fr. Tabora.

Submitted for your approval are the following;

1. **Data Privacy Manual** – This Manual shall be adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. This document regulates the management of personal data by the University, in view of the right to privacy of our stakeholders.

2. **Data Breach Response Protocol** - This manual shall be implemented on all incidents of breach of personal data, which has been collected, processed and stored physically or electronically, on all units and offices of the University, including breaches to facilities where such data have been stored or processed.

Both came as a result of the undersigned's consultation of relevant offices across all units of the University, including our central administrators.

Once approved, and implemented all throughout the University, we then shall be compliant with these major requirements of the Data Privacy Act and of the Regulations of the National Privacy Commission.

ENDORSED
Ateneo de Davao University
DEC 19 2017
JEREMY S. ELIAB
Executive Vice President

№ 03100

Most respectfully yours,

ATTY. EDGAR B. PASCUA II
Data Protection Officer

APPROVED
Ateneo de Davao University
OFFICE OF THE PRESIDENT
DEC 20 2017
FR. JOEL E. TABORA, S.J.
University President

DATA PRIVACY MANUAL

Ateneo de Davao University

INTRODUCTION

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. This organization respects and values your data privacy rights, and makes sure that all personal data collected from its stakeholders, employees, students and alumni are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

DEFINITION OF TERMS

As Used in this Manual;

"**ADDUNet**" – refers to the computer network, which interconnects all the wired and wireless devices owned and/or controlled by the University.

"Closed Circuit Television System" or CCTV is the self-contained surveillance system comprising of cameras, recorders and displays for monitoring activities installed within the University premises, and its peripherals.

"**Data Subject**" – refers to an individual whose personal, sensitive personal or privileged information is processed by the University. It may refer to officers, employees, consultants, and students, as well as the alumni of this organization.

"**Data Processing Systems**" – refers to the automated processing system of the University, as developed by the University Information Technology Office (UITO), which includes, but is not limited to the following as may be developed and maintained by the University:

> "Academic Information System (AIS)" – refers to the online portal made available by the UITO-MIS, for the submission of grades by the faculty for their students, and their evaluation by their coordinators or other evaluating officers.
>
> "Academic Information Management System (AIMS)" – refers to the portal accessible via local area network, exclusively by offices in charge of the collection of, or modification of personal information of the data subjects.
>
> "Employees Portal" the portal accessible to the employees for their retrieval of their personal information and applications for benefits and availment of their employee related rights and privileges.

"Student Information System (SIS)" - refers the online portal for students, which they may access for the retrieval and portability of their personal data, including their grades, schedule, personal information, academic status, financial obligations, and other relevant information pertaining to their education.

"**HRMDO**" shall refer to the Human Resource and Development Office of the University. The office in the University in charge of the management and capabilities enhancement of its employees.

"**Personal Information**" – refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by University, through its authorized representatives or employees holding the information, or when put together with other information would directly and certainly identify an individual.

"**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

"**Processing**" refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

"**Restricted Information**" includes information, whether under the category of a Sensitive Personal information or not, which are exclusive to offices or persons because of their ethical, professional, or legal obligations.

"**Sensitive Personal information**" refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

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;

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

4. Specifically established by an executive order or an act of Congress to be kept classified.

"**University**" shall mean the Ateneo de Davao University, as an institution.

"**University Premises**" shall include all the campuses of the University, including their peripherals, as well as other facilities of the institution as retreat houses, and laboratories outside the campuses.

SCOPE AND LIMITATIONS

A. All employees of the University, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual. This includes persons so authorized to access pertinent data by the University as working scholars and the likes.

B. The foregoing shall include students, in such organizations under the guidance and moderation of agents or employees of the University. In such case, the moderators shall be covered herein as employees, while the students may be subject to the pertinent provisions of their student manuals.

C. The University reserves the right to regulate the use of all data under its control, and maintains and asserts authority over any such information that may be accessed by its offices though whatever means.

D. Considering the nature of the data collected by the University from its Data Subjects, these shall all be generally treated as Sensitive Personal information.

PROCESSING OF PERSONAL DATA

A. **Collection**: The University, through its relevant offices, collects the relevant information of all its employees and students. The same is done via its Human Resource and Development Office, for employees, and via its relevant data collection offices of each unit for its students.

   a. **Data Collection for Students**: The Personal Data of the alumni, students and enrollees of the University, including their full names, addresses, contact numbers, family and academic backgrounds, credentials (including academic records from previous schools attended, CHED, DepEd /TESDA required forms /information, enrollment and academic status, grades, contact hours for classes, schedules for all the semesters attended within and outside the University (for cross enrollment), academic history and pertinent remarks and certifications from other schools, state agencies and relevant University offices, and such other relevant information required by law may be collected and stored by the University. Such personal information may be collected manually or by the University data processing systems.

      i. Upon admission to the university, the data subjects must be informed of the following, by the relevant student services office, in writing,

either via the posting of such notices in a conspicuous place in the immediate premises of the office concerned, or by their inclusion in the templates/forms to be filled up by enrollees;

1. Description of the personal data to be entered into the information or data collection system;
2. Exact Purposes for which they will be processed;
3. Basis for processing, especially when it is not based on the subject's consent;
4. Scope and method of the personal data processing;
5. Recipients, to whom such data may be disclosed;
6. Methods used for automated access by the recipient, and its expected consequences for the data subject;
7. Identity and contact details of the personal information controller (complete name and address of the University);
8. The duration for which such data will be kept;
9. The existence of their rights as a data subject.

ii. The University shall inform its students as data subjects, anytime during their incumbency therein, of any change in its data collection policies stated in the aforementioned item, through their SIS, or enrollment systems, or through its official website/s, or though the posting of such notices in conspicuous places immediate to the relevant student services offices.

iii. Students may, at the instance of the University, modify or update their personal information relation to their contact details and addresses, among others, manually, or though the University data processing systems, under such procedure or process that its relevant student services offices may require.

iv. Subsequent to their admission, data pertaining to grades are acquired by the University by the submission of the teachers / instructors / professors of each student for every class attended, through the manual or automated submission thereof to the Registrars' Offices.

b. **Data Collection for Employees**: The Personal Data of employees of the University, including their full names, addresses, contact numbers, personal and professional backgrounds, credentials, and such other relevant information required by law may be collected by the University. Such personal information may be collected manually or though the University data processing systems.

i. The basic personal data of applicants for employment of the University may be accepted by the HRMDO to the university. At the instance of the HRMDO, it may require the submission of more personal data relative to such applications, either for a more intensive evaluation or as a condition form hiring. At this instance, the data subjects must be informed of the following;

1. Description of the personal data to be entered into the information or data collection system;

2. Exact Purposes for which they will be processed;

3. Basis for processing, especially when it is not based on the subject's consent;

4. Scope and method of the personal data processing;

5. Recipients, to whom such data may be disclosed;

6. Methods used for automated access by the recipient, and its expected consequences for the data subject;

7. Identity and contact details of the personal information controller (complete name and address of the University);

8. The duration for which such data will be kept;

9. The existence of their rights as a data subject.

ii. The university shall inform its employees as data subjects, anytime during their employment in the University, of any change in its data collection policies stated in the aforementioned item, through the University data processing systems., or through its official website/s, or though the posting of such notices in conspicuous places immediate to the HRMDO.

iii. Employees may, at the instance of the University, modify or update their personal information relation to their personal data, manually,

or though the University automated data systems under such procedure or process that the HRMDO may require.

iv. The collection, and maintenance and control of the personal information of persons engaged by the university sans any employer employee relations (e.g. agency, project, contractual employees) , shall be the responsibility of their independent contractors or employers, and subject to the perusal of the university, in accordance with the terms and conditions of their contracts with the latter. Information relative to such persons shall be treated as confidential by the University.

c. Data pertaining to footages and other recordings may be captured by the University within the University Premises, and its peripherals via its CCTV system. An external sign or warning must be made as to the presence of such recording devices. Individuals who object to such recordings may be refused entry to the said premises.

B. **Use**: Personal data collected shall be used by the University;

a. For students / alumni - For the admission and enrollment of students, their promotion, fair evaluation, grant of degrees, retention, transmittal of records to other education institutions and the relevant education or professional regulations bodies or agencies of the state. Data subjects may request such data from or through the intervention of the Registrar's Office of the pertinent unit, for whatever legal purposes they may deem fit.

b. For employees - As part of the permanent files of the employees, which may be used for their evaluation, and for other purposes as allowed by law.

C. **Storage, Retention and Destruction**: This University will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing.

a. The University will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

b. Information gathered shall be part of the permanent academic records of its data subjects, unless the same are ordered destroyed by the state agencies as the Commission on Higher Education, TESDA, or DepEd or DOLE, or by any pertinent state agency, and the Courts.

c. Information relative to data captured by the CCTV system in the university premises may be kept for the minimum of thirty (30) days, and subject to its further retention at the option of the University *motu proprio* or upon the legitimate request of any individual who is a member of the University

community, or by any other person or agency, and by order of the Court. The legitimacy of the requests or orders shall be determined by the Executive Vice President. However, should such requests be made by any individual not belonging to the University community, the advice of the Data Protection Officer may be sought.

D. **Access**:

1. Due to the sensitive and confidential nature of the personal data under the custody of the University, only the data subjects and the authorized representative of the University shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals. The Authorization herein referred to shall be by virtue of a notarized document.

2. As most of the data collected by the University are in the category of "Sensitive Personal information", all its employees are compelled to respect the privacy of all the University's data subjects. Any data breach may be treated as an employment infraction and categorized as "just cause", under the Labor Code of the Philippines, without prejudice to certain liabilities by the employee under relevant laws, including the data Privacy Act of 2012.

3. Access to Restricted Information that are exclusive to certain functions, offices, or persons in the University, by virtue of the ethical, formative, spiritual, and legal responsibilities must be duly respected.

a. This includes such personal information relative to the following offices;

i. Data protection Officer
ii. The Offices of the Guidance Counselors, and Testing Offices of all units
iii. The University Clinic
iv. The Executive Vice-President on matters involving internal security and emergency information and CCTV management
v. The Students Affairs, and prefects of discipline, as well as the Disciplinary Boards.
vi. Ignatian Spirituality and Formation Office, and its subsidiary offices.
vii. The head of the office in charge of any drug testing as required by law, as well as the drug testing coordinator, under RA 9165 or "Comprehensive Dangerous Drugs Act of 2002".

b. Only the University President, for good cause, can permit data sharing for such offices for restricted information with other offices of the University.

4. Employees who may have authority to access personal data may include;

i. Administrative Associates, only for such matters authorized by the head of the office where they are assigned to, as necessary for their specific functions.

ii. Faculty members, for the purpose of evaluating and submitting the grades of their current students, only for the current school year or semester, as the case may be.

iii. Academic directors / cluster heads for evaluating their students, as well as returnees or shiftees.

iv. The following Officers / Directors / heads of the following offices, only as to the limits of and by virtue of their functions;

1. Deans/Headmasters/Principals
2. Registrars
3. Student Affairs /Prefects
4. Admissions Office
5. Guidance Counselors[1]
6. Clinic
7. Academic Vice President
8. Human Resource and Development Office
9. University Librarian
10. Employees directly under the foregoing officials, under the concept of co-responsibility, and with the permission of the DPO.

5. Data sharing of any Personal Information, which are not Restricted, shall only be allowed between offices of the University, subject to the evaluation of the Heads of the Offices concerned and by virtue of law or regulation, as well as University written policies. In case of doubt, the DPO shall asses the requests and shall determine the propriety of the requests.

6. The University President shall have full access to all personal data, as well as Sensitive and Restricted Personal information of any of the institution's data subjects, in the custody of the University. He may authorize access to certain individuals of such personal information, as well as those classified as sensitive.

7. The Data Protection Officer shall only be privy to the processes and the anonymized data of the said offices, unless in instances of personal data breaches, in which case, he may view kind of personal information, only to determine the nature of the breach, and the extent thereof.

[1] They shall adhere to the confidentiality and privacy standards as stipulated in the code of ethics for Guidance Counselors and as stated in the Philippine Guidance and Counseling Association (PGCA) and the American Counseling Association(ACA

8. Limitations of access:

a. Access to any personal data by any person so authorized shall only as far as to such data collected by his office or capacity

b. The authority granted to individuals permitted access to personal data shall not be re-delegated by the latter, unless with the permission of the DPO.

c. No personal data shall be copied, or made portable, nor taken out of the university premises, unless duly authorized by the DPO.

d. Perusal of data shall not be accessed or processed in the direct view of individuals who are not likewise authorized to access the same.

E. **Disclosure and Sharing** All employees and personnel of the University, as well as other persons it shall duly authorize, shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after severance from employment, retirement, resignation, or termination of contract. Each employee which may have access to personal data shall sign an Undertaking for the maintenance of the Privacy of the data Subjects and the University. Personal data under the custody of the University shall be disclosed only pursuant to a lawful purpose, and to authorized recipients.

F. **Requests for copies of records**. Requests for copies of records (for students / alumni) may be made through the pertinent offices (i.e. Registrar, OSA) following the regulations set by the school and the competent state authorities. Request for employment records shall be exclusively made with the HRMDO.

a. Only the data subjects shall be given copies of such records. Legal representatives may request and receive such documents after their submission of the duly notarized powers of attorney.

b. At no instance shall such data be released to third parties,

1. Except upon lawful order of the court, or when required by competent state authorities relative to;

i. Matters of education, qualifications and professional regulations (as DepEd, TESDA, CHED, PRC, CSC) for students and

ii. For employment or labor matters, for employees, when so required by the DOLE.

iii. Other such state authorities, by virtue of law.

2. The DPO shall assess such requests. He shall demand for the written proof of such orders or justification for the requests.

c. Responses to background checks / academic verifications shall only be made upon the written authorization of the data subjects.

d. Requests for copies of any recording made through the CCTV system of the University by entities other than the Courts or competent state authorities may be granted only for legitimate purposes.

SECURITY MEASURES

A. Organization Security Measures

1. Data Protection Officer (DPO)

The designated Data Protection Officer shall be appointment by the University President, with the concurrence of the Board of Trustees, who shall be subject to revocation or substitution by the University, only for good cause, or at the expiration of the term of his appointment. The term of the DPO shall be determined by the University President.

2. Functions of the DPO

The DPO shall perform the following functions;

a. Monitor the University's compliance with the RA 10173, its Implementing Rules and Regulations, issuances by the National Privacy Commission and other applicable laws and policies. He may:

1. Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the University, and maintain a record thereof;

2. Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;

3. Inform, advise, and issue recommendations to the University;

4. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and

5. Advice the University as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

6. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the University;

7. Advise the University regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

b. Ensure proper data breach and security incident management by the University, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or personal data breaches within the prescribed period;

c. Inform and cultivate awareness on privacy and data protection within the organization, including all relevant laws, rules and regulations and issuances of the NPC;

d. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the University relating to privacy and data protection, by adopting a privacy by design approach;

e. Serve as the contact person of the University vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the University;

f. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

g. Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

h. Shall perform all other functions of a DPO, as may be required by law, or the policies of the University, including those which may need his intervention and attention, on matters compatible to his basic functions.

i. He must have due regard for the risks associated with the processing operations of the University, considering the nature, scope, context and purposes of processing. Accordingly, he or she must prioritize his or her activities and focus his or her efforts on issues that present higher data protection risks.

3. Conduct of Privacy Impact Assessment (PIA)

The University shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. The

DPO shall do so following the template or guidelines set by the NPC, as the minimum standard for the PIA.

4. **Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.**

   The University may accommodate a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

5. **Duty of Confidentiality**

   All employees of the University who are privy to personal information will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

6. **Review of Privacy Manual**

   This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

7. **Data Breach Protocol**

   The University shall have its own data breach protocol, which shall likewise be reviewed annually, as initiated and proposed by the DPO.

B. Physical Security Measures

1. **Format of data to be collected**

   Personal data in the custody of the organization may be in digital / electronic format and paper-based/physical format, or whatever format required by the state.

2. **Storage type and location**

   All personal data processed by the organization shall be stored in a data room, where paper-based documents are kept in secured filing cabinets or receptacles while the digital / electronic files are stored in the storage and processing system as provided by the University Information Technology Office.

3. **Access procedure of agency personnel**

Only authorized personnel shall be allowed inside the data processing room. Other personnel may be granted access to the room upon filing of an access request form with the Director of the UITO, and with his approval. Physical data storage access shall only be permitted after the written assent of the Director of the Office in charge of the records.

4. **Monitoring and limitation of access to room or facility**

   All office personnel authorized to enter and access the data processing room or facility as well as the physical storage areas, may do so only during office hours.

5. **Design of office space/work station**

   The computers in specific offices where data is processed are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data. They shall be inaccessible to outsiders. Hence, entry to the office premises by outsiders is generally prohibited, and absolutely forbidden for physical storage areas, and the premises of the data processing room of the UITO.

6. **Persons involved in processing, and their duties and responsibilities**

   Persons involved in processing shall always maintain confidentiality and integrity of personal data. Any breach of the personal data committed by them shall be considered as a major offense and shall be dealt with immediately, and accordingly.

7. **Modes of transfer of personal data within the organization, or to third parties**

   Transfers of personal data of Data Subjects to third parties shall not be generally permitted.

   a. However, these may be permitted subject to the approval of the DPO, and only between offices/entities duly authorized to receive personal data, and for legitimate purposes citing relevant laws in support of the permission.

   b. Inter-office data sharing which are usual and routinely shall be permitted, subject to the parameters set by the DPA and relevant education and labor laws.

8. **Retention and disposal procedure**

   All personal information shall form part of the permanent records of data subjects and may only be destroyed upon the order of the court, or by virtue of the relevant laws and regulations.

C. Technical Security Measures

1. **Monitoring for security breaches**

The University shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system as provided by the MIS- UITO.

2. **Security features of the software/s and application/s used**

The Computers used by all the offices of the University are property of the institution. They shall be used only for the purpose that they are intended for. The offices of the University, shall utilize the software applications as provided by reputable suppliers as determined by the UITO. No person shall not introduce into the system any other applications without written permission of the director of the UITO. The director of the UITO shall have full authority to determine the necessity of the software or applications, in case such requests are made.

3. **Process for regularly testing, assessment and evaluation of effectiveness of security measures**

The University shall cooperate with the review of security policies, the conduct vulnerability assessments and the performance penetration testing within the company on regular schedule to be prescribed by the UITO.

4. **Encryption, authentication process, and other technical security measures that control and limit access to personal data**

Each personnel with access to personal data shall verify his or her identity using the access codes and devices provided by the ADDUNet. Passwords should not be shared for whatever reason. The liability for data breaches shall be prima facie presumed against the personnel whose access codes and devices pertain to.

BREACH AND SECURITY INCIDENTS

1. **Data Breach Response Team**

All offices, and employees of the University shall cooperate with the Data Breach Response Team which shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. **Measures to prevent and minimize occurrence of breach and security incidents**

The University shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

3. **Procedure for recovery and restoration of personal data**

   The University, though the UITO, shall maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, comparison with the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach must be made.

4. **Notification protocol**

   In case of data breach, the head of each office which has access to personal information, or any other office with knowledge of such incident shall coordinate with the DPO and the Head of the Data Breach Response Team who shall in turn inform the management of the need to notify the NPC and the data subjects affected, within the period prescribed by law.

5. **Documentation and reporting procedure of security incidents or a personal data breach**

   In case of data breach, the head of each office which has access to personal information, or any other office with knowledge of such incident shall assist the Data Breach Response Team who shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

INQUIRIES REQUESTS FOR RECTIFICATIONS AND COMPLAINTS

Data subjects may inquire or request for rectification, or information regarding any matter relating to the processing of their personal data under the custody of the organization, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization, specifically the Data Protection Officer and briefly discuss the inquiry, together with their contact details for reference.

Inquiries, complaints and requests shall be filed in three (3) printed copies, or to the official email of the DPO (**dataprotection@addu.edu.ph**). The DPO shall confirm with the complainant its receipt of the complaint or inquiry.

INTERNAL POLICIES

The internal policies of the servicing offices of the University, which has access to Personal Information, shall be suppletory to this manual, if these are based on state regulations, established professional ethical considerations, or on recorded official institutional policies. In case of conflict between such internal policies, and this manual, the latter shall prevail, unless due to overriding legal and ethical reasons, to be determined by the DPO.

EFFECTIVITY

The provisions of this Manual are effective immediately, after its approval by the University President.

PERSONAL DATA CORRECTION FORM

To

_____
Data Protection Officer
Ateneo de Davao University
Jacinto Street, Davao City

Basic Information

Name of the person requesting _____
Records you want corrected _____

Details of the Legal representative (In case of minors and those incapacitated, or analogous reasons)

Name of the legal representative _____
Please attach the following

a. Special power of attorney
b. Gov't issued ID bearing the Data Subject'[2]s photo and signature
c. Gov't issued ID bearing the representative's photo and signature

I WISH TO EXERCISE MY RIGHT OF RECTIFICATION IN ACCORDANCE WITH SECTION 16 OF RA 10173, OR THE DATA PRIVACY ACT OF 2012

As such, I hereby request:

A. The RECTIFICATION of the following erroneous data concerning me: (Use the back portion if needed)

Erroneous Data	Correct Data	Certifying Document (Proof of correct Data)

B. The said rectification be also REPORTED to the following parties who previously received such processed personal data:

C. That I be NOTIFIED of the effective rectification of my data or the justified disapproval of the request via (Choose at least one)

a. Contact No._____
b. Email Address _____
c. Postal Address _____

_____ _____
Date Signature

[2] Refers to an individual whose personal information is processed.

REQUEST FOR INFORMATION ON PERSONAL DATA

To

_____
Data Protection Officer
Ateneo de Davao University, Jacinto Street, Davao City

Name of the person requesting _____

Details of the Legal representative (In case of minors and those incapacitated or analogous reasons)

Name of the legal representative _____

Please attach the following

a. Special power of attorney
b. Gov't issued ID bearing the Data Subject'[3]s photo and signature
c. Gov't issued ID bearing the representative's photo and signature

I WISH TO EXERCISE MY RIGHT TO BE INFORMED IN ACCORDANCE WITH SECTION 16 OF RA 10173, OR THE DATA PRIVACY ACT OF 2012

As such, I hereby request:

A. The information of the following data concerning me: (Use the back portion if needed);

(Please check)	Legitimate Purpose for the inquiry
☐ • Description of the personal data to be entered into the system	_____
☐ • Exact Purposes for which they will be processed	_____
☐ • Basis for processing, especially when it is not based on your consent	_____
☐ • Scope and method of the personal data processing	_____
☐ • Recipients, to whom your data may be disclosed	_____
☐ • Methods used for automated access by the recipient, and its expected consequences for you as a data subject	_____
☐ • Identity and contact details of the personal information controller	_____
☐ • The duration for which your data will be kept	_____
☐ • Scope and method of the personal data processing	_____
☐ • Recipients, to whom your data may be disclosed	_____
☐ • Methods used for automated access by the recipient, and its expected consequences for you as a data subject	_____
☐ • Identity and contact details of the personal information controller	_____
☐ Others_____	_____

B. That I be NOTIFIED of the information as to my personal data or the justified disapproval of the request via (Choose at least one)

a. Contact No._____
b. Email Address _____
c. Postal Address _____

_____ _____
Date Signature

Note: Records that are usual and customary (academic records, employment records) that are regularly issued by the University may be directly requested to the offices concerned, i.e. Registrar, HRMDO, etc

[3] Refers to an individual whose personal information is processed.

OBJECTION TO THE USE OF PERSONAL DATA

To

_____
Data Protection Officer
Ateneo de Davao University
Jacinto Street, Davao City

Name of the person requesting _____

Details of the Legal representative (In case of minors and those incapacitated or analogous reasons)

Name of the legal representative _____

Please attach the following

a. Special power of attorney
b. Gov't issued ID bearing the Data Subject[4]' s photo and signature
c. Gov't issued ID bearing the representative's photo and signature

I WISH TO EXERCISE MY RIGHT TO OBJECT IN ACCORDANCE WITH SECTION 16 OF RA 10173, OR THE DATA PRIVACY ACT OF 2012

As such, I hereby OBJECT:

A. To the use of the following personal data (Use the back portion if needed)

Data	Reason	Proof or basis for the objection

B. That I be NOTIFIED of the action taken or the justified disapproval of the request via (Choose at least one)

a. Contact No._____
b. Email Address _____
c. Postal Address _____

_____ _____
Date Signature

[4] Refers to an individual whose personal information is processed.

UNDERTAKING

Know all men by these presents this _____ 20__;

I _____, of legal age, Filipino, and a resident of _____ Philippines.

Do hereby, fully, and knowingly execute this undertaking,

1. **DURATION and EFFECTIVITY**: This undertaking shall be valid during my engagement in the Ateneo de Davao University (University), and thereafter, should my services be severed for whatever cause.
2. **UNDERTAKING**:
    a. I shall retain as confidential all matters relating to the personal information of students, employees and other stakeholders of the University, which may be made available to me, in the exercise of my functions or otherwise.
    b. I shall treat as confidential, until duly authorized in writing by the proper authority of the University, matters relating to any intellectual property, including researches, software and applications, statistical, technical, or scientific data, institutional plans and projections, photographs videos and audio recordings, belonging to the University, or its officers, employees, students, alumni and other stakeholders which may be made available to me, the exercise of my functions or otherwise.
    c. I shall keep highly confidential matters relating to the security and safety of the University premises, its officers, employees, students, alumni and other stakeholders of the University which may be made available to me, the exercise of my functions or otherwise.
3. **REPORTORIAL OBLIGATIONS**: I shall report to the Data Protection Officer, any breach of the privacy of any of its officers, employees, students, alumni and other stakeholders, of the University, that has come to my attention, or may be caused by reason of the exercise of my function, intentionally or otherwise.
4. **CONFLICT OF INTERESTS**: I shall not engage into any endeavor which conflicts with the privacy of any of the officers, employees, students, alumni and other stakeholders, of the University, nor shall I profit from any information relative thereto.
5. I understand that should I violate this undertaking, that I may be liable under RA 10173 (Data Privacy Act of 2012) and other relevant laws.

I have understood the contents of this undertaking and shall abide by it I good faith.

IN WITNESS WHEREOF, the affiant has executed this Undertaking effective as of the date above shown.

_____
Signature over Printed Name
Affiant

ID No._____
Competent Proof of Identity

ACKNOWLEDGEMENT

REPUBLIC OF THE PHILIPPINES)
DAVAO CITY.....)

BEFORE ME, a Notary Public in and for Davao City, personally appeared the affiant, this _____ at Davao City, Philippines, with his/her Competent proof of Identify, known to me and by me known to be the same person who executed the foregoing document, and who acknowledged to me that the same is his/her free and voluntary act and deed.

WITNESS MY HAND AND SEAL on the place and date first above written.

Doc No. _____;
Page No. _____;
Book No. _____;
Series of 20___.

DATA BREACH RESPONSE PROTOCOL

I – General Provisions

Section 1. Scope / Coverage: This manual shall be implemented on all incidents of breach of personal data, which has been collected, processed and stored physically or electronically, on all units and offices of the Ateneo de Davao University, including breaches to facilities where such data have been stored or processed.

Section 2. Definition. For the Purpose of this Manual, the following terms shall be used in the context as herein stated.

a. Core Activity refers to a key operation or process carried out by the University to achieve its mandate or function: Provided, that processing of personal data forms an integral and necessary part of such operations or processes;

b. Commission shall mean the National Privacy Commission

c. Data Breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any data transmitted, or stored, or otherwise processed,

d. Data Breach Response Team. As described in section 3 hereof. May be referred to as the "DBRT"

e. Data processing systems refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

f. Data Protection Officer or "DPO" refers to an individual designated by University to be accountable for its compliance with RA 10175, or the Data Privacy Act, its IRR, and other issuances of the Commission:

g. Data subject refers to an individual whose personal information is processed.

h. Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

i. 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

j. "Restricted Information" includes information, whether under the category of a Sensitive Personal information or not, which are exclusive to offices or persons because of their ethical, professional, or legal obligations.

k. 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;

l. Sensitive personal information refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

m. University refers to the Ateneo de Davao University.

n. University Data Storage Facility refers to any facility, or receptacle or any premises of the University where personal data may be stored or processed, physically or electronically.

II – The Data Breach Response Team

Section 3. Purpose. The Data Breach Response Team is mandated to ensure the integrity, promptness and regularity of all investigations of incidents of data breach in the University. In this regard; it is empowered to;

1. Supervise and / or control the investigations relative to data breaches.

2. Create, as the DBRT desires, reasonable and legal procedures for investigation of incidents of data breach.

3. Call upon witnesses, relevant to any investigation it may conduct

4. Recommend to the University President the specific actions that may be done relative to data breach

5. Recommend university policies in relation to data privacy management.

6. Consults with the DPO other on whether or not any occurring data breach requires the University, to submit a report to the Commission

7. Such other functions that the University may delegate it, and those which are compatible to its general functions.

Section 4. Composition. The Breach Response Team shall be composed of the following;

1. The Data Protection officer, who shall act as the head of the team

2. The Executive Vice President

3. The Director of the University Information Technology Office

4. The Vice President for Finance

5. The Director of the Human Resource and Development Office

6. The University Legal Counsel

7. Head of the Communication or press relations of the University

III – Breach Protocol

Section 5. Immediate Response Protocol. The following shall be the immediate actions that must be taken within 24 hours, in the event of any Data Breach

1. The head of the office where the data breach appears to have occurred, must contact the Data Protection Officer and the University Legal Counsel, and report the incident.

2. The DPO shall make his initial assessment and shall record the date and time when the breach was discovered, as well as the current date and time when response efforts have been initiated.

3. The DPO shall immediately alert and activate everyone on the DBRT, as well as the relevant personnel or administrator or head of office involved, to begin executing protocols in this Manual. Should the breach involve data from the University's core activities, the Academic Vice President, and the Director of Human Resources Development Office must be promptly notified. Should the

same involve restricted information, the head of office in custody or control of such data shall likewise be immediately notified.

4. The head of office in custody or control of the data or Data Storage Facility breached must secure the premises around the area / or the equipment where the breach occurred to help preserve evidence.

5. Additional data loss must be inhibited. The affected machines must be taken offline. These however must not be turned off. No personnel may probe into the equipment sans the authority of the Team.

6. The DPO shall document everything known thus far about the breach: (See Annex)

    A. Identify:

        i. The name of the reporter

        ii. To whom the matter was initially reported,

        iii. Names of individuals who know of the incident (Witnesses)

    B. Specify:

        i. The type of breach,

        ii. What data was probably compromised

        iii. How was data was stolen,

        iv. The data processing systems affected,

        v. If there are devices are missing.

        vi. The facility broken into.

7. The Team may initially Interview those involved in discovering the breach and anyone else who may know about it.

8. The Team shall assess priorities and risks based on the initial data collected.

9. If indeed a breach has been committed within the context of RA 10173, report the same to the national Privacy Commission within 72. Hours, subject to the consultation with the team.

10. If no breach has been actually committed, the incident shall be recorded, together with the basis for such findings. However, this is without prejudice to the possibility

of review, should any member of the team, or the DPO finds probable cause for the re-evaluation.

11. No press release may be made, unless allowed by the University President, after due advice from the Team.

Section 6. Comprehensive Investigation Protocol. The team shall conduct the following subsequent to its initial determination of breach.

1. Further intensive investigation must be conducted to determine the possible causes and contributory factors of the breach. Should the Team find it necessary, it may delegate the technical investigation of the breach to internal specialists or may source out the same. The advice of the Director of the University Information Technology Office must be given weight.

2. Should the breach be by virtue of the unlawful access or manipulation of outsiders, investigation may ensue, with the aid of government agencies in charge of cybercrime law enforcement.

3. If by Initial Investigation the breach was caused by a member of the University Community, the matter may be submitted to the Human Resource Director or Director of the office in charge of student disciple for the unit involved, as the case may be, for the Conduct of the necessary investigation, following the requirements of due process.

4. The offenders may be dealt with depending on their capacity and intentions.

   a. Should the breach be by virtue of the unlawful act by an employee, the same shall be reported for appropriate administrative action, and without prejudice to his prosecution in the appropriate courts of law. In case the breach was by virtue of an accident committed by a member of the University Community, the appropriate administrative action may only be recommended. If the negligence is criminal in nature, prosecution in the appropriate courts of law may still be pursued by the University against the offender.

   b. Should the breach be by virtue of the unlawful access or manipulation of outsiders, the matter shall be referred to the University Legal Counsel for the filing of the appropriate criminal or civil actions.

5. Assessment shall be made on the possible legal obligations of the University due to the breach. The Team shall identify the priority or order of what must be addressed.

6. The Team shall propose actions to rectify the breach committed. Rectification may include the notification of the University of the same to affected Data subjects, especially if the breach has compromised their security and privacy

7. The Team shall identify and inform the administration of the possible conflicting initiatives that may result from the legal actions or other recommendations that it may raise from the investigation.

Section 7. Security incident. Any incident that may tend to undermine the security and privacy of any data may be subject of an inquiry or investigation by the Team. The team shall recommend to the University President the immediate action needed to prevent any threat of breach.

IV – NOTIFICATIONS

Section 8. Notification to the National Privacy Commission. Should the breach affect the Personal information of the Data Subjects of the University, the Data Protection Officer shall determine whether the same constitutes as among the incidents that must be reported to the Commission. Such Notification shall be made within 72 hours upon knowledge of, or when there is reasonable belief by the DPO that, a personal data breach requiring notification has occurred, after due consultation with the Team. The affected data subjects shall be similarly notified.

Section 9. When required. Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the University believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Section 10. Contents of Notification. The notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the University, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

Section 11. Delay of Notification. Notification may be delayed only 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, or as allowed by RA 10173.

IMMEDIATE RESPONSE CHECKLIST

1. **Date and time of the breach** _____

2. **What was the facility, system, equipment breached?** _____

3. **The name of the reporter.** _____
   i. What is his designation? _____
   ii. Who is his immediate superior?_____

4. **To whom was the matter initially reported?** _____

5. **Who are the witnesses?**
   a. Name _____ Designation_____
   b. Name _____ Designation_____
   c. Name _____ Designation_____
   d. Name _____ Designation_____

6. **Describe the Breach**
   a. The manner of Breach:
      ☐ Accidental
      ☐ Intentional / Unlawful

   b. Classification of the Data breached
      ☐ Electronic
      ☐ Physical
      ☐ University Data Storage Facility

   c. The Type of Breach:
      ☐ Destruction
      ☐ Loss
      ☐ Alteration
      ☐ Unauthorized Disclosure
      ☐ Unauthorized Access
         ☐ Duplication. Manner of duplication of data, if known _____
         ☐ Hacking.
         ☐ Equipment
      ☐ Others, Please describe_____

7. What data was probably compromised?
   ☐ Personal Data (Names, Address, Grades, Salary)
   ☐ Sensitive personal information
   ☐ Restricted Information
   ☐ Others (Describe) _____
   _____

8. The systems affected, (for electronic breaches)
   ☐ Student Information System
   ☐ Academic Information System
   ☐ Academic Information management system
   ☐ Employees Portal
   ☐ Online Purchasing
   ☐ Other such automated systems which contain personal data

9. What Facility was breached? _____

10. Are there are devices that are ☐ missing or ☐ destroyed?
    Please indicate _____

_____ _____

Signature over printed name Date and Time