



# Benguet State University

La Trinidad, Benguet



# DATA PRIVACY POLICY

(DPA, CHAPTER V; DPA-IRR, RULES VI & VII)

**Approved by  
the Board of Regents**  
*Under BOR Res. No. 156a, s. 2020*

Document Code	DPO-DPP-001
Circularized under	Administrative Order No. 008, s. 2020
Responsible Office	Office of the University President
Responsible Office	Data Protection Officer
Revision History	Original
Effectivity	October 2020
Next Review	September 2021
Control No.	Website

## I. PRELIMINARIES

A. **AUTHORITY.** Republic Act No. 10173,<sup>1</sup> Executive Order No. 2, s. 2016.<sup>2</sup> NPC Circular 16-01<sup>3</sup> and NPC Advisory No. 2017-01, 14 March 2017;<sup>4</sup>

### B. OVERVIEW

1. **THE LAWS INVOLVED.** Our Constitution expresses the policy that *“the State shall adopt and implement a policy of full disclosure of all its transactions involving public interest, subject to reasonable conditions prescribed by law.”*<sup>5</sup> Additionally, it recognizes *“the right of the people to information on matters of public concern.”*<sup>6</sup> However, the same Constitution postulates that *“the State values the dignity of every human person and guarantees full respect for human rights”*<sup>7</sup> and that the State also *“guarantees the right of the people to be secure in their persons, houses and effects against unreasonable searches and seizures.”*<sup>8</sup> The gist is that though the right to information on matters of public concern is a fundamental right it finds a counter balance in a person’s equally recognized fundamental right to privacy.

A legislation that permits the limited disclosure of public documents is Republic Act No. 67139 and its Implementing Rules and Regulations (IRR). It stipulates that all public documents must be made accessible to the public during office hours,<sup>10</sup> except for certain types of official information, records or documents.<sup>11</sup>

The more recent Data Privacy Act of 2012 upholds the State's twin policies of protecting the right to privacy while ensuring the free flow of information for innovation and growth.<sup>12</sup> This law, passed in June 6, 2012, seeks to implement the constitutional provisions on protecting all forms of information, be it private, personal, or sensitive. It sets certain parameters under which personal data may be processed (e.g., disclosed) in a manner that conforms to data privacy principles. Consistent with the constitutional provisions, it excludes from its scope information that fall within matters of public concern. This law ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual’s data privacy rights.

The latest on this subject is Malacañang’s 2016 Executive Order No. 2, providing that there shall be a legal presumption in favor of access to information, public records and official records and that no request for information shall be denied. It qualifies, though, that such disclosure must clearly fall under any of the exceptions enshrined in the Constitution, existing law or jurisprudence or those listed in the inventory annexed to the E.O or its updated version.<sup>13</sup>

---

<sup>1</sup> Data Privacy Act of 2012

<sup>2</sup> Operationalizing in the Executive Branch the People’s Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefore.

<sup>3</sup> Security of Personal Data in Government Agencies, 10 October 2016

<sup>4</sup> Designation of Data Protection Officers

<sup>5</sup> 1987 Philippine Constitution, Article II, Section 28

<sup>6</sup> *Id.* Article III, Section 7

<sup>7</sup> *Id.* Article II, Section 11

<sup>8</sup> *Id.* Article III, Section 2

<sup>9</sup> Code of Conduct and Ethical Standards for Public Officials and Employees; 20 February 1989

<sup>10</sup> *Id.* Rule VI

<sup>11</sup> IRR, R.A 6813

<sup>12</sup> Data Privacy Act of 2012, Sec. 2.

<sup>13</sup> Annex A: Inventory of Exceptions Annexed to EO No. 2

E.O No. 2 clarifies that *“while providing access to information, public records, and official records, responsible officials shall afford full protection to the right to privacy of the individual.”* For this purpose, it requires that each government office shall ensure that personal data in its custody or control is disclosed or released only if it is material or relevant to the subject-matter of the request and its disclosure is permissible under the DPA, EO or existing law, rules or regulations, among others.<sup>14</sup>

## 2. BSU A PERSONAL INFORMATION CONTROLLER.

Benguet State University, by definition of the DPA, is a Personal Information Controller (PIC) in that through its various data processing units it controls the processing of personal data whether these be personal information, sensitive personal information, or privileged information; or instructs another (called the Privacy Information Processor) to process personal data on its behalf. These are obtained from their respective clientele (Data Subjects) in relation to the discharge of their legitimate office mandates and functions, and other professional services accessed by such data subjects. These are controlled and retained by said offices in various types and forms.

As a PIC, BSU is obligated to implement reasonable and appropriate measures to protect personal data in its information and communications systems against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

From the preceding discussions we comprehend that the processing of personal data, including its use and disclosure, retention, and destruction are regulated. We also understand that the determination of the applicability of any of the exceptions on the disclosure of personal data shall be the responsibility of the head of the office that is in custody or control of the information, public record or official record.<sup>15</sup>

### C. STATEMENT OF PRINCIPLE

BSU respects and values data privacy rights, and makes sure that all personal data are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality. As a consequence, it is imperative that guidelines be provided governing our handling practices of personal data and against which they would be assessed to avoid violations of data privacy laws, rules and regulations.

### D. STATEMENT OF PURPOSE

This Data Privacy Policy is adopted for a two-fold purpose: 1) to inform university personnel of BSU's data protection and security measures, and 2) to guide and assist all University units engaged in the processing of personal data to meet their obligations under the Data Privacy Law, its Implementing Rules and Regulations, related issuances by the National Data Privacy Commission, and Executive Order No. 2, s. 2016, in the implementation thereof.

This Policy encapsulates the privacy and data protection protocols that need to be observed and carried out within the University for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of all data subjects without sacrificing data quality. As may be necessary, definite guidelines shall be issued for specific offices with unique personal data handling processes.

---

<sup>14</sup> E.O 2, Sec. 7

<sup>15</sup> *Loc. cit.*

**It must be stressed that the laws impose obligations on those persons engaged in the processing of personal data, and prescribes stiff penalties for specific offenses.<sup>16</sup>**

#### E. SCOPE AND LIMITATIONS

This Data Privacy Policy is essentially an internal issuance and is meant for the use and application of university personnel in all Campuses of the University. All BSU personnel, regardless of the type of employment or contractual arrangement must comply with the terms set out in this Privacy Policy. The public shall be guided by the University's Privacy Notice, which is a separate privacy document.

The burden of proving that this Policy is not applicable to a particular information falls on those involved in the processing of personal data or the party claiming the non-applicability. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

#### F. DEFINITION OF TERMS<sup>17</sup>

1. **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;
2. **Sensitive Personal Information** – refers to personal information about an individual's race, ethnic origin, marital status, age, color, religious/philosophical/political affiliations, health, education genetic or sexual life, legal proceedings, government issued identifiers and other information specifically established by an executive order or an act of congress to be kept classified.
3. **Privileged Information** – “any and all forms of information which, under the Rules of Court and other pertinent laws, constitute privileged communication, such as, but not limited to, information which a person authorized to practice medicine, surgery or obstetrics may have acquired in attending to a patient in a professional capacity.”
4. **Data Subject** - refers to an individual whose personal, sensitive personal, or privileged information is processed;
5. **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 personal information about and/or relating to him or her. It shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
6. **Personal Information Controller (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. 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.
7. **Personal Information Processor (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

---

<sup>16</sup> See R.A No. 10173 (DPA of 2012), Chapter VIII; DPA-IRR, Rule XIII

<sup>17</sup> *Id.* Chapter I, Sec. 3; IRR-Rule I, Sec. 3

8. **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.
9. **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 or 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.
10. **Filing system** - refers to any act 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 that 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 person is readily accessible.
11. **Data sharing** - refers to the disclosure or transfer to a third party of personal data under the custody or control of BSU. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information processor to a personal information controller.<sup>18</sup>
12. **Data Sharing Agreements** – any written contract or agreement entered into by BSU and a third party containing the terms and conditions of the sharing of personal data.
13. **Data 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.
14. **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.
15. **Privacy Notice** – a statement informing a data subject of how BSU processes personal data from collection to destruction.
16. **Security Measures** – refers to the organizational, physical, and technical measures employed to protect personal data from both natural and human dangers.
17. **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
18. **Data Center** – refers to a designated centralized repository which may be physical or virtual, may be analog or digital, used for the storage, management, and dissemination of data.<sup>19</sup>
19. **Public document** – are: (a) the written official acts, or records of the official acts of the sovereign authority, official bodies and tribunals, and public officers, whether of the Philippines, or of a foreign country; (b) documents acknowledged before a notary public,

---

<sup>18</sup> DPA-IRR, Rule I, Sec. 3.f

<sup>19</sup> NPC Circular 16-01 (10 October 2016), Rule I, Sec. 3.E and Rule II, Sec. 7



except last wills and testaments; and (c) public records, kept in the Philippines, of private documents required by law to be entered therein.<sup>20</sup>

20. **Data Protection Officer** – refers to the duly designated officer/s accountable for the university’s compliance with the DPA, its IRR, issuances by the NPC, any other government-issued privacy rule or regulation, as well as the implementation of this Privacy Manual.<sup>21</sup>
21. **Compliance Officer for Privacy** - is an individual or individuals who perform some of the functions of a DPO.<sup>22</sup>
22. **Data Breach Response Team** – is a designated team responsible for ensuring immediate action in the event of a security incident or personal data breach.<sup>23</sup>
23. **Head of Office (HO)** – shall refer to the personnel who has direct supervision and control over an office and its staff either by reason of position or designation.<sup>24</sup>

## II. PROCESSING OF PERSONAL DATA

- A. **DATA PRIVACY PRINCIPLES.**<sup>25</sup> Processing of personal data shall be subject to compliance with the requirements of the Data Privacy Law and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.
  1. **Transparency.** Data subjects or clients must be aware of the nature, purpose, and extent of the processing of their personal data, including the risks and safeguards involved, their rights as a data subject,<sup>26</sup> and how these can be exercised. Any information and communication provided a data subject must always be in clear and plain language to ensure that they are easy to access and understand.
  2. **Legitimate purpose.** The processing of information shall be limited to the declared, specified, and legitimate purpose which must not be contrary to law, morals, or public policy. It should be determined before collection and made known before, or as soon as reasonably practicable after collection. Data subjects must be provided specific information on the purpose and extent of the processing of their personal data. (*i.e. automated processing for profiling, research, reference, or data sharing, etc.*).
  3. **Proportionality.** Process only the data identified as needed to perform your job responsibilities and in your approved records retention schedule. Only personal data that is necessary, relevant, suitable and compatible with such declared, specified, and legitimate purpose of your office shall be collected. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

### B. GENERAL GUIDELINES

1. **COLLECTION.** For each collection of personal data, it must be ensured that the data processor has legal authority to do so and that the collection must be for a declared, specified legitimate purpose; that data is processed fairly and lawfully, and that processing should ensure data quality.

---

<sup>20</sup> Rules of Court, Rule 132, Sec. 19

<sup>21</sup> DPA, Sec. 21(b), IRR, Sec. 50(b), NPC Cir. 2016-01, Sec. 4

<sup>22</sup> NPC Adv. Opinion 2017-01, 14 March 2017 (Designating DPOs)

<sup>23</sup> NPC Cir. 16-03

<sup>24</sup> Our definition

<sup>25</sup> DPA-IRR, Rule IV, Sec. 17,

<sup>26</sup> See Part VII.A below

- a. **Identify the type of personal data** that will be processed. Collect only the data for which you are authorized and that is necessary, adequate, relevant, and compatible with your declared, specified legitimate purpose and the discharge of the functions of your office.<sup>27</sup> Do not consider data for future reference or possible later use.
  - b. **Collect data directly from your data subject.** Consent is required prior to the processing of personal data, subject to exemptions provided by the DPA and other applicable laws and regulations. A *"Data Privacy Consent Form"*<sup>28</sup> should first be accomplished by a data subject before any processing of personal data. This shall form part of the office documentation. The collection of personal data from third parties or external sources must be specifically authorized by some law or rule.
  - c. **Provide specific information** to the data subject in clear and plain language regarding the purpose and extent of processing including, where applicable, the automated processing of his/her personal data for profiling or data sharing.
  - d. **Personal data processing for research purposes** is allowed when the personal data is publicly available, or has the consent of the data subject. *Provided*, that the research is intended for a public benefit and that it be subject to the requirements of applicable laws, regulations, or ethical standards.<sup>29</sup> *Provided further*, that the researcher comply with any code of ethics or any rules and regulations on research issued and implemented by institutions involved in research. *Provided, finally*, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.
  - e. **Uphold the rights of your data subject**,<sup>30</sup> including the right to correct, refuse, withdraw consent, or object. Should your data subject refuse consent, explain fully the consequences. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.
2. **ACCURACY AND CORRECTION.** Take reasonable steps to ensure that processed personal data is accurate, complete and kept up-to-date before use or disclosure.
    - a. **Establish measures** to ensure that collected personal data is accurate, complete and up to date. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted. Define a documented process for the correction of personal data under your care and identify staff responsible for these or otherwise keeping them up-to-date.
    - b. **Access and correction rights** by data subjects should form part of these measures.
  3. **USE AND ACCESS.** Use personal data only for the purpose/s for which it is collected. If it is to be used later for a purpose not indicated in A.2, consent of the data subject must first be secured. Further processing beyond the original purpose should have adequate safeguards.
    - a. **Establish procedural, technical and physical measures (Access Control Policy)** to ensure that personal data will be used only for authorized purposes and by authorized parties.

---

<sup>27</sup> Refer to definitions; this document

<sup>28</sup> Annex B, Model Data Privacy Consent Form

<sup>29</sup> IRR-DPA (RA No. 10173), 5(c)

<sup>30</sup> DPA, Sec.16

- b. **Restrict access** to the Data Center to yourself or to assigned personnel that shall have appropriate security clearance. Access should be enforced by a control system that records when, why, and by whom the data center is accessed. The procedures shall be reviewed regularly by the office concerned, the management or the DPO.
        - c. **Data collected from parties other than the data subject for purpose of research** shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research: Provided, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity
4. **RETENTION.** Only the needed and necessary personal data should be retained and stored, and only for the minimum period required by law. They should not be retained longer than necessary. Reference shall be made to the BSU Records Disposition Schedule (RDS) formulated under the supervision of the National Archives of the Philippines vis-à-vis NAP General Circular No. 1.<sup>31</sup>
  - a. **Determine the retention periods** for the personal data in your custody considering the fulfillment of the declared, specified, and legitimate purpose for the processing; the establishment, exercise or defense of legal claims; and the legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
  - b. **Lay out procedures** and documentation for the destruction, disposal, or de-identification of the personal data. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subject.
  - c. **Personal data originally collected** for a declared, specified, or legitimate purpose may be stored for longer periods if these are to be processed further for historical, statistical, or scientific purposes and in cases laid down in law. This is subject to the implementation of the appropriate organizational, physical, and technical security measures required by the DPA in order to safeguard the rights and freedoms of the data subject.
  - d. **Personal data shall not be retained in perpetuity** in contemplation of a possible future use yet to be determined.
5. **DISCLOSURE AND SHARING.** Personal data under the custody of the University shall be disclosed only when allowed by law and pursuant to a lawful purpose and made to identified and authorized recipients of such data.
  - a. **Determine if your office is legally authorized** to disclose personal data. If so, the purpose of the disclosure and its means should be defined and, likewise, consonant to the purpose of the collection.
  - b. **Disclose only the personal data** authorized and necessary for the indicated purpose or relevant to the subject matter of the request.

---

<sup>31</sup> National Archives of the Philippines; Rules and Regulations Governing the Management of Public Records and Archives Administration; January 20, 2009



- c. **Request for information shall not be denied** unless it clearly falls under any of the exceptions listed in the inventory or updated inventory of exceptions circularized by the Office of the President through E.O No. 2.<sup>32</sup>
- d. **When resolving a pending request for access** to personal data you must consider the following:
  - 1) the information requested falls under matters of public concern/interest;
  - 2) the individual requesting for personal data has declared and specified the purpose of his or her request;
  - 3) the declared and specified purpose is not contrary to law, morals, and public policy; and
  - 4) the personal data requested is necessary to the declared, specified, and legitimate purpose. Each request should be evaluated in relation to its declared purpose.

The determination of the applicability of any of the exceptions to the request shall be your responsibility as HO. In case of doubt, consult the Data Protection Officer.

- e. **Sharing or disclosure with other government agencies** must always be for the purpose of a public function or provision of a public service,<sup>33</sup> consistent with and necessarily required under the general mandate of BSU and the agency concerned.<sup>34</sup> This should be covered by a Data Sharing Agreement. This subject is spelled out in more detail in NPC Circular 16-02 of 10 October 2016.<sup>35</sup>
  - f. **Sharing or disclosure between and among BSU offices** must be specifically authorized under the program, system or initiative (common users) or under paragraph six (6) above.
  - g. **The sharing or disclosure of personal data which is aggregated** or kept in a form in which a data subject will no longer be identified (*i.e.* in the form of summaries or statistical tables) need not be covered by a data sharing agreement.
6. **DELETION, DESTRUCTION AND DISPOSAL.** The purpose of disposal/deletion is to irreversibly delete or destroy the personal data so that it becomes completely unreadable, accessible or irretrievable. The method used must, therefore, match with the type of storage technology, including paper-based copies.
- a. **Hard Copies.** When handling hard copies such as paper printouts, CDs, DVDs, or Blu-ray discs, shred the copy in order to completely destroy the data. Recycling hard copies (*e.g., use as scratch papers*) is not prohibited, provided that they do not hold personal data.
  - b. **Soft Copies.** When storing soft-copy data, organize files in such a way that they are deleted when needed. Different types of electronic media demand specific methods of destruction in order that secure destruction is effected. The greatest challenges in the secure destruction of electronic records are keeping pace with the changes in technology and the methodologies required to conduct complete destruction. The irreversible destruction of data in electronic media devices (media sanitization) is a must. It is strongly advised that the assistance of our information technology

<sup>32</sup> See Annex A

<sup>33</sup> NPC Advisory Opinion No. 2017-54; 11 September 2017

<sup>34</sup> NPC Advisory Opinion No. 2017-52; 11 September 2017

<sup>35</sup> Data Sharing Agreements Involving Government Agencies

professionals be obtained to carry this out. Media destruction/disposal procedures, an allied system in the university's Records Disposition Schedule, shall be formulated.

### C. SPECIFIC GUIDELINES

1. Request for access to files, records or for other documents containing personal and sensitive personal data shall be directly filed with or referred to the Head of Office. Where the office receiving the request is not the primary custodian of the information/data being sought, the request must be referred to the office that has primary custody of such information or data.
2. Access to the data center shall be monitored by the HO. All those who enter and access the data center must register in a logbook dedicated for the purpose which shall indicate the name, date, time, purpose, and duration of each access.
3. If the data subject is the requesting party he/she shall accomplish a "*Request for Issuance of Documents/Information*" designed by your Office.<sup>36</sup> The request shall be processed under Republic Act No. 11032 otherwise known as the Ease of Doing Business and Efficient Government Service Delivery (EODB-EGSD) Act of 2018.
4. If the requesting party be a person other than the data subject, the request shall be treated under the procedures laid out in BSU's Freedom of Information Manual.<sup>37</sup> Always verify the requester's identity and validity of requests.
  - a. Only those matters of public concern may be made available to the public as:
    - i. personal data relating to the position or functions of a current or former government employee;
    - ii. personal data relating to the service performed by a current or former government contractor; and
    - iii. information regarding a benefit of a financial nature given by the government, at its discretion, to an individual.
  - b. Other types of personal data, especially sensitive personal information, may be released only if necessary, to the declared, specified, and legitimate purpose of the requesting party.
5. Where a particular document or form contains personal and sensitive personal information which is not of public concern, you may redact such personal data. There is a need to balance, in a case to case basis, the right to information of the public and the right to data privacy. Thus, any information included in the inventory of exceptions of E.O No. 2, s. 2016 which are included in a requested document shall be redacted. Redaction is the permanent removal of information within a document.<sup>38</sup> It can be done in the following manner:
  - a. *Physical documents.* Photocopy the original document and using a black marker pen, correction fluid, redaction tape, or other means, block out the concerned information or by some tool physically remove it from the photocopied version. After the concerned information has been redacted from the physical document, it must be

<sup>36</sup> The form can be patterned after that of the HRMO request form

<sup>37</sup> BOR Resolution No. 2611, s. 2017, Promulgated March 23, 2017

<sup>38</sup> NPC Advisory Opinion No. 2019-026; 24 April 2019

scanned again to produce an access version. Check the modified document to ensure all the redacted information is unreadable before releasing it.

- b. *Digital or electronic documents.* In redacting a digital document, the rule is to ensure that sensitive information is not just visually hidden or made illegible, but is actually removed from the source file. Redactions made to digital documents can in some circumstances be reversed, therefore an edited version of an electronic document must never be released. Call upon our IT experts for assistance when in doubt.
  - c. *As an alternative to redaction.* Where a document or file contain information which are included in the inventory of exceptions and a part or parts thereof are disclosable to the public, and redaction is deemed difficult, the information shall be extracted by reproducing it in a separate file or by photocopying a part or parts of a set of data.
  - d. *Before release of redacted document.* Before the redacted information, official record, or public record is released, the requesting party shall be required to sign a written undertaking that he or she shall not share nor disclose the information obtained through the FOI Program to any other person or entity, or use the information obtained in a manner that is not in accordance with the purpose stated in the request. This can be integrated as part of the "Request for Issuance of Documents/Information" mentioned earlier.
6. Facsimile technology, email, internet, web and wireless transmissions shall not be used for transmitting documents containing personal data.
  7. Where documents or media containing personal data is transmitted by mail or post, the HO shall ensure the use of registered mail or, where appropriate, guaranteed parcel post service. He/She shall establish procedures that ensure that such documents or media are delivered only to the person to whom they are addressed, or his or her authorized representative: *Provided*, that similar safeguards shall be adopted relative to documents or media transmitted between offices or personnel within the agency.

If found necessary, data processing units should formulate more detailed and specific guidelines adapted to their particular working environment or functions. Once this is cleared by the University Data Protection Officer, it should be posted in a conspicuous place in the office for the information, guidance, and appreciation of other employees and of the public.

### III. SECURITY MEASURES<sup>39</sup>

All personal data maintained by the University shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to the DPA and other issuances of the Commission. Thus, the University shall allow only data processors providing sufficient guarantees to implement appropriate security measures in such a manner that processing will meet the requirements of the DPA ensuring the protection of the rights of data subjects. To this end, reasonable organizational, physical, and technical security measures must be taken by University data processors to maintain the availability, integrity, and confidentiality of personal data. These security measures must be intended for the protection against natural dangers (accidental loss or destruction) and human dangers (unauthorized access, use, modification, etc.) of personal data, taking into account the nature of the record to be protected.

---

<sup>39</sup> DPA, Chapters V & VII; DPA-IRR, Rules V & VI

A. **ORGANIZATIONAL SECURITY MEASURES.** The system's environment, particularly to the individuals carrying them out. Implementing the organizational data protection policies aim to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful processing (i.e. access control policy, employee training, surveillance, etc.).

1. **DUTY OF CONFIDENTIALITY.** Strict confidentiality shall be an obligation of all employees with access to personal data. All BSU employees and personnel shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. All personnel involved in the processing and use of personal data shall be governed by a "Non-disclosure Agreement".<sup>40</sup>

2. **DATA PROTECTION OFFICER AND COMPLIANCE OFFICERS FOR PRIVACY**<sup>41</sup>

a. **Mandatory Designations.** Pursuant to the provisions of the law, the University has a duly designated Data Protection Officer who shall be responsible for overseeing the university's compliance with the DPA and such other data privacy laws, rules and regulations. Compliance Officers for Privacy (COP) are designated each for the Buguias and Bokod Campuses. The COPs shall be under the supervision of the DPO. Their contact details are as follows:

**DATA PROTECTION OFFICER**  
2/F, Main Administration Building  
Benguet State University, La Trinidad 0601  
Benguet, Philippines  
Email: [dpo@bsu.edu.ph](mailto:dpo@bsu.edu.ph); Landline: (074) 422-2176

<b>COMPLIANCE OFFICERS FOR PRIVACY (COP)</b>	
BSU, Bokod Campus	BSU, Buguias Campus
Daclan, Bokod 2605, Benguet	Loo, Buguias 2607, Benguet
Contact No. 0912-250-0169	Contact No. 0919-924-0941
Email: <a href="mailto:h.lino@bsu.edu.ph">h.lino@bsu.edu.ph</a>	Email: <a href="mailto:gracita.pne@gmail.com">gracita.pne@gmail.com</a>

b. **Position of the DPO or COP.** The DPO or COP should be full-time or organic employee of BSU in either a career or appointive position. They must be independent in the performance of their functions, and should be accorded a significant degree of autonomy by the University and not assigned functions that may give rise to any conflict of interest.

c. **Duties and Responsibilities of the DPO and COP.** A DPO shall, among others:

- 1) Oversee the University's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:
  - collect information to identify the processing operations, activities, measures, projects, programs, or systems of the university and maintain a record thereof;
  - analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
  - inform, advise, and issue recommendations to the university;

<sup>40</sup> Annex C

<sup>41</sup> NPC Advisory Opinion No. 2017-01; 14 March 2017

- ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
  - advise the university as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;
- 2) Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the University;
  - 3) Advise the University regarding complaints and/or the exercise by data subjects of their rights (*e.g.*, requests for information, clarifications, rectification or deletion of personal data);
  - 4) Ensure proper data breach and security incident management by the University, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
  - 5) Inform and cultivate awareness on privacy and data protection within the organization, including all relevant laws, rules and regulations and issuances of the NPC;
  - 6) Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the University relating to privacy and data protection, by adopting a privacy by design approach;
  - 7) Serve as the contact person of the University vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns;
  - 8) Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
  - 9) Perform other duties and tasks that may be assigned by the University that will further the interest of data privacy and security and uphold the rights of the data subjects.

Except for items 1) to 3), a COP 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.

The DPO or COP must have due regard for the risks associated with the processing operations of the University, taking into account the nature, scope, context and purposes of processing. Accordingly, they must prioritize their activities and focus their efforts on issues that present higher data protection risks.

- d. **Protection.** To strengthen the autonomy of the DPO or COP and ensure the independent nature of their role in the organization, the University should not directly or indirectly penalize or dismiss the DPO or COP for performing his or her tasks. It is not necessary that the penalty is actually imposed or meted out. A mere threat is sufficient if it has the effect of impeding or preventing the DPO or COP from performing their tasks. However, nothing shall preclude the legitimate application of administrative, civil or criminal laws against the DPO or COP, based on just or authorized grounds.



e. **General Obligations of the University relative to the DPO or COP.** The University should:

- 1) effectively communicate to its personnel, the designation of the DPO or COP and their functions;
  - 2) allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;
  - 3) provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO or COP to keep themselves updated with the developments in data privacy and security and to carry out their tasks effectively and efficiently;
  - 4) grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems;
  - 5) where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;
  - 6) promptly consult the DPO or COP in the event of a personal data breach or security incident; and
  - 7) ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.
3. **CONDUCT OF PRIVACY IMPACT ASSESSMENT (PIA).** The University shall undertake a Privacy Impact Assessment (PIA) for every processing system that involves personal data as otherwise provided in this Manual.
4. **CONDUCT OF TRAININGS OR SEMINARS.** The University shall sponsor, from time to time, trainings or seminars to keep personnel, especially the DPO and CPOs, updated vis-à-vis developments in data privacy and security. It shall conduct a mandatory training on data privacy and security at least once a year for personnel directly involved in the processing of personal data. Management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.
5. **REVIEW OF PRIVACY POLICY.** This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the university shall be updated to remain consistent with current data privacy best practices. There shall be periodic reviews of procedures adopted by and being implemented in the various personal data processors of the University.

**B. PHYSICAL SECURITY MEASURES.** Policies and procedures should be instituted that shall monitor and limit access to and activities in the office, room, workstation or facility containing personal data. It shall include guidelines that specify the proper use of and access to electronic media (*i.e.* locks, backup protection, workstation protection, etc.), physical design of office space, permissible means of transfer, etc.

1. **FORMAT AND MEDIUM OF PERSONAL DATA.** Define the format and medium of the personal data to be processed and where these are to be stored. Be guided by the university's

Records Management System (RSM) and other rules governing specific documents and data.

2. **STORAGE TYPES AND LOCATION.** It must be certain that all types of personal data are secured and protected in whatever form they are processed: physical, digital or electronic. The classification conducted by the Office Document Custodians of the various university units/offices in relation to the BSU Records Management System and BSU FOI Manual with the assistance of the OQAA would be of assistance.
3. **DATA CENTERS.** Centralized repositories shall be established by the University within all its campuses that shall henceforth be referred to as "*Data Centers*",<sup>42</sup> which may be physical or virtual, may be analog or digital, used for the storage, management, and dissemination of data.
4. **ACCESS PROCEDURE FOR BSU PERSONNEL.** Only authorized personnel shall be allowed inside the Data Center and who shall be entrusted with and have custody of the access key. Other authorized staff may be given a duplicate of the key. Other University personnel may be granted access to the room upon approval of the Office Head. Only the individuals actually authorized shall be in the data room at any given time
  - a. **Protect personal data in the processing system** against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. Regulate the manner of access to and examination of the files, records and other documents to avoid damage and loss, prevent undue interference with the duties of office personnel, and assure the exercise of the same constitutional right by other persons.<sup>43</sup> Only the data subject and the authorized personnel of the University shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.
  - b. **Physical media.** If personal data is stored in paper files or any physical media these should be physically secured (lock and key). An office log must be maintained from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. The log records, including all applicable procedures, shall be regularly reviewed.<sup>44</sup>
  - b. **Maintain the integrity of data.** Persons involved in personal data processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room or Data Centers.
5. **MODES OF TRANSFER OF PERSONAL DATA WITHIN THE ORGANIZATION, OR TO THIRD PARTIES.** Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.
6. **OFFICE SPACE AND/OR WORK STATION.** Personnel shall be assigned office space or work stations with the least volume of foot traffic to minimize risk of breach and other security incidents. Computers shall be positioned with considerable space between them to maintain privacy and protect the personal data processing.

---

<sup>42</sup> NPC Circular 16-01 (10 October 2016), Rule I, Sec. 3.E and Rule II, Sec. 7

<sup>43</sup> Legaspi vs. Civil Service Commission, G.R. No. L-72119 (29 May 1987)

<sup>44</sup> Id. Rule III, Sec. 22

C. **TECHNICAL SECURITY MEASURES.** This involves the technological aspect of security in protecting personal information (*i.e.* computer network, encryption, data center policies, data transfer policies, software security, authentication, etc.).

1. **NETWORK SECURITY.** Safeguards to protect the University's 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 shall be adopted. These shall include the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
2. **DATABASE/SERVER SECURITY.** Where possible, staff handling personal data shall not be allowed to save files on a local computer (individual PC) but directed to save files only to their allocated network drive created in assigned data center.<sup>45</sup> Where University computers, laptops, and other devices are used in the processing of personal data these shall be protected by passwords or passcodes. Passwords or passphrases used to access personal data should be of sufficient strength to deter password attacks. A password policy should be adopted and enforced.<sup>46</sup>
3. **BACK-UPS.** A backup file for all personal data under custody should be maintained. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.
4. **ENCRYPTION AND AUTHENTICATION.** The University shall adopt means for the encryption of personal data with the most appropriate encryption standards during storage and while in transit; authentication processes, and other technical security measures that control and limit access.
5. **SOFTWARE APPLICATIONS REVIEW.** Software applications should be reviewed and evaluated by a technical team created by the University before the installation thereof to ensure the compatibility of security features with overall operations and compliance with data privacy laws. The DPO shall be a consulting member thereof.
6. **REVIEW OF SECURITY POLICIES.** The University shall review security policies, conduct vulnerability assessments and perform penetration testing on regular schedule to be prescribed by the appropriate department or unit.

#### **IV. BREACH AND SECURITY INCIDENTS<sup>47</sup>**

##### **A. DATA BREACH RESPONSE TEAM.**

1. **CREATION.** The University has in place a Data Breach Response Team responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.
2. **FUNCTIONS.** The team must be ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any

---

<sup>45</sup> NPC Circular 16-01 (Security of Personal Data in Gov't. Agencies), Rule II, Sec. 7, Rule III, Sec. 19

<sup>46</sup> *Id.*, Rule II, Sec. 8

<sup>47</sup> NPC Circular 16-03, Personal Data Breach Management

resulting damage, and comply with reporting requirements. It shall be responsible for the following:

- a. Implementation of the security incident management policy of the personal information controller or personal information processor;
  - b. Management of security incidents and personal data breaches; and
  - c. Compliance by the personal information controller or personal information processor with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.
2. NOTIFICATION PROTOCOLS. The Data Breach Response Team shall prepare and circularize detailed notification and reporting protocols for incident or breach in accordance with the DPA and its IRR, and any other issuance of the NPC.
  3. BREACH REPORT. The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

## B. PRIVACY IMPACT ASSESSMENT

As part of its security incident management protocols the University shall undertake Privacy Impact Assessments (PIA) for both new and existing systems, programs, procedures, measures, or technology products that involve or impact processing personal data. It should be undertaken for new processing systems prior to their adoption, use, or implementation. Changes in the governing law or regulations, or those adopted within the University, CHED, or PASUC may likewise require the conduct of a PIA, particularly if such changes affect personal data processing. It may choose to outsource the conduct a PIA to a third party.

## C. PROCEDURE FOR RECOVERY AND RESTORATION OF PERSONAL DATA

Always maintain a backup file for all personal data under your custody. In the event of a security incident or data breach, always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach. Take the required action to preserve the integrity of the personal data.

## V. OUTSOURCING AND SUBCONTRACTING AGREEMENTS<sup>48</sup>

### A. SUBCONTRACTING OF PERSONAL DATA

1. Processing of personal data may subcontracted or outsourced upon approval of the University President *provided that*, contractually or other reasonable means shall be used to ensure that proper safeguards are in place, to guarantee the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the DPA and its IRR, other applicable laws for processing of personal data, and other issuances of the NPC.
3. The processing shall be governed by a contract or other legal act that binds the PIP to BSU. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and

---

<sup>48</sup> Rule X, DPA-IRR

categories of data subjects, the obligations and rights of the parties, and the geographic location of the processing under the subcontracting agreement.

**B. AGREEMENTS FOR OUTSOURCING.** Processing by a personal information processor (PIP) for the University shall be governed by a contract that binds the personal information processor to BSU.

1. The contract or legal act shall 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 personal information controller, and the geographic location of the processing under the subcontracting agreement.
2. The contract or other legal act shall stipulate, in particular, that the Personal Information Processor shall:
  - a. Process the personal data only upon the documented instructions of the University, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
  - b. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;
  - c. Implement appropriate security measures and comply with the DPA, its IRR, and other issuances of the Commission;
  - d. Not engage another processor without prior instruction from BSU: *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;
  - e. Assist BSU, 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;
  - f. Assist BSU in ensuring compliance with the DPA, its IRR, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;
  - g. At the choice of BSU, delete or return all personal data to her 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 DPA or another law;
  - h. Make available to BSU all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by BSU or another auditor mandated by the latter;
  - i. Immediately inform BSU if, in its opinion, an instruction infringes the DPA, its IRR, or any other issuance of the Commission.

**C. DUTY OF BSU.** BSU shall comply with the requirements of the DPA, its IRR, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.



## VI. RULES ON ACCOUNTABILITY<sup>49</sup>

### A. ACCOUNTABILITY FOR TRANSFER OF PERSONAL DATA

1. **RESPONSIBILITY FOR PERSONAL DATA.** BSU and its data processors shall be responsible for any personal data under their 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.
2. **PROCESSING BY PIPs.** BSU and its data processors shall be accountable for complying with the requirements of the DPA and its IRR, and other issuances of the NPC. 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.
3. **COMPLIANCE OFFICER.** The Head of the data processing unit shall automatically be a Compliance Officer and accountable for compliance with the DPA. The identity of the Head of Office shall be made known to a data subject upon request.

### B. ACCOUNTABILITY FOR VIOLATIONS

1. **PERSON LIABLE.** University personal data processors who fails to comply with this Manual, 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.
2. **PROSECUTION.** In case of criminal acts and their corresponding personal penalties, the person who committed the unlawful act or omission shall be recommended for prosecution by the NPC based on substantial evidence.

## VII. INQUIRIES AND COMPLAINTS<sup>50</sup>

### A. RIGHTS OF A DATA SUBJECT.<sup>51</sup> Every data subject has the following rights as provided under the DPA and other privacy laws.

1. **RIGHT TO BE INFORMED.** The data subject has a right to be informed whether personal data pertaining to him/her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.

The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information processor via the university's Data Privacy Notice, or at the next practical opportunity:

- a. Description of the personal data to be entered into the system;
- b. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
- c. Basis of processing, when processing is not based on the consent of the data subject;
- d. Scope and method of the personal data processing;

---

<sup>49</sup> Id., Rule XII

<sup>50</sup> NPC Privacy Tool Kit, 3<sup>rd</sup> Edition

<sup>51</sup> DPA, Chapter IV; Rule VIII, id.

- e. The recipients or classes of recipients to whom the personal data are or may be disclosed;
  - f. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
  - g. The identity and contact details of the personal data processor;
  - h. The period for which the information will be stored; and
  - i. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.
2. **RIGHT TO OBJECT.** Data subjects have the right to indicate their refusal to the processing of their personal data. Once they have served notice of the withholding of consent, further processing of their personal data will no longer be allowed, unless:
    - a. The processing is required pursuant to a subpoena, lawful order, or as required by law; or
    - b. The collection and processing is undertaken pursuant to any lawful basis or criteria or where the data is not covered by the DPA.
  3. **RIGHT TO ACCESS.** Data subjects may be given access to or a copy of their personal data upon request. They also have the right to request access to the circumstances relating to the processing and collection of their personal data, insofar as allowed by law. They may be charged a small fee for this service.
  4. **RIGHT TO RECTIFICATION.** They have the right to request us to immediately correct any inaccuracy or error in their personal data or to complete the information they believe is incomplete. Upon request, and after correction has been made, inform any recipient of the personal data of its inaccuracy and the subsequent rectification that was made.
  5. **RIGHT TO ERASURE OR BLOCKING.** In the absence of any other legal ground or overriding legitimate interest for the lawful processing of personal data, or when there is substantial proof that personal data is incomplete, outdated, false, or has been unlawfully obtained, they may request us to suspend, withdraw, or order the blocking, removal, or destruction of their personal data from our filing system. We may also notify those who have previously received their processed personal data.
  6. **RIGHT TO DATA PORTABILITY.** In case their personal data was processed through electronic means and in a structured and commonly used format, they have the right to obtain a copy of such personal data in such electronic or structured format, subject to the guidelines of the National Privacy Commission with regard to the exercise of such right.
  7. **TRANSMISSIBILITY OF RIGHTS.** Upon the death of a data subject, or in case of incapacity or inability to exercise legal rights, the data subject's lawful heirs and assigns may invoke such rights in his/her place.
  8. **LIMITATION ON RIGHTS; MANNER OF EXERCISE.** The rights mentioned under this item are not applicable if personal data are processed only for scientific and statistical research purposes, and without being used as basis for carrying out any activity or taking any

decision regarding them as the data subject. Their rights as data subjects are also subject to other limitations provided by law. It is required that they exercise their rights as described in this Notice in a reasonable and non-arbitrary manner, and with regard to the rights of other parties.

All requests, demands or notices which they may make under this Notice or applicable law must be made in writing and will only be considered received when done so by the University Data Protection Officer.

- B. **PROCEDURES.** The processing units shall adopt procedures for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted shall be received and acted upon. These should include a confirmation with the complainant of receipt of the complaint.

### VIII. EFFECTIVITY

**BOR APPROVAL.** This Data Privacy Policy shall be effective upon its approval by the University's Board of Regents or as may otherwise be indicated. Amendments thereto, including specific office operational policies, shall be approved by the University's Administrative Council with notice to the Board of Regents if found necessary.

\*\*\*

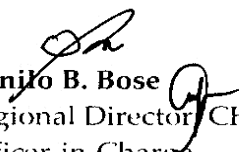
### CERTIFICATION

I CERTIFY that this Data Privacy Policy was presented to and recommended for approval by the University Administrative Council in its meeting of 24 June 2020 under **AdCo Res. No. 022, s. 2020**. I CERTIFY, further, that it was approved by the University Board of Regents during their meeting of October 22, 2020 through **BOR Res. No. 156a, s. 2020**.



Grace T. Bengwayan  
University and Board Secretary

Attested:



Danilo B. Bose  
Regional Director CHED-CAR  
Officer-in-Charge  
Office of the University President

FOR B.