



**FEU ALABANG**

# **DATA PRIVACY MANUAL**

## I. INTRODUCTION

FEU Alabang is dedicated to upholding individual's data privacy rights and has implemented this Data Privacy Manual to encourage conscientiousness in respecting these rights. This manual promotes adherence to the fundamental principles of transparency, legitimate purpose, and proportionality along with the enforcement of robust data security measures.

FEU Alabang is committed to complying with the provisions of Republic Act No. 10173, also known as the Data Privacy Act of 2012, including its implementing rules and regulations, relevant policies, and issuances of the National Privacy Commission and all other requirements, and standards to continuously improve and effectively manage the security of personal data.



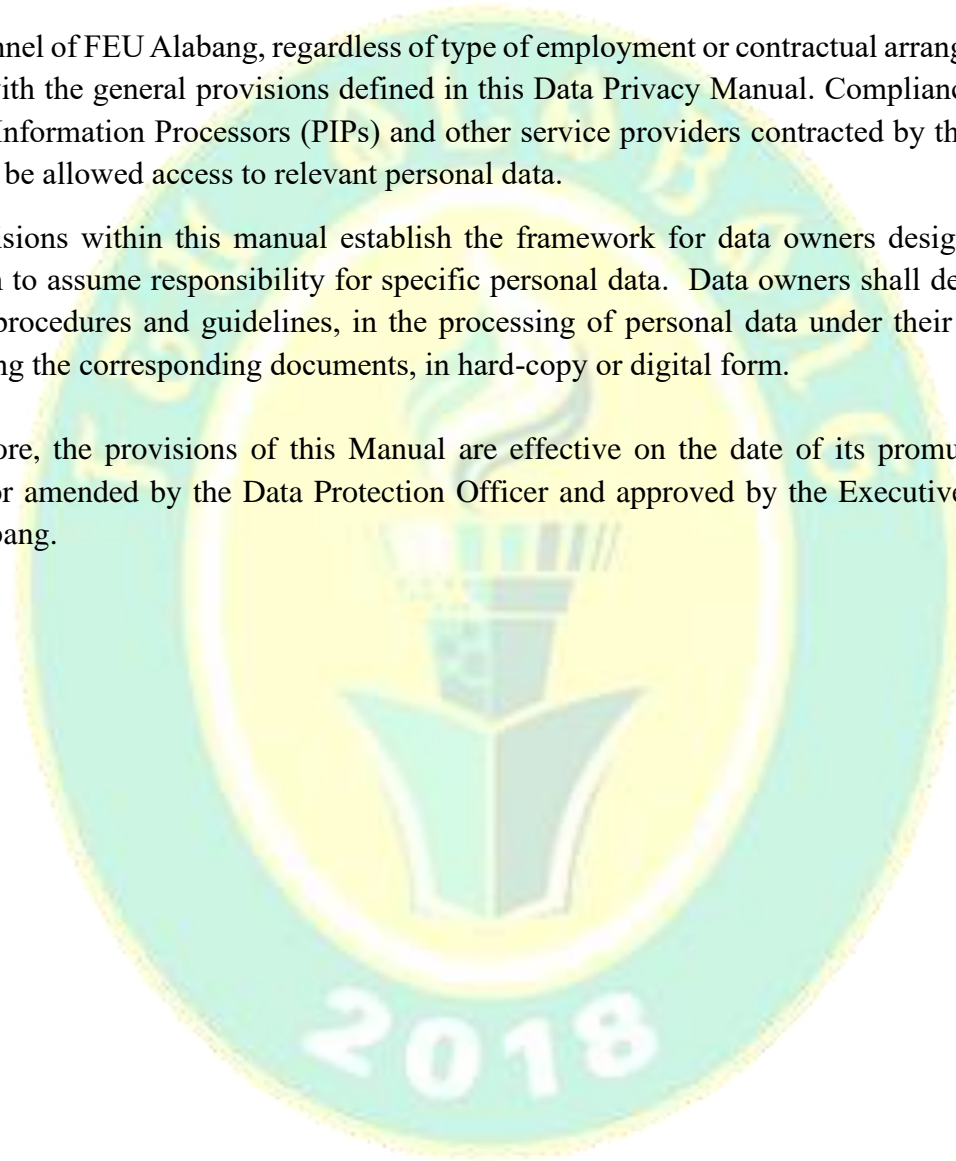
## II. SCOPE AND EFFECTIVITY

This Data Privacy manual guides the acts and decisions of all types of students, parents, guardians, faculty, associates, contractual personnel, retirees, applicant students, applicant faculty, applicant associates, clients, customers, alumni, subcontractors, outsources, licensees, and other persons whose personal data are directly or indirectly processed by FEU Alabang.

All personnel of FEU Alabang, regardless of type of employment or contractual arrangement, must comply with the general provisions defined in this Data Privacy Manual. Compliance extends to Personal Information Processors (PIPs) and other service providers contracted by the institution, who shall be allowed access to relevant personal data.

The provisions within this manual establish the framework for data owners designated by the institution to assume responsibility for specific personal data. Data owners shall define detailed policies, procedures and guidelines, in the processing of personal data under their custody and formulating the corresponding documents, in hard-copy or digital form.

Furthermore, the provisions of this Manual are effective on the date of its promulgation until revoked or amended by the Data Protection Officer and approved by the Executive Director of FEU Alabang.



### III. PROCESSING OF PERSONAL DATA

FEU Alabang collects, stores, perform operations, retrieves, or otherwise process the personal information of students, parents, guardians, faculty, associates, alumni, contractors, and other parties and stakeholders to carry out the performance of its functions of instructions as a higher education institution.

In all actions and decisions involving personal data, FEU Alabang shall ensure that the following privacy principles are applied:

**Transparency.** The individual must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

**Legitimate purpose.** The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

**Proportionality.** The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

#### A. Grounds and purposes of processing personal data

The basis of FEU Alabang's processing of personal data may be one or more of the following grounds:

1. An academic institution offering tertiary education and senior high school.
2. Deciding and acting the welfare of its students, their parents and guardians, faculty, associates, alumni, and
3. Administering its internal and external affairs as an academic institution.

Based on one or more of the above-mentioned grounds, FEU Alabang processes personal data to achieve the following purposes:

1. Academic, research, extra-curricular, student welfare, and disciplinary purposes;
2. Supervision of academic and researchers endeavors;
3. Management of human resources and supervision of work conduct;
4. Student and employee application processing and identity verification purposes;

5. Documentation and record-keeping purposes;
6. Medical, physical, psychiatric, and psychological attention purposes;
7. Alumni linkage, donation, and funding purposes;
8. Customer, client, or community service purposes;
9. Contractual and financial purposes;
10. Regulatory and audit purposes.

**B. Types of personal data processed by FEU Alabang are:**

1. Personal details such as name, birthdate, gender, civil status, and affiliations;
2. Contact information such as address, email, mobile, and telephone numbers;
3. Academic information such as grades, course, and academic standing;
4. Employment information such as government-issued numbers, salary, position, and functions;
5. Applicant information such as academic background and previous employments;
6. Medical information such as physical, psychiatric, and psychological information.

FEU Alabang shall adopt the following general provisions on the processing of personal data that adhere to the general principles of collection, processing, and retention of personal data, and to the criteria for lawful processing of personal information, sensitive personal information, and privileged information.

**C. Collection**

1. A Privacy Policy Notice shall be provided to the data subject prior to the collection of personal data. The Privacy Policy Notice of the Institution shall be written in clear and plain language to ensure understandability, shall be accessible at any point in time, and shall include the following:
  - a) Service Description
  - b) Identification of the PIC
  - c) Personal data that are collected
  - d) Collection method
  - e) Timing of collection
  - f) Purpose(s) for which personal data will be collected and used
  - g) Storage and transmission of personal information
  - h) Method of use
  - i) Location of personal data
  - j) Third party transfer
  - k) Retention period
  - l) Participation of data subject
  - m) Inquiry

2. Consent on the Privacy Policy Notice shall be obtained directly from the data subject, or from parent or legal guardian of a data subject of minor age, prior to collection of personal data. Withdrawal of consent shall be always allowed upon receipt of a written intent.
3. Only personal data that is necessary and compatible with the declared, specified, and legitimate purpose shall be collected directly from the data subject, or parent or legal guardian of a data subject of minor age.
4. A formal confirmation that the provided personal data is accurate and may be used for the declared, specified, and legitimate purpose shall be obtained directly from the data subject, or from parent or legal guardian of a data subject of minor age.

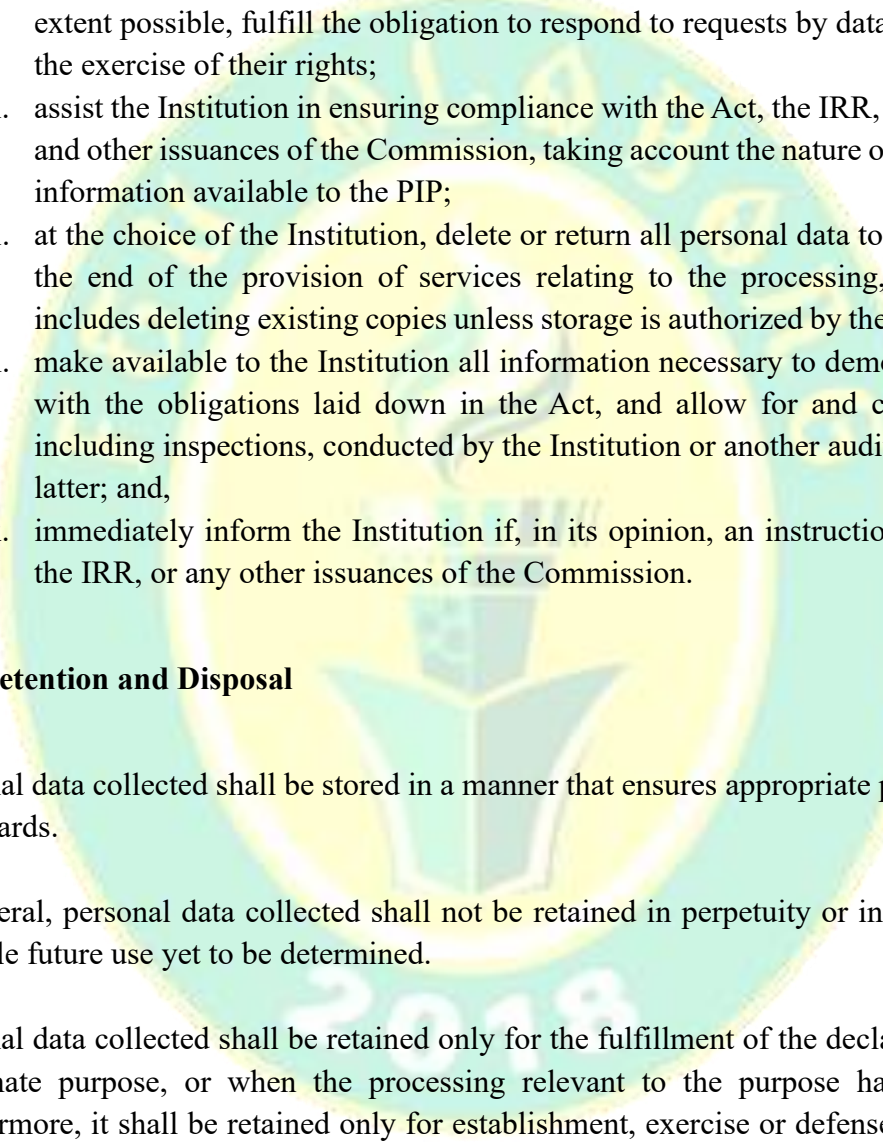
#### **D. Usage**

1. Processing of personal information shall be allowed under the following conditions:
  - a) Consent of the data subject has been obtained prior to collection or as soon as practicable and reasonable.
  - b) The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement.
  - c) The processing is necessary to protect vitally important interests of the data subject, including his or her life and health.
  - d) The processing is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law.
  - e) The processing is necessary for the fulfillment of the constitutional or statutory mandate of a public authority.
  - f) The processing is necessary to pursue legitimate interests of the institution, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.
2. Processing of sensitive personal information and privileged information is prohibited, except in any of the following cases:
  - a) Consent is given by the data subject, or parent or legal guardian of a data subject of minor age, or by the parties to the exchange of privileged information, prior to processing, which shall be undertaken pursuant to a declared, specified, and legitimate purpose.

- b) The processing is provided for by existing laws and regulations, provided that said laws and regulations do not require the consent of the data subject for the processing and guarantee the protection of personal data.
  - c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing.
  - d) The processing is necessary for the purpose of medical treatment, provided that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured.
  - e) The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.
3. Only personal data collected directly from the data subject, or from parents or legal guardian of a data subject of minor age, shall be processed.
  4. Personal data collected shall be fairly and lawfully processed. Processing of personal data collected shall be in a manner compatible with declared, specified, and legitimate purpose.
  5. Only personal data collected that is accurate and kept up-to-date shall be processed. A policy and procedure on regular updating of personal data collected shall be implemented.
  6. Inaccurate or incomplete personal data shall be rectified or supplemented. Otherwise, the personal data shall be restricted for further processing or shall be destroyed.
  7. Processing of personal data collected shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which the personal data are to be processed.
  8. There shall be transparency in processing personal data. Data subjects shall be provided with sufficient information to know the nature and extent of processing. Information provided to the data subject shall be in clear and plain language to ensure that they are easy to understand, and shall be accessible at all times.
  9. The Institution shall uphold the rights of data subjects in processing personal data collected. Processing of personal data shall be discontinued immediately upon receipt of a written intent from a data subject, or from parent or legal guardian of a data subject of minor age, to withdraw consent, object, or refuse processing.

10. Processing of personal data collected or shared from a party other than the data subject, or parent or legal guardian of a data subject of minor age, shall be allowed under any of the following conditions:
  - a) It is expressly authorized by law, and that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose, and proportionality.
  - b) Consent have been obtained from the data subject, or from parent or legal guardian of a data subject of minor age, even when the personal data was collected or shared by an affiliate or mother company, or similar relationships.
  - c) It is for purposes of research, and the personal data collected is publicly available or consent from the data subject, or from parent or legal guardian of a data subject of a minor age, have been obtained. Adequate safeguards shall be in place and no decision directly affecting data subjects shall be made on the basis of the personal data collected or processed. The rights of the data subjects shall be upheld without compromising research integrity.
  - d) It is for the purpose of a public function or provision of a public service.
11. Processing of personal data collected beyond originally declared, specified, or legitimate purpose shall be allowed for historical, statistical, or scientific purposes, and in cases laid down in law.
12. Processing of personal data for the purpose of surveillance, interception, or recording of communications shall comply with the Act, including adherence to the principles of transparency, proportionality, and legitimate purpose.
13. Subcontracted or outsourced processing of personal data shall be governed by a contract or other legal act to ensure that proper safeguards are in place, to ensure the confidentiality, integrity, and availability of the personal data processed, to prevent its use for unauthorized purposes, and to generally comply with the requirements of the Act, the IRR, other applicable laws for processing of personal data, and other issuances of the Commission. Subcontracting or outsourcing agreements shall:
  - a) bind the PIP to the Institution;
  - b) set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the Institution, and the geographic location of the processing;
  - c) stipulate, in particular, that the PIP shall:
    - i. process the personal data only upon the documented instructions of the Institution, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
    - ii. ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;



- 
- iii. implement appropriate security measures and comply with the Act, the IRR, and other issuances of the Commission;
  - iv. not engage another processor without prior instruction from the Institution, provided that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
  - v. assist the Institution, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
  - vi. assist the Institution in ensuring compliance with the Act, the IRR, other relevant laws, and other issuances of the Commission, taking account the nature of processing and the information available to the PIP;
  - vii. at the choice of the Institution, delete or return all personal data to the Institution after the end of the provision of services relating to the processing, provided that this includes deleting existing copies unless storage is authorized by the Act or another law;
  - viii. make available to the Institution all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the Institution or another auditor mandated by the latter; and,
  - ix. immediately inform the Institution if, in its opinion, an instruction infringes the Act, the IRR, or any other issuances of the Commission.

#### **E. Storage, Retention and Disposal**

1. Personal data collected shall be stored in a manner that ensures appropriate privacy and security safeguards.
2. In general, personal data collected shall not be retained in perpetuity or in contemplation of a possible future use yet to be determined.
3. Personal data collected shall be retained only for the fulfillment of the declared, specified, and, legitimate purpose, or when the processing relevant to the purpose has been terminated. Furthermore, it shall be retained only for establishment, exercise or defense of legal claims, or for legitimate business purpose that is consistent with standards or approved by appropriate government agency.
4. A personal data retention policy that is aligned with the appropriate standards and regulatory requirements shall be implemented by the institution.

5. Retention of personal data collected and processed further for historical, statistical, or scientific purposes, and in cases laid down in law, shall be allowed with the implementation of appropriate organization, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of data subjects. It is recommended that the personal data collected and process further, be aggregated or kept in a form which does not permit identification of data subjects.
6. Appropriate policy to securely dispose or discard personal data collected that is beyond its retention period shall be implemented to prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of data subjects.

## **F. Sharing and Disclosure**

1. Data sharing shall be allowed only under any of the following conditions:
  - a) It is expressly authorized by law, and that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose, and proportionality.
  - b) Consent for disclosure or sharing have been obtained from the data subject, or parent or legal guardian of a data subject of minor age, even when the personal data was collected or shared by an affiliate or mother company, or similar relationships. In addition, sufficient information on the disclosure or sharing shall be provided to data subjects prior to collection of personal data or before data is shared. A data sharing agreement shall also cover data sharing even for commercial purposed including direct marketing. Further processing of shared data shall adhere to the data privacy principles laid down in Act, the IRR, and other issuances of the Commission.
  - c) It is for purposes of research, and the personal data collected is publicly available or consent from the data subject, or parent or legal guardian of a data subject of minor age, has been obtained. Adequate safeguards shall be in place and no decision directly affecting the data subjects shall be made on the basis of the personal data collected or processed. The rights of the data subjects shall be upheld without compromising research integrity.
  - d) It is for the purpose of a public function or provision of a public service, which shall be covered by a data sharing agreement.
2. The following information on disclosure and sharing shall be provided to data subjects prior to collection of personal data or before personal data is shared:
  - a) Identity of the PIP that will be given access to the personal data.
  - b) Purpose of data sharing.
  - c) Categories of personal data concerned.
  - d) Intended recipients or categories of recipients of the personal data.

- e) Existence of rights of data subjects, including the right to access and correction, and the right to object.
  - f) Other information that would sufficiently notify the data subjects of the nature and extent of data sharing and the manner of processing.
3. The data sharing agreement shall establish adequate safeguards for data privacy and security and uphold rights of data subjects. All party to the data sharing agreement shall comply with the Act, the IRR, and all other issuances of the Commission.



## **IV. SECURITY MEASURES**

FEU Alabang shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. Necessary steps shall be taken to ensure that any FEU Alabang personnel or associates acting under authority and who has access does not process personal data except upon instructions or as required by law.

The following security measures shall aim to maintain the availability, integrity, and confidentiality of personal data, and are intended for protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. The measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

In addition, the Institution shall strive to adopt a personal data security management system that is aligned to the requirements of appropriate national and international standards.

### **A. Organizational Security Measures**

1. A Data Protection Officer shall be designated to be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.
2. The Institution shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and for such purpose, take into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedom of data subjects. These policies shall:
  - a) implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
  - b) implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed.
  - c) determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility and,
  - d) provide for documentation, regular review, evaluation, and updating of the privacy and security policies.

3. Records of processing activities shall be maintained. These records shall sufficiently describe its data processing systems and identify duties and responsibilities of individuals who will have access to personal data. The records shall include:
  - a) Information about the purpose of the processing of personal data, including any intended future processing or data sharing.
  - b) A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing.
  - c) General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits of disposal or erasure of personal data.
  - d) A general description of the organizational, physical, and technical security measures in place.
  - e) The name and contact details of the President of the Institution and, where applicable, the joint controller, its representative, and the compliance officer or DPO, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.
4. All FEU Alabang personnel or associates shall hold and operate personal data in their possession or that come to their knowledge, under strict confidentiality and secrecy, especially if the personal data are not intended for public disclosure. This obligation shall extend even after transferring to another position, upon resignation, or upon termination of employment or contractual relations. Orientations, training, or capacity building programs regarding privacy or security policies, shall be conducted for all Institution personnel.
5. The Institution shall develop, implement, and review policies and procedures:
  - a) for the collection of personal data.
  - b) that limit the processing of data to ensure that it is only to the extent necessary for the declare, specified, and legitimate purpose.
  - c) for access management, system monitoring, and protocols to follow during security incidents or technical problems.
  - d) for data subjects to exercise their rights under the Act.
  - e) for data retention, including timeline or conditions for erasure or disposal of records.
6. The Institution shall engage only with PIPs that provide sufficient guarantees to implement appropriate security measures specified in the Act and the IRR, and that ensure the protection of the rights of the data subjects. Engagements with PIPs shall be covered with appropriate contractual agreements.
7. The Data Protection Officer has the responsibility to:
  - a) Comply with legal and regulatory obligations related to data privacy.
  - b) Provide data protection support to various units and offices.

- c) Enforce FEU Alabang's policies related to data privacy, information security, records management, and data governance.
  - d) Coordinate with relevant offices to strengthen organizational, physical and technical security measures, and
  - e) Supervise Privacy Lead Persons in the ensuring data privacy across FEU Alabang.
8. Privacy Lead Persons have the responsibility to
- a) Support the Data Protection Officer's endeavors and initiatives.
  - b) Implement privacy policies and initiatives.
  - c) Proactively prevent, monitor, mitigate, and manage existing or reasonably foreseeable security incidents and personal data breaches in their respective units.
  - d) Shall conduct a Privacy Impact Assessment (PIA) of their units relative to all activities, projects, and systems involving the processing of personal data. This shall be done under the guidance and supervision of the Data Protection Team

## **B. Physical Security Measures**

1. Detailed policies and procedures shall be established to monitor and limit access to and activities in the room, workstation, and facilities, including guidelines that specify the proper use of and access to all kinds of media containing personal data collected.
2. Office spaces and workstations shall be designed/re-designed to provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.
3. Duties, responsibilities, and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or workstation, at any given time.
4. All personnel or associates involved in the processing of personal data shall implement policies and procedures regarding the transfer, removal, disposal, and re-use of all kinds of media, to ensure appropriate protection of personal data.
5. Detailed policies and procedures shall be established to prevent mechanical destruction of files and equipment. The rooms, workstations, and facilities shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

### C. Technical Security Measures

The Institution shall adopt and establish the following technical security measures:

1. A security policy with respect to the processing of personal data.
2. Safeguards to protect computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network.
3. Ability to ensure and maintain the confidentiality, integrity, availability, and resilience of processing systems and services.
4. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach.
5. Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
6. A process for regularly testing, accessing, and evaluating the effectiveness of security measures.
7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

## **V. DATA BREACH AND SECURITY INCIDENTS**

FEU Alabang shall be responsible for any personal data under its control and custody, including data that have been outsourced or transferred to a PIP or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

The Institution shall be accountable for complying with the requirements of the Act, the IRR, and other issuances of the Commission. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a PIP or third party.

In these regards, the Institution shall, at all times, be prepared for any data breach and security incidents with the implementation of a Data Security Incident Management Policy which includes the following:

1. A Data Security Incident Response Team with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach. At the minimum, the team shall be composed of the Data Protection Office, Risk Manager, and Chief Internal Audit Executive. The responsibility of the team shall include:
  - a. Implementing the security incident management policy.
  - b. Managing security incident and personal data breaches.
  - c. Compliance with the relevant provisions of the Act, the IRR, and all related issuances by the Commission on personal data breach management.
2. Organizational, physical, and technical security measures, and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure timely discovery of a security incident. The measures shall include:
  - a. Conduct of a privacy impact assessment to identify attendant risks in the processing of personal data. It should take into account the size and sensitivity of the personal data being processed, the impact and likely harm of a personal data breach.
  - b. Data governance policy that ensures adherence to the principles of transparency, legitimate purpose, and proportionality.
  - c. Implementation of appropriate security measures that protect the availability, integrity, and confidentiality of personal data being processed.
  - d. Regular monitoring for security breaches and vulnerability scanning of computer networks.
  - e. Capacity building of personnel or associates to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents. Any personnel or associates, who becomes aware of a personal data breach and security incident, shall immediately inform his/her direct supervisor, who shall in turn, inform the DPO, or the DPO directly.
  - f. Procedure for regular review of policies and procedures, including the testing, assessment, and evaluation of the effectiveness of the security measures.



3. Incident response procedure intended to contain a security incident or personal data breach and restore the integrity of the information and communications system.
4. Mitigation of possible harm and negative consequences to data subjects in the event of a personal data breach.
5. Compliance with the Act, the IRR, and all related issuances of the Commission pertaining to personal data breach notification.

In the event of any personal data breach and security incident, the Institution shall:

1. Convene the Data Security Incident Response Team immediately upon knowledge of the incident. The team shall:
  - a. Manage effectively and respond timely to the incident.
  - b. Assess the impact of the breach.
  - c. Ensure that corresponding actions are taken to mitigate its impact.
  - d. Coordinate the formulation and implementation of corrective actions to lessen recurrence of the incident.
  - e. Manage the incident until its final resolution.
2. Notify the Commission and affected data subjects within seventy-two (72) hours upon knowledge of the incident, when there is reasonable belief that:
  - a. Sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud.
  - b. The personal data have been acquired by an unauthorized person.
  - c. The incident is likely to give rise to a real risk of serious harm to the affected data subjects.
3. Consider the following if there is doubt as to whether notifying the Commission and the affected data subjects is indeed necessary:
  - a. Likelihood of harm or negative consequences on the affected data subjects.
  - b. Reduction of risks arising from the personal data breach reasonably believed to have occurred.
  - c. Involvement of:
    - i. information that would likely affect national security, public safety, public order, or public health.
    - ii. at least one hundred (100) individuals.
    - iii. information required by all applicable laws or rules to be confidential; or,
    - iv. personal data of vulnerable groups.

4. Prepare an incident report that includes the following:
  - a. Nature of the breach that includes:
    - i. Description of the incident.
    - ii. chronology of events, and
    - iii. an estimate of the number of data subjects affected.
  - b. Description of the personal data involved.
  - c. Remedial measures taken that include:
    - i. Description of the measures taken to address the breach.
    - ii. actions being taken to secure or recover the personal data that were compromised,
    - iii. actions performed to mitigate possible harm or negative consequences and limit the damage or distress to those affected by the incident.
    - iv. actions being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification, and
    - v. measures being taken to prevent a recurrence of the incident.
  - d. Name and contact details of person(s) designated to provide additional information.
5. If notifying the Commission is required, submit the incident report to the Commission within five (5) days from notification. In any case, all incident reports shall be made available when requested by the Commission. A summary of all incident reports shall be submitted to the Commission annually, comprised of general information including:
  - a. Number of incidents and breach encountered.
  - b. Information classified according to their impact on the availability, integrity, or confidentiality of personal data.

## VI. INQUIRIES AND COMPLAINTS

FEU Alabang shall, at all times, uphold the rights of data subjects.

Data subjects may send inquiries on matters relating to the processing of their personal data collected, or the data privacy and security policies implemented by the Institution.

Data subjects may also send complaints on suspected or actual data breach or security incident, violation of their rights to data privacy, or inconsistencies in the implementation of the provisions of the data privacy policies adopted by the Institution.

Inquiries and complaints shall be sent to [dpo@feualabang.edu.ph](mailto:dpo@feualabang.edu.ph) or directly to the Data Protection Officer whose information is below;

### **The Data Protection Officer**

FEU Alabang

Wood District, Corporate Woods cor. South Corporate Avenues

Filinvest City, Alabang

Telephone Number: (02) 8288-8338 Loc 137

Email: [dpo@feualabang.edu.ph](mailto:dpo@feualabang.edu.ph)



## VII. DEFINITION OF TERMS

Whenever used in this manual, the following terms shall have the respective meaning:

- A. **“Act”** refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012.
- B. **“Commission”** refers to the National Privacy Commission.
- C. **“Consent of the data subject”** refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative, or an agent specifically authorized by the data subject to do so.
- D. **“Data owner”** refers to an individual or entity that has approved management responsibility for controlling the processing of specific personal data.
- E. **“Data subject”** refers to an individual whose personal, sensitive personal, or privileged information is processed.
- F. **“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.
- G. **“Data sharing”** is the disclosure or transfer to a third party of personal data under the custody of FEU Alabang or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the Institution. The term excludes outsourcing, or the disclosure or transfer of personal data by the Institution to a personal information processor.
- H. **“Direct marketing”** refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.
- I. **“Filing system”** refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for the purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

- J. **“Implementing Rules and Regulations” or “IRR”** refers to Implementing Rules and Regulations of the Data Privacy Act of 2012.
- K. **“Information and communications system”** refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.
- L. **“Personal data”** refers to all types of personal information.
- M. **“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.
- N. **“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.
- O. **“Personal information controller” or “PIC”** refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes;
1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization.
  2. A natural person who processes personal data in connection with his or her personal, family, or household affairs.
- There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose, or extent of its processing.
- P. **“Personal information processor” or “PIP”** refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.
- Q. **“Processing”** refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating, or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.

- R. **“Profiling”** refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
- S. **“Privileged information”** refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.
- T. **“Public authority”** refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions.
- U. **“Security incident”** refers to an event or occurrence that affects or tends to affect data protection or may compromise the availability, integrity, and confidentiality of personal data. It includes incidents that would result to personal data breach, if not for safeguards that have been put in place.
- V. **“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.
  4. Specifically established by an executive order or an act of Congress to be kept classified.
- W. **“Institution”** refers to FEU Alabang.

## VIII. PROMULGATION

The provision of this Data Privacy Manual shall take effect this May 27<sup>th</sup> 2024, unless revoked or amended by FEU Alabang.

Prepared by:

**(sgd) Engr. Reynaldo C. Muli**  
Data Protection Officer  
Senior Director for Higher Education  
FEU Alabang

Approved by:

**(sgd) Engr. Remelita H. Avenido**  
Executive Director  
FEU Alabang

