CONSENT FORM
(FOR NON FACULTY APPLICANT/EMPLOYEE)

I, _____ of legal age, being an applicant/employee of _____, affirm that:

1. _____ may process information about me which includes my name, address, date of birth, citizenship, gender, contract information (mobile number and email), birth certificate, marriage certificate (if any), dependent certificate (if any), government issued identifications (TIN, PAG IBIG, SSS, Philhealth), NBI clearance, educational background (transcript of records and diploma), certificates of awards and recognition, certificates from trainings, certificate of employment, background investigation necessary to get information on previous employment, medical and health related documents and declarations, and other information which may be considered personal and sensitive personal information (collectively, Personal Information) under the Data Privacy Act of 2012. Processing is any operation performed in the Personal Information, such as but not limited to, collection, retention, disclosure, publication and destruction ("Processing").

2. The processing of my personal information is for the purposes of:
   a) Validation and identification of the applicant/employee
   b) Employment assessment and evaluation
   c) Verification such as background checks and educational attainment verification
   d) Lawful non-commercial information with respect to its legitimate interests
   e) Protection of the health and vital interest of the applicant/employee thru medical or health evaluation and activities
   f) Payroll processes, benefits processing, disciplinary actions and other administrative tasks
   g) Setting up or processing needed in human resources information systems.
   h) Processing of grants of documents needed in partnerships that _____ will undertake
   i) Use in emergency situations to protect the vital and medical interest of the applicant/employee.

3. _____ may share or disclose my Personal Information to:
   a. Colleges, Departments and Units relevant to the position currently held by the employee or is being applied for by the applicant
   b. Government agencies where mandatory reporting is required such as BIR, SSS, PAG IBIG, PhilHealth and DOLE and other appropriate government agencies or offices
   c. For medical or health related requirements
   d. Employment information requests by prospective organizations that the employee is transferring to or applying for.
   e. Personal Data SHALL NOT be shared with parties not currently stated without prior additional consent from the data subject.

4. All applicant/employee are maintained by the Human Resources Department upon acceptance. Such data is stored by HR Department in perpetuity as to provide a service to support requirements of the data subject for their right to access, right to correct, right to data portability as in the case of benefits claims document requirements. There is a clause under the Data Privacy Act on not allowing perpetual storage of personal data. However, for undeclared and unforeseen purposes, HR Department is acquiring the consent of the applicant/employee as the purpose is clearly declared and foreseen as previously stated. In case of separated employees, the period of retention is ten (10) years.

5. All applicants that were not accepted, the personal data collected of the applicant shall be kept for a period of one (1) year from application period. Upon the lapse of the one (1) year period, paper documents shall be shredded for secure disposal. Electronic records shall be deleted securely as well. In case of separated employees, the personal data collected shall be kept for a period of ten (10) years. Upon the lapse of the ten (10) year period, paper documents shall be shredded for secure disposal. Electronic records shall be deleted securely as well.

Under RA 10173 also known as the Data Privacy Act of 2012, the following are the rights of the Data Subject:

1. The right to be informed means that the data subject has the right to know when his or her personal data shall be, are being, or have been processed.

2. The right to access involves being able to compel any entity possessing any personal data to provide the data subject with a description of such data in its possession, as well as the purposes for which they are to be or are being processed.

3. The right to object requires that the consent of the data subject be secured in the collecting and processing of his or her data.

4. The right to erasure or blocking allows the data subject to suspend, withdraw or order the blocking, removal, destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.

5. The right to rectify, allows the data subject to dispute any inaccuracy or error in the personal information processed, and to have the personal information controller correct it immediately.
6. The right to data portability enables the data subject to obtain and electronically move, copy, or transfer personal data for further use.
7. The right to file a complaint with the National Privacy Commission.
8. The right to damages entitles the aggrieved data subject to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of his or her personal information.

_____

Signature over Printed Name

_____

Date Signed