CARAGA STATE UNIVERSITY

DATA PRIVACY MANUAL

Table of Contents

PART I. INTRODUCTION

The Caraga State University (CSU) hereby adopts this Data Privacy Manual in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission.

It is the policy of CSU to respect and uphold data privacy rights, and to ensure that all personal data collected from employees, students, their parents or guardians and other stakeholders are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality as stated in DPA.

This Manual outlines the data protection and security measures adopted by the University to protect data privacy rights, and shall serve as a guide in the exercise of rights under the DPA.

PART II. POLICY STATEMENT

CSU is committed to protect the privacy rights of individuals on personal information pursuant to the provisions of Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations and other government policies and issuances.

All CSU faculty, administrative staff, officials and students are enjoined to comply with and to share in the responsibility to secure and protect personal information collected and processed by CSU in pursuit of legitimate purposes.

General Privacy Policy Statements

A. CSU adheres to the general principles of transparency, legitimate purpose and proportionality in the collection, processing, securing, retention and disposal of personal information.

B. The faculty, administrative staff, officials, students or third parties whose personal information is being collected shall be considered as data subjects for purposes of these policies.

C. Data subjects shall be informed the reason or purpose of collecting and processing of personal data.

D. The data subjects shall have the right to correct the information especially in cases of erroneous or invalid or obsolete data, and to object to collection of personal information within the bounds allowed by privacy and other related laws.

E. The data subject has the right to file a complaint in case of breach or unauthorized access of his personal information.

F. CSU shall secure the personal information of faculty, administrative staff, officials, students and third parties from whom personal information is collected and shall take adequate measures to secure both physical and digital copies of the information.

G. CSU shall ensure that personal information is collected and processed only by authorized personnel for legitimate purposes of the University.

H. Any information that is declared obsolete based on the internal privacy and retention procedures of the University shall be disposed of in a secure and legal manner.

I. Any suspected or actual breach of the CSU Data Privacy Policy must be reported to any member of the Data Protection Team in accordance with the procedure provided in Part IX Section 2 of this Manual.

J. Data subjects may inquire or request for information from the Data Protection Team, regarding any matter relating to the processing of their personal data under the custody of CSU, including the data privacy and security policies implemented to ensure the protection of their personal data pursuant to Part IX Section 1 of this Manual.

PART III. DEFINITION of TERMS

A. "**Authorized personnel**" refers to employees or officers of the University specifically authorized to collect and/ or to process personal information either by their function of their office or position, or through specific authority given in accordance with the policies of the University.

B. "**Compliance Officer for Privacy (COP)"** refers to the University officer designated to assist the supervising DPO in the performance of its functions. The COP shall perform all other functions of a DPO and is a member of the Data Protection Team.

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 Sharing**" refers to the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.

E. "**Data subject**" refers to an individual whose personal, sensitive personal or privileged information is processed. For purposes of this Manual, students, employees and third parties whose information is being collected and processed by the University (i.e. applicants for admission or employment, former students or alumni whose records are required by law to be kept and maintained by the University). The data subjects have the right to be informed [Part V Section 3] and object or complain [Part IX Sections 1 and 2], right to access [Part VIII Section 2] their individual information, and the right to correct, rectify or block [Part VII Sections 1 and 2] any erroneous or false information.

F. "**Data Protection Officer or DPO**" refers to the University officer designated by the CSU President to monitor and ensure the implementation of the Data Privacy policies of the University. The DPO isalso the de facto head of the Data Protection Team.

G. "**Data Protection Team**" refers to the group of persons designated to acton inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the Data Privacy policy of the University. The CSU Data Protection Team (DPT) is composed of the Data Protection Officer (DPO), the Compliance Officer for Privacy (COP) and Personnel Information Controllers (PICs).

H. "**Personal data**" refers to all types of personal information collected and processed by the University from the data subjects.

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. "**Personal Data Classification**" refers to the *categories of personal information* collected and processed by CSU. Personal data is classified as follows:

1. **Public**- these are information readily available and may be disclosed to the public. Examples: CSU offices directory, subject offerings, names of officers, Principal and teachers as stated in the Administration portion of the CSU website, published research containing the names of teachers and students

2. **Confidential**- Those which are declared confidential by law or policy of CSU and which may only be processed by authorized personnel, and if disclosed may cause material harm to the University, or information is sensitive in nature as will affect the health or well-being of the individual.

   Examples: employees and student names, addresses, contact numbers, GSIS/SSS Numbers,PhilHealth Numbers, HMDF/ Pag-ibig Numbers, Passport Numbers, employee's and student's health information, student counselling, disciplinary records and medical records (Data Privacy Law); financial information of parents of students and employees, personnel evaluation recordsand student records (like transcript of records and student evaluation results and other records as enumerated in Part III.U, Employee 201 files and the information contained therein.

3. **Classified**- These are information the access of which is highly restricted, and if disclosed may cause severe or serious harm or injury to the employee, student or third party.

   Examples: Employee and student CSU account or computer passwords (Data Privacy Law, Anti-Cyber Crime Law, CSU IT policies), bank account numbers, PIN numbers of employee and student ATM's.

K. "**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.

L. "**Personal Information Controller or PIC**" refers to the Universityas the entity which controls the processing of personal data, or instructs another to process personal data on its behalf.

M. "**Personal Information Processor or PIP**" refers to the University Official designated as such to whom the personal information controller instructs the processing of personal data pertaining to a data subject.

N. "**Privacy Impact Assessment**" refers to the process undertaken and used to evaluate and manage the impacts on privacy of University programs, projects, processes, measures, systems, or technology products. Such process takes into account the nature of the personal data to be protected, the personal data flow. The risks to privacy and security posed by the processing, current data best practices, cost of security implementation, and where applicable, the size of the organization, its resources and complexity of operations.

O. "**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.

P. "**Privacy Statement"** is a notification or statement, in the format specified under Part V Section 3.A of this Manual provided to an individual informing them of the use and purpose for collecting or processing the information, and/or which allows such individual to consent to such processing of information.

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

R. "**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;

S. "**Security Clearance**" is a document authorizing a CSU employeeto have access to sensitive personal information on CSU property or through online facilities.

T. "**Sensitive personal information**" refers to personal information about:

1. An individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.
2. Confidential and classified personal data as defined in Part III.J.2 and Part III.J.3.
3. 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.
4. 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
5. Specifically established by an executive order or an act of Congress to be kept classified.

U. "**University records**" refer to the records of students of all acts, events, accomplishments, results or research and all documents depicting the various activities of the students. These include but are not limited to the following:

1. Personal and academic records of the student
2. Birth Certificates

3. Academic reports
4. Medical Records
5. Guidance Records
6. Disciplinary records
7. Documents/ certificates for foreign students
8. Individual financial records

V. "**University personnel**" means all employees (regardless of the type of employment or contractual arrangement) of the University.

PART IV. SCOPE AND LIMITATIONS

This Manual applies to all units of the University, employees regardless of the employment status, students, officers and third parties whose information (applicants for admission or employment and former students or alumni whose university records are required) to be kept and secured by the University. The data covered by this Manual is limited to personal information as defined under Part III.K, collected and processed by the University.

This Manual is reviewed annually and updated regularly to comply with the current data privacy laws, policies and regulations.

PART V. COLLECTION OF PERSONAL INFORMATION

Section 1. Privacy Principles espoused by the University

A. TRANSPARENCY. Data Subject's consent should be obtained before collecting the information and the latter should be informed of the purpose for which the information is to be collected.

Example: In the enrolment process, upperclassmen are required to fill out the Student Data Sheet. The purpose of such collection of information is stated in the form and the consent of the student is obtained through the form which is filled out and signed by the student.

B. PROPORTIONALITY. Personal Information collected must be reasonably necessary or directly related to the University functions**.**

Example: In the application for admission as a student in CSU, only information such as name, address, contact numbers, previous Higher Education Institution (HEI), parent's or guardian's name, which are necessary for the evaluation of eligibility for admission to the University is collected.

C. FOR LEGITIMATE PURPOSE. In collecting personal information, the University shall use the information only for legitimate purposes as discussed in Part VI of this Manual.

Example: Personal information of students such as student's name, parents name and addresses and contact numbers shall be used only for purposes such as enrolment, academic activities and other student services which is allowed under the provisions of the Commission on Higher Education (CHED) and other related government agencies.

Section 2. Provisions for Specific Offices and personnel

A. Office of Admissions, University Registrar's Office, Internationalization, Guidance and Counselling, Alumni Office, Office of Student Internship Programand differentColleges of all CSU campuses

The Office of Admissions, the University Registrar's Office, Internationalization, Guidance and Counselling, Alumni Office, Office of Student Internship Programand different Colleges and units of the University collect personal information for the purpose of evaluating the eligibility of the applicant for admission or in case of current students, for enrolment in the University.

In the course of the collection of information, these authorized personnel from these offices request data subjects (students and their parents or guardians and to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and/ or enrolment processes). These offices collect, process the information and encode the same in the Student (profile) Data base. Only authorized personnel are allowed to encode and access student data.

Access is restricted pursuant to the provisions of this Manual which specifically provides that all student records should be kept confidential.

B. Human Resources Management Services

The Human Resource Office collects the information from employees or applicants for purposes of evaluating the applicant for eligibility for employment, and availment of employee benefits (i.e. retirement, educational and medical benefits) and collates the information in the individual 201 files of the employees.

Pursuant to existing laws and policies of the University, the 201 files or employee's individual employment records are confidential and access is restricted to authorized personnel only.

C. Health and Wellness Services Unit

The Health and Wellness Office collects sensitive information relating to the medical and dental health of faculty, administrative staff, officials, students.

Access to the data collected is restricted and limited only to authorized personnel in the office such as the university doctor, dentist or nurse assigned in the Office. Sensitive information may not be released without the prior consent of the data subject except incases life of the data subject (i.e. epidemic cases as provided under the DOH rules and regulations) is at stake.

D. Management Information Services (MIS)

The MIS is tasked to process, secure and store the information and data base systems of the University. All personal information collected from students

and other stakeholders by the different offices mentioned above are primarily encoded and stored in the Student Records Management System. Employee personal information collected by the HRMS is encoded and stored in the Human Resources Information System.

Access to the data is also restricted and given only to predetermined authorized personnel in relation to their specific function which requires them to access or process student oremployee information. In all instances, any access to personal information of students must be with their consent before it is endorsed by the Unit head concerned, and approved by the authorized CSU Official.

E. Office of the Campus Safety and Security Services

The Office of the Campus Safety and Security Services collects information of any disciplinary incident that any stakeholders might be involved in, including accompanying sanctions. The OCSSS will also acquire other forms of data (pictures, videos of activities, etc.) via official documentation of such activities through recordings from closed-circuit security television (CCTV)

The OCSSS collects information from vehicle owners as applicants for the issuance of a gate pass. The data used to evaluate the applicants' eligibility for entering the university premise. The gate pass then serves as a ticket for vehicle owners entering the school grounds. The collected information such as personal information, photocopy of the Driver's License, Government ID, and OR/CR of the vehicle, which all contain confidential information, are treated with high confidentiality, and access is restricted to OCSSS personnel only.

F. Other Offices and all CSU Faculty and Staff

All other offices of CSU campuseswho collect, process or store student or employee personal information, if any, are subject to the policies provided under this Manual. Unit heads are responsible for ensuring compliance of the provisions of this Manual within their offices.

Section 3. Privacy Policies

To ensure that the rights of the data subjects are protected, the above-mentioned offices are subject to the following policies:

A. Data Subjects are notified and their consent secured

Collection of information is done with the consent of Data Subjects (Students and their guardians (if students are minor) which consent is included in the forms filled-out during application for admission, enrolment or availment of student services such as scholarships, on the job trainings, and the like.

Forms for collection of personal information include a provision or a variation of these privacy statements:

“All information shall be used by the University for legitimate purposes specifically for and shall be processed by authorized personnel in accordance with the Data Privacy Policies of the University.”

"I hereby allow/authorize CSU to use, collect and process the information for legitimate purposes specifically for, and allow authorized personnel to process the information."

In case, there is no form or written document containing the privacy statement, the authorized personnel tasked to collect the information may verbally notify them of the purpose and ask the Data Subject to allow the University personnel to collect and process the information and shall record the processing of information with consent in writing.

B. Access only to Authorized Personnel

Only authorized personnel are allowed to access and process the personal information collected from the employees, students, their parents or guardians and alumni in accordance with Data Privacy policies of the University.

Example: Only the registrar or her duly authorized representative or personnel is allowed complete access to the student profile which includes the name, student number, parents names, addresses, contact numbers, grades etc.

C. Information is reasonably necessary and directly related to Universityfunctions or purposes

Authorized university personnel shall collect personal information which is reasonably necessary or directly related to the University's primary or secondary functions or activities. Personal Information shall not be collected in anticipation that it may be useful in the future ("just in case" it is needed). The physical records or those which are not digitally stored and secured in CSU data base are stored in the particular offices of the each Office. For student records from previous years which are required to perpetually stored and maintained by the University, or a warehouse in a secured location is maintained by a third party tasked to physically store and secure the records. Access is restricted where such records may only be retrieved upon specific instructions of the University Registrar and only for legitimate purposes or upon request of the student or alumni for copies of their individual university record or pursuant to the University Registrar's procedures and policies on request for records.

Personal information shall be collected by lawful and fair means, which is allowed under the University's policies.

Example: For foreign students, nationality, passport numbers and the contact numbers of the parents or guardians are necessary in case of emergencies and other situations where the student's parents or embassy are required to be notified.

PART VI. USE AND DISCLOSURE OF INFORMATION

Authorized university personnel are allowed to access, use and process said information for legitimate primary or secondary purposes of the University and/or that which is stated in the privacy statement contained in the forms or documents signed by the students or third parties or employees.

Section 1. Primary Purpose

As an educational institution, personal information is collected primarily for the educational purposes of the students and employment purposes. This also includes information collected for purposes set out in the privacy statements contained in the documents signed by students or employees. Such information is allowed to be processed and used by authorized personnel for such purposes.

Section 2. Secondary Purposes

Secondary purposes are those which are collateral to the primary purposes and which are necessary to process the information. This includes monitoring the current administrative or disciplinary standing (for student and employee discipline), financial condition (for scholarship purposes) or the health and psychological wellness of students and employees (health purposes). Authorized university personnel are allowed to use personal information collected and/or processed for such purposes provided the following circumstances are present:

A. the student or employee or alumni has consented to the use or disclosure for the secondary purpose; or

B. the student or employee or alumni would reasonably expect the University through its authorized personnel to use, or process personal information for secondary purpose and that the secondary purposes are directly related to the primary purposes; or

Section 3. Sensitive Personal Information

Sensitive personal information may not be disclosed or processed, except in any of the following cases:

A. Consent is given by data subject, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose of the University.

B. The processing of the sensitive personal information provided for by existing laws and regulations, such as medical history to be disclosed by the student as part of the monitoring of the health of the student, 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 to achieve the lawful and non-commercial objectives of public organizations and their associations provided that the processing is confined and related to the bona fide members of these organizations or their associations; the sensitive personal information are

not transferred to third parties; and consent of the data subject was obtained prior to processing.

E. 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.

F. The processing concerns sensitive personal information or privileged information 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.

Section 4. Government-Related Use and Disclosures

Personal information is allowed to be used and disclosed to government agencies to satisfy reportorial requirements in line with their constitutionally or legislatively mandated functions pursuant to existing laws or when the use of pursuant to lawful order of a court or tribunal.

Section 5. Requirements Relating to Access by CSU Personnel to Sensitive Personal Information

A. On-site and Online Access

No CSU employee shall have access to sensitive personal information on property or through online facilities unless he or she has received a security clearance from the CSU President. An CSU employee shall only be granted a security clearance when the performance of his or her official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

B. Off-Site Access

Sensitive personal information maintained by CSU may be transported or accessed from a location off or outside of CSU property. A request for such transportation or access shall be submitted to and approved by the CSU President. The request must include proper accountability mechanisms in the processing of data.

The CSU President shall approve requests for off-site access in accordance with the following guidelines:

1. Deadline for Approval or Disapproval. The CSU President shall approve or disapprove the request within two (2) business days after the date of submission of the request. Where no action is taken by the head of agency, the request is considered disapproved;

2. Where a request is approved, the President shall limit the access to not more than one thousand (1,000) records at a time.

3. Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard.

PART VII. ACCURACY OF INFORMATION

Section 1. Verification of information

Authorized university personnel must take reasonable steps to ensure that the personal information collected or processed, up-to-date, complete, relevant and not misleading.

The information collected from students and employees is verified by the particular offices collecting the information. Student information is verified by the UniversityRegistrar's Office while the HRMS conducts the verification of employee information and background checks.

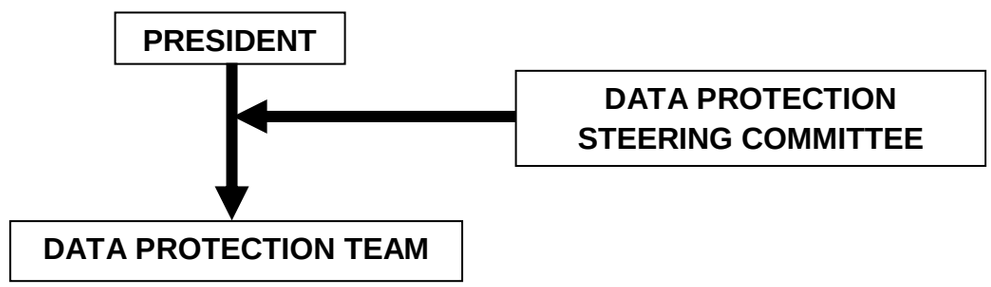
Section 2. Correction, or update of information

Students may update their personal information through forms available from the University Registrar's Office, while for employees they may write to or directly go to the HRMS Office to update their information**.** In case of erroneous or false information, the students or employees may have the information corrected, rectified, blocked or erased (blocking and erasure only to the extent allowed by CHED and other applicable laws) using the same process.

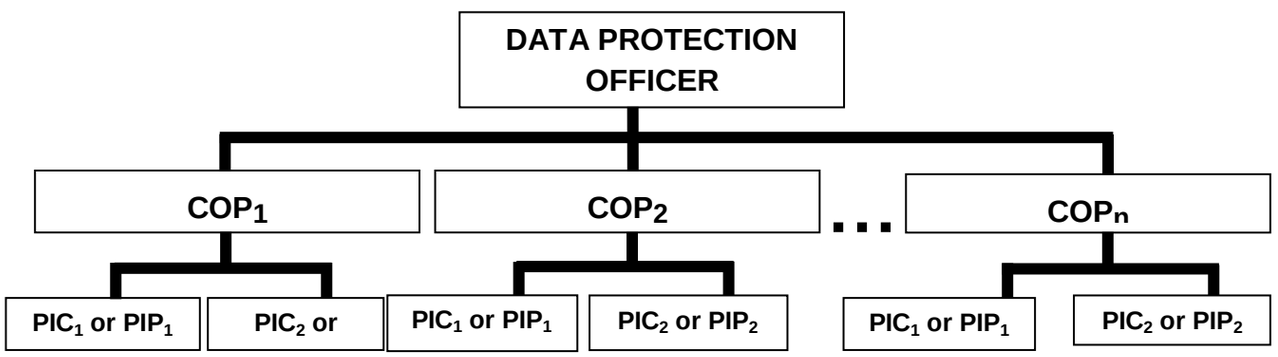
PART VIII. SECURITY OF PERSONAL INFORMATION

Section 1. Security Measures

A. Data Privacy Organizational Structure



DATA PROTECTION TEAM



B. Duties and Responsiblities of the Data Privacy Officials

1. **President:** shall be responsible for complying with the data security requirements as stipulated in the DPA;

2. **Data Protection Steering Committee** shall ensure the compliance of the data privacy act and security requirements.It shall review and recommend to the CSU President policies governing the administration, management and development planning of the data privacy requirements. It is composed of a Chairperson, Vice Chairperson and at least two (2) members (at least one (1) personnel from each campus of the University) and Secretariat. The Chairperson should be a Vice President – designate of the University. The Vice Chairperson should be at least a third (3rd) level Employee of CSU and is not a PIC.

   Chairperson: He/She shall be the presiding officer of the presidingofficer of the committee. In his/ her absence, the Vice Chairperson shall preside over the meetings.

   Vice Chairperson: He/she shall take over the duties and responsibilities of the Chairperson in the event of the later's absence and do other functions as directed by the chairperson.

   Secretariat: The DPT shall serve as the Secretary of the committee. It shall be his/her duty to issue notices for meetings of the committee, to keep the minutes of its proceedings, and to send copy of such minutes to each member of the committee. He or she shall also forward to each member of the committee a copy of the order of business of every regular meeting at least three days in advance.

3. **Data Protection Team:** is composed of the Data Protection Officer (DPO), Compliance Officer for Privacy (COP) and Personal Information Controllers PIC).

4. **Data Protection Officer:**

   a) Monitor the Personal Information Controllers (PIC's) or Personal Information Processors (PIP's) compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. The DPO may:

      (1) Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;

      (2) Analyse and check the compliance by third-party service providers;

      (3) Inform, advise and issue recommendations to the PIC and PIP;

      (4) Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personnel data processing; and

      (5) Advice PIP or PIC as regards the necessity of executing a Data Sharing Agreement with the third parties, and ensure its compliance with the law;

b) ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

c) advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification, or deletion of personal data);

d) ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

e) inform and cultivate awareness on privacy and data protection within your organization, including all relevant laws, rules, and regulations and issuances of the NPC;

f) advocate for the development, review, and/or revision of policies, guidelines, projects, and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;

g) serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning date privacy or security issues or concerns and the PIC or PIP;

h) cooperate, coordinate, and seek advice of the NPC regarding matters concerning date privacy and security; and

i) 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.

5. Compliance Officers for Privacy (COPs): Except for items (1) to (3), COPs shall perform all other functions of a DPO. Where appropriate, he or she shall also assist the supervising DPO in the performance of the latter's functions (NPC advisory 2017-01).

6. Personal Information Controller:

a) shall be accountable for complying with the requirements of the Act, these Rules, and other issuances of the NPCand 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;

b) shall designate an individual or individuals who are accountable for the organization's compliance with the DPA. The identity of the individual or individuals so designated shall be made known to a data subject upon request;

c) shall be responsible for any personal data under its control or custody, including information 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.

C. Institutional Data Privacy Manual

The University data privacy policies are contained in the institutional Data Privacy Manual which is reviewed annually and regularly updated.

D. Conduct of Awareness Campaign and Data Privacy Trainings

The University regularly attends and conducts awareness campaigns and data privacy trainings, seminars and conferences as part of its commitment to ensure that all its students and employees comply with its data privacy policies.

E. Conduct of Privacy Impact Assessments

Privacy Impact Assessment (PIA) is conducted to ensure that the potential privacy impact of the University's processes, information system programs and other initiatives which process personal information of students, employees and third parties are evaluated as detailed in Part XI.

F. Information System

The University shall take reasonable steps to protect the personal information in its possession from misuse, loss or unauthorized access, modification or disclosure.

As most of the personal information of students and employees are stored in the University data bases, access to personal information in digital or digitized form by authorized CSU personnel is restricted and individually identifiable. An approval process is in place for internal requests (i.e. special requests for authority to view student profile for disciplinary cases, counselling, or health concerns) for access to restricted student or employee records contained in the University information systems. As a general rule, only authorized personnel may request for access of the information systems of personal information in accordance with the procedure established by MIS, and [VIII (B)] of thisManual.

Physical access to the servers and network equipment is highly restricted to authorized personnel only. Various security appliances and devices are employed to safeguard the university network and its systems. Twenty-four (24)-hour security is also provided by the University to secure the areas where the University data centers are located.

G. Digital Data Security Measures in the University

The university offers different services to its employees and students. One of these services includes access to various Information Systems (IS) applications, both desktop, and online applications. Come along with this access grants are the following data security measures:

1. Establish passwords. The University use of a Lightweight Directory Access Protocol (LDAP) application to authenticate user credentials during logins. The application manages user accounts and stores passwords with SHA1 encryption.

2. Set up firewall. The firewall will use of a high-performance web proxy cache as its URL filter. It should have the capability of acting as HTTP/HTTPS reverse proxy and includes an Exchange-Web-Access (OWA) Assistant, SSL filtering, and antivirus integration via C-ICAP.

3. Antivirus protection. The antivirus works at the server level. On the other hand, each end-user desktop has also an antivirus application.

4. Updating of patches. Regular updates of patches are performed. There are some applications where updates would only take place after verifying the compatibility of the IS applications running with it like on operating systems.

5. Wireless Connectivity. When using the WiFi, the users are obliged to key-in their login credentials through the Captive Portal to gain network access using their computers or gadgets. The LDAP application then authenticates the captured credentials.

6. Schedule backups. The database, server configuration, and application source codes have different schedules for backups. The server configuration backup is performed every month or whenever an update will take place. The database backup is executed with the use of a bash script and store it to another server – the backup server. It has daily incremental, weekly full, and monthly full backups. The application source code has monthly backups for the whole desktop applications and for online services. Whenever there are updates on the application module, versioning, and backup of the previous change are kept.

7. Multiple-factor Security. The University will use at least two-factor security procedure consisting of an archive format compression, password and other protection technique to ensure the security, integrity and confidentiality of the data or information.

8. Monitor steadily. Each MIS personnel is designated to monitor their respective areas of responsibility. Say the Network Administrator, together with its Technical Support personnel, is tasked to monitor network activities and concerns. Each of the identified areas, such as network, database, website, and portals, etc. were monitored daily.

9. Securing emails. The university has its official email for all its employees and students. The email service should have security features like advanced phishing and malware protection, confidential mode, review suspicious activity, and more.

10. Technology transfer. The MIS personnel continuously conducts technology transfer to end-user on the security of data and files. This is done through an in-person, phone call, chat/messenger, and email.

H. Physical Arrangement/Facilities

Access to student, employee and alumni personal information is limited to authorized personnel of the specific offices collecting or processing the information.

Aside from access restriction, the storage facilities for the hard copies of documents containing personal information are also secured (i.e locked) in cabinets or storage facilities. Only authorized personnel can open or have access to keys to the storage facilities. The storage units or facilities are placed in areas which are not usually accessible to the public, safe from physical hazards such as rain, wind and dust, and located in areas which are usually manned by the authorized personnel.

Round the clock security is also provided for the entire University including areas where the hard copies of such documents are kept and secured.

Section 2. Request for Access

As a general rule, only authorized personnel shall have access to student or employee or alumni personal information. Students or parents or guardians (in case of minors) who wish to have access to their own personal information may submit a written request directly to the Registrar's Office andmay be allowed access to their specific individual information or given copies, pursuant to thepolicies and guidelines on requesting for access or copies of student records. Request for information through telephone is not allowed. In case of email inquiry, proof of actual parent (if students are minors) or student identity shall be submitted along with the email request.

Employees who wish to view the personal information in their individual personnel file, may file a written request or directly go to the HRMS Office, and request for viewing of such information in the presence of an authorized personnel of the office.

As a general rule only authorized personnel may be allowed to have access to the personal information subject to the procedure established in this section. In such cases where any individual or entity [other than the student, parent or guardian in case of minors, or employee] wishes to have access pursuant to the instances or exceptions provided under Data Privacy Act or [VI] of this Manual, a written request shall be submitted to the Unit Head who may either endorse or reject the same. If approved, the endorsed request shall be submitted to the DPO or her duly authorized representative for approval. If the request involves digital or digitized data, then the approval of the MIS Director is required prior to endorsement of the Unit Head to the DPO. Only written requests properly endorsed by the Unit Head shall be considered for approval.

The written request shall state the name of the requestor, the purpose, the type of access requested (i.e. copying or viewing only), and the time frame or time limit within which access shall be given with a guarantee that the information shall be used solely for purposes allowed by law and a statement that such shall be treated with utmost confidentiality.

In cases where government agencies empowered under the law to request for personal information (i.e. BIR, DOH), request for access, university personnel must ensure that the request is in writing, citing the authority upon which the request is made. In cases where the request is a result of a valid order or decision of a tribunal or court, a copy of such order shall be attached to the written request.

Once approved by the DPO, it shall be transmitted to the Unit Head or appropriate Office for implementation.

The Unit Head who endorsed the same shall be responsible for monitoring compliance of the requestor on the terms of the approved request (i.e time limit and confidentiality).

In case there is doubt on the propriety of any request for access, university personnel should consult or seek clearance from the Legal Affairs Office or the DPO.

Section 3. Retention and Destruction of Personal Information

Under the provisions existing laws, the University is required to permanently keep the student and employee records including the information contained therein. In line with this, no personal information may be destroyed unless allowed by such laws, and such destruction, if allowed or authorized by law, must be documented in writing by the University. Unauthorized destruction should be reported to the DPO or any member of the DPT pursuant to the procedure stated in the succeeding section.

PART IX. Inquiry, Complaints and Breach Notification

Section 1. Inquiry on Data Privacy issues

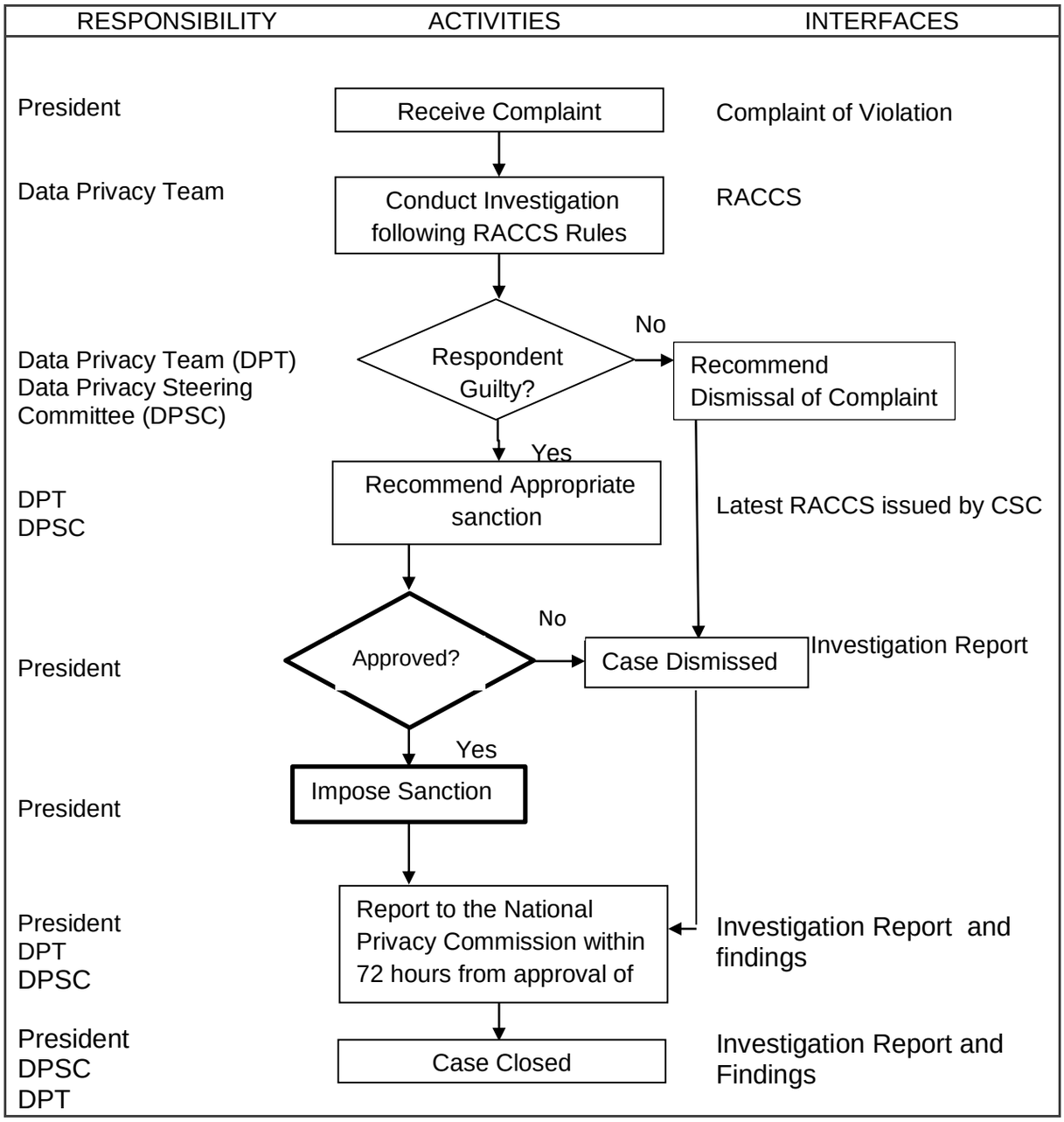
Data subjects may inquire or request for information from the Data Protection Team (DPT), regarding any matter relating to the processing of their personal data under the custody of CSU, including the data privacy and security policies implemented to ensure the protection of their personal data.

Section 2. Procedure for Complaints and Breach Notification

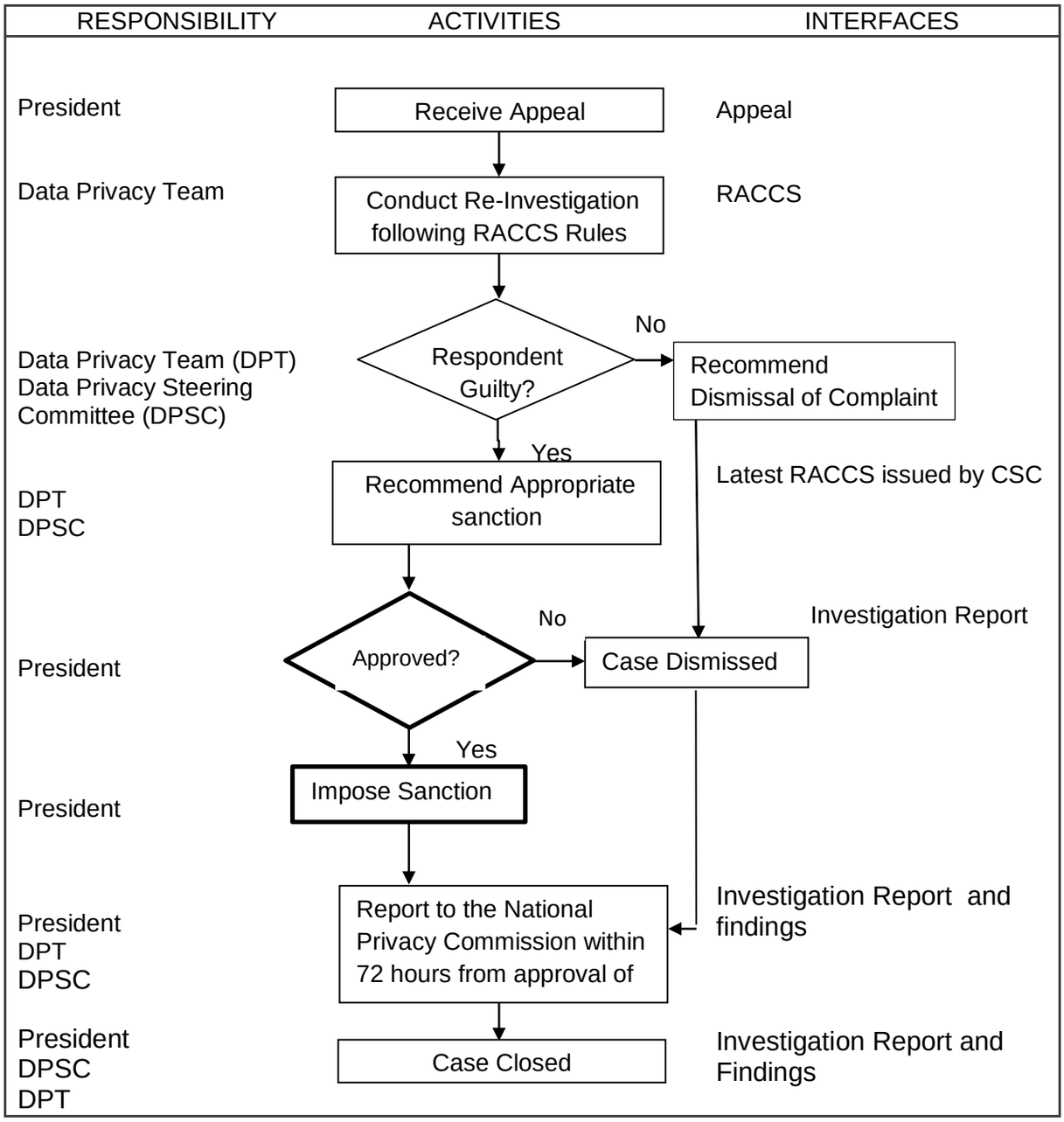
Any suspected or actual breach of the CSU Data privacy policy, violation of data privacy rights, or any breach, loss or unauthorized access or disclosure of personal information in the possession or under the custody of the University must be reported immediately to the CSU President or Data Protection Team by filing a complaint following latest RRACS rules issued by the Civil Service Commission. The DPO shall convene the entire team in case of a complaint, or motu-propioin case the violation of policies or data breach, loss, unauthorized access or destruction as an investigation committee to recommend actions, particularly when the violation is serious or causes or has the potential to cause material damage to the University or any of its students or employees. The DPT shall report the case to the DPST for appropriate action. Such recommendation of the DPST shall be submitted to the President of the University for Approval. Any appeal on such approved recommendation/Decision shall be made by any of the affected parties within 15 days from receipt of the approved Decision.

In case of a complaint for violation of the CSU Data Privacy Policies as contained in the provisions of this Manual, or any serious breach, loss or unauthorized access, disclosure or destruction of personal information in the possession or under the custody of the University and within reasonable time, or in cases of serious security breach as provided under Republic Act No. 10173 or the Data Privacy Act of 2012 and its Implementing Rules and Regulations Act, the University shall report the same to the National Privacy Commission within seventy-two (72) hours from knowledge thereof.

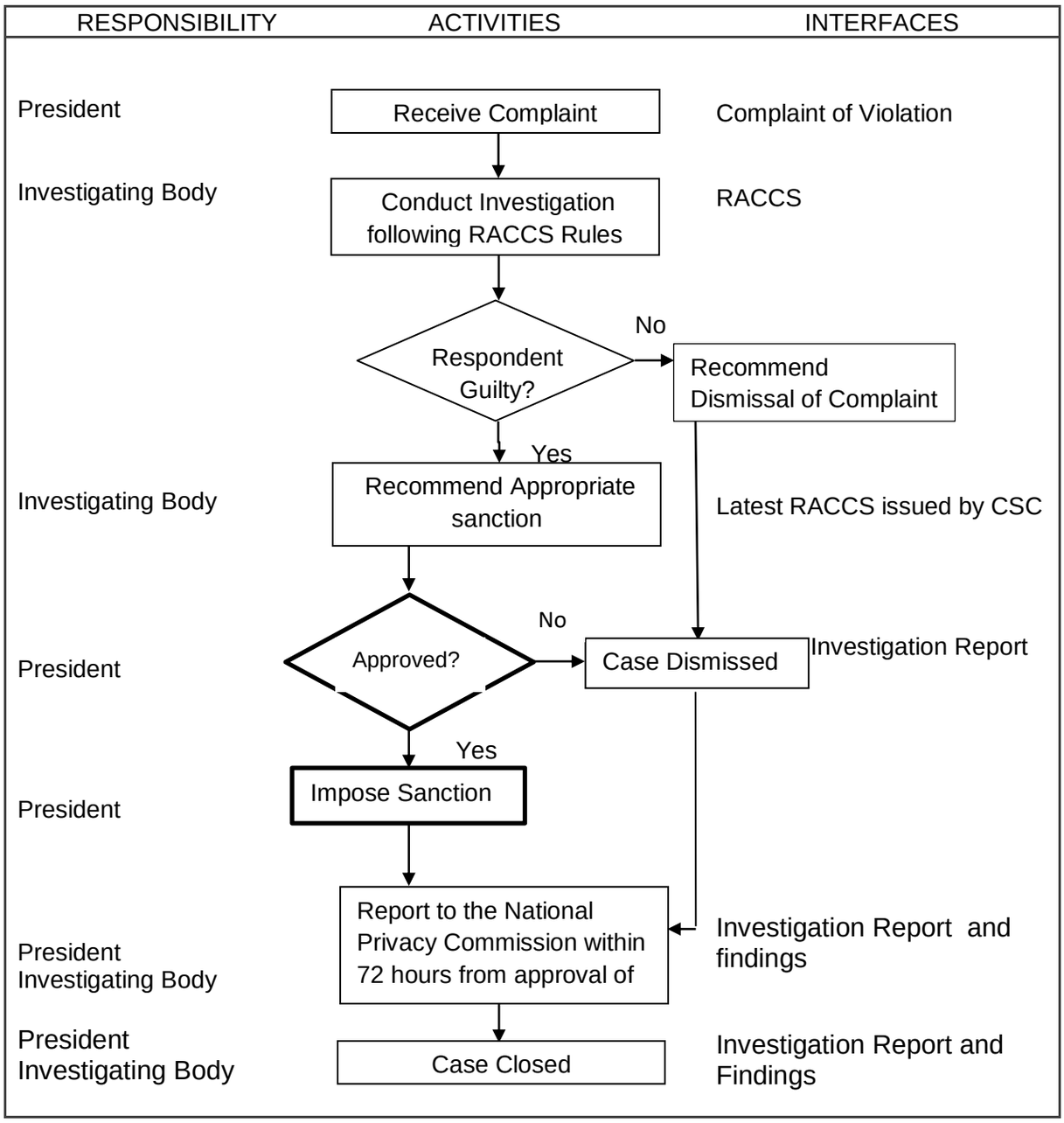
PROCESS FLOW



If Respondent file an Appeal:



In case the Respondent is a member of DP Steeting Committee or DP Team



A. Breach Report

The PIC shall notify the President through the DPT by submitting a report, whether written or electronic, containing the required contents of notification. The report shall also include the name of a designated representative of the PIC, and his/her contact details.

All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the PIC. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. A general summary of the reports shall be submitted to the NPC annually by CSU.

B. Breach Notification

This Manual adopts the breach notification of the DPA and its IRR.

The CSU and affected data subjects shall be notified by the personal information controller within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that, a personal data breach requiring notification has occurred.

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 personal information controller and CSU also believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Depending on the nature of the incident, or if there is delay or failure to notify, the CSU may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

Content of Breach 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 personal information controller, 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.

PART X. PENALTIES

Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the DPA and its IRR, and other issuances of the NPC, shall be liable for such violation, and shall be subject to its corresponding sanction, penalty, or fine, without prejudice to any civil or criminal liability, as may be applicable as provided in Rule XIII, Section 52 of RA 10173.

Moreover, CSU may conduct administrative actions based on latest Rules on Administrative Cases adopted and promulgated by the Civil Service Commission, independent of the above sanction or even in the absence thereof. Any violation to the DPA is considered as Grave Misconduct.

PART XI. PRIVACY IMPACT ASSESSMENTS

To ensure that the potential privacy impact of the University's processes, information system programs and other initiatives which process personal information of students, employees and third parties are evaluated, privacy impact assessments are conducted for such projects, programs and initiatives.

A. Conduct of Impact Assessment

To assess the potential privacy impact of the University's processes, information system programs and other initiatives which process personal information of students, employees or third parties in consultation with the University stakeholders, privacy impact assessments shall be conducted prior to implementation to identify and minimize potential privacy risks.

The privacy impact assessment shall include but not limited to the following:

1. systematic description of the process, nature, scope, context and the purposes of the processing, including, where applicable, the legitimate interest pursued by University;

2. assessment of the necessity, proportionality of the processing operations in relation to the purposes and compliance measures;

3. identification and assessment of the risks to the rights and freedoms of data subjects;

4. identification and additional measures to be placed to address and mitigate the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with DPA, its IRR and the University Data Privacy policies into account the rights and legitimate interests of data subjects and other persons concerned.

Privacy impact assessments conducted for CSU processes or projects shall be evaluated by the Data Protection Team and shall be submitted to the Data Privacy Steering Committee for recommendation to the University President for approval.

B. Privacy Impact Assessment Team

The Privacy Impact Assessment Team will be composed of a Team Leader and at least two (2) members. Their duties and responsibilities are as follows:

Team Leader:

1. Develop the privacy impact assessment (PIA) proposal.
2. Conduct the approved PIA proposal.
3. Monitor and Evaluate the conduct of PIA.
4. Present and publish the results of the PIA.
5. Submit the PIA final report or manuscript to the DPO for evaluation.

Members:

1. Assist the team leader in developing the PIA proposal, and conduct of the said approved proposal.
2. Assist in the monitoring and evaluation the PIA.
3. Write the manuscript of the PIA.
4. Do other functions as directed by the team leader.

PART XII. EFFECTIVITY

The provisions of this revised Manual shall take effect on _____.

Prepared by: LUISITO I. TABADA