Surigao State College of Technology (SSCT) DATA PRIVACY MANUAL

SSCT hereby adopts this Data Privacy Manual in compliance with Republic Act No. 10173 or *An Act Protecting Individual Personal Information and Communication Systems in the Government and the Private the Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes*, its Implementing Rules and Regulations (IRR), and other relevant policies and issuances of the National Privacy Commission (NPC).

The Data Privacy Act passed into law in 2012 consistent with the Philippines' policy of protecting the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. To promote such policy, the Act, alongside the IRR, shall govern the processing of personal data by any natural or juridical person in the government or in the private sector, which must in turn establish policies and implement measures to guarantee the security of personal data under their control and/or custody.

With the Data Privacy Act, its IRR other pertinent laws, and the principles of transparency, legitimate purpose, and proportionality as its backdrop, SSCT abides by this Manual in carrying out its operations. This is so as to ensure that personal data under its control remain safe and secured while being processed in the course of its key operations and processes.

This Manual aims to inform students, their parents/or guardians, employees, partners, and stakeholders of SSCT's data protection and security measures, and to guide them in the exercise of their rights under the Data Privacy Act and other relevant regulations and policies.

ARTICLE I
INTRODUCTION

SECTION 1. DEFINITIONS

"Authorized Personnel" refers to employee/s or officer/s of SSCT authorized to collect and/or to process Personal Data either by the function of their office or position, or through specific authority given in accordance with the policies of SSCT.

"Commission" or the **"NPC"** shall refer to the National Privacy Commission

"Compliance Officer for Privacy" or **"COP"** refers to an individual duly authorized by SSCT to perform some of the functions of the DPO especially in other Campuses of SSCT.

"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/her Personal, Sensitive Personal, or Privileged Information. It 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.

"Data Privacy Response Team" refers to a group of individuals designated by SSCT to respond to inquiries and complaints relating to data privacy, and to assist in ensuring SSCT's compliance with the Data Privacy Act, its IRR, and any other government-issued data privacy regulations and issuances, as well as in implementing this Manual.

"Data Processing Systems" refers to the structures and procedures by which Personal Data is collected and further processed by SSCT in its Information and Communications System/s and/or relevant Filing system/s, including the purpose and intended output of the Processing.

"Data protection Officer" or **"DPO"** refers to the officer duly designated by SSCT to be accountable for the latter's compliance with the Data Privacy Act, its IRR, and any other government-issued data privacy regulations and issuances, as well as implementation of the Manual. The DPO shall also act as a liaison between SSCT and the National Privacy Commission for privacy-related compliance matters.

"Data Sharing" is 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.

"Data Subject" refers to an individual whose Personal, Sensitive Personal, and/or Privileged Information are processed. For purposes of this Manual, it refers to employees (whether temporary, regular, casual, or part-time), students, alumni, on-the-job trainees, applicants, clients, office visitors and other persons whose Personal Data are collected and processed by SSCT as an integral and necessary part of SSCT operations.

"Filing System" refers to any set of information relating to a natural or juridical person to the extent that, although the information is not processed by the equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to the individuals or by the reference to criteria relating to individuality, in such a way that specific information relating to a particular person is readily accessible.

"Information and Communication System" refers to a system for generating, sending, receiving, storing or otherwise Processing electronic data messages, or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.

"Personal Data" refers to all types of Personal Information collected and processed by SSCT. The term Personal Data includes, but is also limited to, the following:

(a) **"Confidential Personal Data"** pertains to all information to which access is restricted and of which Processing requires the written consent of the

Data Subject concerned, such as but not limited to Employee 201 files and information contained therein, device passwords, and/or passcodes, bank account numbers, ATM card numbers, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

(b) "**Public Personal Data**" pertains to Personal Information and of a Data Subject which may be disclosed to the public by SSCT due to, or as required by, its operations and for government regulatory compliance and company disclosures.

"**Personal Data Breach**" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or, or access to, Personal Data transmitted, stored, or otherwise processed. A Personal Data Breach may be in any of the following nature:

(a) "**Availability Breach**" which results from the loss of, or accidental or unlawful destruction of Personal Data;
(b) "**Confidentiality Breach**" which results from the unauthorized disclosure of, or access to Personal Data; and/or
(c) "**Integrity Breach**" which results from the alteration of Personal Data.

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

"**Personal Information Controller**" or "**PIC**" refers to a natural or juridical persons, or any other body, including SSCT, who/which controls the Processing of Personal Data, or instructs another to process Personal Data on its behalf.

"**Personal Information Processor**" or "**PIP**" refers to any natural or juridical person, or any other body, to whom a PIC, including SSCT, outsources or gives instructions as regards the Processing of Personal Data of a Data Subject or group of Data Subjects.

"**Privacy Impact Assessment**" is a process undertaken and used to evaluate and manage the impact on privacy of a particular program, project, process, measure, system, or technology product of SSCT or its PIP/s. It 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 privacy best practices, and the cost of security implementation. SSCT shall conduct a Privacy Impact Assessment annually through the joint accomplishments by key personnel of SSCT.

"**Privacy Policy**" refers to the statement that governs SSCT practices of handling Personal Data. It instructs the users of Personal Data (i.e, Authorized Personnel) on the processing of Personal Data and informs them of the rights of the Data Subjects and their correlative obligations as users of Personal Data with respect thereto. This Manual outlines the Privacy Policy of SSCT.

"Privacy Notice" refers to the statement made to a Data Subject to inform him/her of how SSCT processes his/her Personal Data.

"Privileged Information" refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communications.

"Processing" refers to any operation or set of operations performed upon Personal Data including, but not limited to, its collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction. Processing may be performed through automated means or by manual processing.

"Security Incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality or Personal Data. It includes incidents that would result to a Personal Data Breach, if not for safeguards that have been put in place.

"Security Measures" refers to the physical, technical, and organizational measures employed by SSCT to protect Personal Data from natural and human dangers.

"Sensitive Personal Information" refers to Personal Information:

(a) about an individual's race, ethnic region, marital status, age, color, and religious, philosophical, or political affiliations;
(b) about an individual's health, education, genetic or sexual life, 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;
(c) issued by government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and
(d) specifically established by an executive order or an act of Congress to be kept classified.

SECTION 2. SCOPE AND LIMITATIONS

This Manual shall lay down the data protection and Security Measures of SSCT. It shall govern the Processing of Personal Data of Data Subjects by SSCT and the latter's PIP/s if any. All employees of SSCT, regardless of the type of employment, as well as all PIP/s, are enjoined to comply with the terms laid down in this Manual.

SECTION 3. DATA PRIVACY PRINCIPLES

In the Processing of Personal Data, SSCT, its employees and PIP/s shall abide by the following principles:

a) **Transparency**. The Data Subject shall be informed of the nature, purpose, and extent of the Processing of his/her Personal Data, including the risks and

safeguards involved, the identity of SSCT, his/her rights as a Data Subject, and how these rights may be exercised.

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

c) **Proportionality**. The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data will be processed by SSCT only if the purpose of the Processing could not be reasonably fulfilled by other means.

ARTICLE II
DATA PROTECTION OFFICER AND COMPLIANCE OFFICER FOR PRIVACY

SECTION 1. DATA PROTECTION OFFICER

SSCT shall have a Data Protection Officer who shall be responsible for overseeing the compliance of SSCT with the Data Privacy Act of 2012, its IRR, other pertinent laws and government issuances on data privacy, and this Manual.

Upon the request of a Data Subject, the name of the DPO shall be made available by SSCT.

SECTION 2. COMPLIANCE OFFICER FOR PRIVACY

Each Campus or office may appoint among its ranks a COP, who shall be responsible for overseeing the compliance of SSCT with the Data Privacy Act of 2012, its IRR, other pertinent laws and government issuances on data privacy, and this Manual.

Upon the request of a Data Subject, the name of the COP shall be made available by SSCT.

SECTION 3. GENERAL QUALIFICATIONS

The DPO and/or COP/s should have sufficient understanding of the processing operation being carried out by the college.

SECTION 4. TERM

The DPO and/or COP/s shall be regular or permanent position in SSCT.

SECTION 5. VACANCY

Where the position of either the DPO or COP is left vacant, the college shall appoint or reappoint within a reasonable period of time. SSCT may require the incumbent DPO or COP/s, as the case may be or any employee of the college who demonstrate position of the general qualification required by Article II, Section 3 hereof, to occupy the vacant position in a holdover capacity, until the appointment of the new DPO or COP.

SECTION 6 FUNCTION OF THE DPO AND / OR COP

The DPO and/or COP/s shall have the following functions:

(a) Monitor SSCT's compliance with this manual, the Data Privacy Act, its IRR, issuances of the Commission, and other applicable laws, and policies. For such purpose, the DPO and/or COP/s may:
   (i) collect or cause the collection of information to identify the processing operations, activity measures, projects, programs, or system of the college, and maintain the maintenance of records thereof;
   (ii) analyze and check, or cause the analyzation and checking of, compliance of SSCT's Processing activities, including the issuance of security clearances to, and compliance of service providers, with the applicable laws and contracts on data privacy:
   (iii) inform, advice and issue recommendations to the college with regard to compliance with applicable laws and contracts on data privacy, as well as the implementation of this manual.

(b) ensure the conduct of Privacy Impact Assessments relative to activity measures, projects, programs, or systems of the college at least once a year;

(c) advice the college regarding the exercise by Data Subject of their Rights as specified in Article III hereof, as well as complaints made to the DPO and/or COP/s of the college;

(d) ensure the SSCT's proper management of Security Incident/s if any, including the latter's preparation and submission to the Commission of reports and other documentation concerning such Security Incident/s within the prescribed period;

(e) cultivate awareness of data protection regulations within SSCT including this Manual, the Data Privacy Act, its IRR, and other government issuances on data privacy;

(f) advocate for the development, review and/or revision of policies, guidelines, projects, and/or programs of SSCT relating to privacy and data protection;

(g) serve as a contact person of SSCT vis-à-vis Data Subject, the Commission, and other authorities and all matters concerning data privacy and security issues or concerns;

(h) cooperate, coordinate, and seek the advice of the commission regarding matters concerning privacy and data protection;

(i) lead the Data Privacy Response Team of SSCT; and

(j) perform other duties and tasks that SSCT may assign to further the interest of privacy and data protection and uphold the Rights of Data Subject, as specified in Article III hereof.

The COP/s of SSCT may perform any of the functions of the DPO. Where appropriate, the COP/s shall assist the DPO in the performance of the latter's functions.

ARTICLE III
RIGHT OF THE DATA SUBJECT

As provided under the Data Privacy Act, a Data Subject shall have the following rights in connection with the Processing of his/her Personal Data. SSCT Employees and PIP/s, as the case may be, shall respect the rights of all Data Subjects. To exercise said rights the Data Subject may accomplish the Data Privacy Right Form, indicating therein the right he/she wishes to exercise with respect to his/her Personal Data, and transmit the same to SSCT through its Authorize Personnel, DPO or COP/s.

SECTION 1. RIGHT TO BE INFORMED

The Data Subject has the right to be informed whether Personal Data pertaining to him/her shall be, are being, or have been processed. Before entry of his/her Personal Data into the SSCT's Information and Communications System/s and or Filing System/s or to the next practicable opportunity, the data subject is entitled to be furnished with the following information:

a) description of the Personal Data to be entered into the Information and Communications System/s and/or Filing System/s of the College;
b) purpose/s for which Personal Data are being or will be processed;
c) basis of Processing, in case Processing is not based on the Consent of the Data Subject;
d) scope and method of the Processing of Personal Data;
e) recipient/s or classes of recipient/s to whom the Personal Data are or may be disclosed or shared;
f) in case of automated access, and where allowed by the Data Subject, the methods utilized therefore, and 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) identity and contact details of SSCT; its representative, and/or, upon request, the DPO and/or COP/s;
h) period for which the Personal Data will be stored; and
i) existence of his/her rights as a Data Subject, including the right to lodge a complaint before the Commission.

SECTION 2. RIGHT TO OBJECT

The Data Subject shall have the right to object to the Processing of his/her Personal Data. The Data Subject shall also be notified and given an opportunity to withhold his/her consent to the Processing in case of changes or any amendment to the information supplied or declared to the Data Subject in the immediately preceding Section. When a Data Subject objects or withholds consent, SSCT shall no longer Process the Personal Data, unless:

a) the personal Data is needed pursuant to a subpoena;
b) the Processing is for obvious purposes, including, when it is necessary for the performance of, or in relation to a contract or service to which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between SSCT and the Data Subject (e.g., to assess the qualification of an applicant for the suitability of a current employee for promotion or transfer, SSCT may require information as regards the person's educational attainment); or
c) the Personal Data is being collected and processed pursuant to a legal obligation (e.g., to make the mandatory contributions to an employee's Government Service Insurance System (GSIS), Pag-IBIG Home Development Mutual Fund, and the PhilHealth accounts, SSCT has to obtain the pertinent social security numbers of the employee).

SECTION 3. RIGHT TO ACCESS

The Data Subject has the right to demand reasonable access to the following:

a) contents of his/her Personal Data that were processed;
b) sources from which Personal Data were obtained;
c) names and addresses of recipient/s of the Personal Data;
d) manner by which his/her Personal Data were processed;
e) reasons for the disclosure of the Personal data to recipient/s, if any;
f) information on automated processes where the Personal Data will, or is likely to, be made us the sole basis for any decision that significantly affects or will affect the Data Subject;
g) date when Personal data concerning the Data Subject were last accessed and modified.
h) the designation, or name or identity, and address of the personal information controller.

SECTION 4. RIGHT TO CORRECTION

The Data Subject has the right to dispute the inaccuracy or error in his/her Personal Data, and have SSCT accordingly correct or cause the correction thereof. If the personal data has been corrected, SSCT shall ensure the accessibility of both the new and the retracted Personal Data by the intended recipient/s thereof. Recipients or third parties who have previously received such processed Personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

SECTION 5 RIGHT TO ERASURE OR BLOCKING

The Data subject shall have the right to suspend, withdraw, or order the blocking, removal or deconstruction of his/her Personal Data from SSCT's information and Communications System/s and/ or filing System/s, and may exercise such right, upon discovery and /or substantial proof of any of the following:

a) the Personal Data is incomplete, out-dated, false or unlawfully obtained;

b) the Personal Data is being used for purpose/s not authorized by the Data Subject;
c) the Personal Data is no longer necessary for the purpose/s for which they were collected;
d) the subject withdraws consent or objects to the Processing and there is no other legal ground or overriding legitimate interest for the Processing;
e) the personal data concerns information prejudicial to the Data Subject, unless justified by the freedom of speech, of expression or the press, or otherwise authorized;
f) The processing is unlawful; or
g) The Right/s of the Data Subjects has been violated.

Upon reasonable request of the Data Subject, SSCT shall notify third parties who have previously received such processed Personal Data of the Data Subject's decision to exercise such right.

SCETION 6. RIGHT TO DATA PORTABILITY

Where his/her Personal Data is processed by electronic means in a structured and commonly used format and upon his/her written request, the data Subject shall have right to obtain from SSCT a copy of such Personal Data in an electronic or structured format that is commonly used and allows for further use by the Data Subject.

SECTION 7. RIGHT TO COMPLAIN BEFORE THE COMMISSION

The Data Subject shall have the right to complain before the Commission for any data privacy violation committed by SSCT, if any.

SECTION 8. TRANSMISSIBLITY OF RIGHTS

Any lawful heir and/or assign of the Data Subject may invoke the Rights of the Data Subject to which he/she is an heir and/or assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her right.

ARTICLE IV

PROCESSING OF PERSONAL DATA

Whenever necessary, SSCT may modify any of its Data Processing Systems but, under all circumstances, must respect the rights of the Data Subjects and observe compliance with this Article, among others, in Processing the Personal Data of Data Subjects.

SECTION 1. COLLECTION

1.1 Conditions. SSCT shall only collect and process the Personal Data of a Data Subject upon the concurrence of the following conditions:

a) Prior to collection, or as soon as practicable, Data Subject shall have the right to be informed of:
   i) the specific purpose for the collection and Processing of Personal Data;
   ii) the extent of Processing of Personal Data; and
   iii) his/her Rights as a Data Subject.

b) SSCT shall have obtained the Consent of the Data Subject to whom the Personal Data relates, unless the collection and Processing of the Personal Data are:
   i) pursuant to law and/or government issuances;
   ii) necessary to perform a contract to which the Data Subject is a party, or to take steps prior to entering into a contract;
   iii) necessary to protect the interest of the Data Subject;
   iv) necessary to perform a task in the interest of the public or in the exercise of official authority vested upon SSCT; or
   v) necessary to protect the lawful rights and interest of SSCT in court proceedings, or to establish, exercise, or defend a legal claim.

SECTION 2. USE

2.1 General. The use of the Personal Data shall only be for the purpose/s specified and declared to the Data Subject, and with the Consent of the Data Subject, unless such use of personal data falls under the enumeration listed in Section 1, Article IV of this Manual.

2.2 Purpose. SSCT's use of the Personal Data shall only be for the purpose of carrying out the operation of SSCT. The Processing of Personal Data of Data Subjects shall be for the following general purposes, among others:

a) to document and manage SSCT records;
b) to conduct due diligence prior to executing a contract, and to facilitate the fulfillment of the terms of the contract thereafter;
c) to respond to queries, complaints, and requests;
d) to provide information about SSCT's services;
e) to conduct research and analysis to improve customer experience;
f) to maintain security; and
g) to comply with legal, regulatory, and contractual requirements or obligations.

The use and processing of Personal Data also depends on SSCT transactions involved.

If the Data Subject is a Prospective employee, SSCT may collect, use, or process the Data Subject's Personal Data to:

a) evaluate his/her suitability for employment and, with a written or expressed consent, retain his/her Personal Data for a maximum of five (5) years for future job opportunities that may be of interest to the Data Subject.
b) communicate with the Data Subject about his/her employment application;
c) if hired, process his/her Personal Data as may be necessary for purposes such as, but not limited to payroll, benefits application, allowances and refunds processing, tax processing, retirement benefits, and other purposes that demand or require processing of his/her Personal Data (*e.g.*, to execute business transactions directly related and/or incidental to his/her job/business travels, socials, and so on);
d) while employed, evaluate his/her performance career development;
e) provide assistance to, and account for, employees in case of emergency; and
f) perform such other processing or disclosure that may be required in the course of the SSCT's operations or under law or regulations.

If the Data Subject is a visitor of SSCT premises or any of its campuses, SSCT may use, collect, or process the Data Subject's Personal Data to:

a) Grant access to the premises; and
b) Maintain the security within the premises.

2.3 Government – Mandated Use. SSCT may use and process the Personal Data of Subjects for government regulatory compliance, reportorial requirements, and pursuant to a lawful order of any court or tribunal.

2.4 Quality. Personal Data processed by SSCT must be accurate and, to the extent necessary, up-to-date. Personal Data that is inaccurate or incomplete shall be corrected, supplemented, and/or erased by SSCT through its Authorized Form, from the Data Subject, provided that such request is not vexatious and/or unreasonable.

SECTION 3. RETENTION

3.1 General. Personal Data should only be stored for as long as necessary to carry out legitimate business operations of SSCT. The purpose/s for which it was collected and processed, as well as the applicable periods prescribed by law, if any, shall be considered in retaining the Personal Data.

The Retention Period for the Personal Data collected and processed shall be as specified in Data Processing Systems.

3.2 Storage. The Personal Data of Data Subjects shall be stored in the pertinent Information and Communications System/s and Filing System/s of SSCT, such as but not limited to, password-protected computer devices, secure filing cabinets, secure filing rooms. Where necessary to further its business and to keep its security software tools up-to-date, SSCT reserves the right to change and/or update its Information Communication System/s and filing System/s.

SECTION 4. DISCLOSURE AND SHARING

4.1 Confidentiality. At every stage of the Data Processing Systems employed by SSCT and even after the termination of the relation of the Data Subject with the college, Authorized Personnel and PIP/s shall maintain the confidentiality and secrecy of Personal Data that come to their knowledge and possession.

4.2 Access and Security Clearance. Only Authorized Personnel and PIP/s are allowed to access and process the Personal Data of the Data Subject. In accessing and processing Personal Data. All Authorized Personnel and PIP/s, as well as employees who request to access Personal Data of Data Subject are enjoined to comply with this Manual.

4.2.1 Exercise of Data Privacy Right. A Data Subject who seeks to access and/or modifies his/her Personal Data with SSCT shall accomplish the Data Privacy Right Form. The Data Privacy Right Form may be filed with the Authorized Personnel previously dealt with by the Data Subject as processor of his/her Personal Data.

4.2.2. Access Request. Any person, including an employee who is not an Authorized Personnel but wishes to access Personal Data of Data Subjects pursuant to his/her function in the college, shall accomplish the Access Request Form, Verbal requests for access shall not be allowed. The Access Request Form may be filed with the Authorized Personnel who has custody of the Personal Data to be accessed. The Authorized Personnel may either approve or reject the same, depending on the merits of the reasons provided for the requested access. In no case shall access be approved if no meritorious reason is provided in the Access Request Form. If approved, the Authorized Personnel shall endorse for final approval the Access Request Form to the DPO or COP if the request happens in other Campuses.

4.2.3 Monitoring. The DPO/COP shall supervise and monitor the implementation of Article IV, Section 4.2.1 and 4.2.2 hereof.

4.2.4 Propriety of Exercise of Right and/or Access Request. In case of doubt on the propriety of the exercise of right and/or access request, as the case may be the COP of other Campuses shall consult and/or seek clearance from the DPO.

4.2.5 Security of Access. Whenever Authorized Personnel and PIP/s of the College obtain access to Personal Data of Data Subjects in the course of their functions in SSCT and/or contractual relations with the College, they shall observe the Security Measures prescribed in this Manual. Anyone with access to Personal Data shall only process the same in accordance with a purpose of the Processing, and may not share, disclose, or distribute the Personal Data unless instructed by SSCT, and with the consent of the Data Subject.

SECTION 5. DISPOSAL

5.1 Schedule. Upon expiration of the Retention Period on the Data Processing Systems, all physical and electronic copies of the Personal Data shall be destroyed

and disposed of using secure means that would render the Personal Data unreadable and irretrievable and prevent the occurrence of any Personal Data Breach and other Security Incidents.

5.2 Procedure. The disposal procedure per Data Processing System shall be as specified Data Processing Systems.

ARTICLE V
SECURITY MEASURES

SSCT shall establish and implement reasonable and appropriate physical, technical, and organizational measures to ensure privacy and data protection. These Security Measures aim to protect Personal Data against natural dangers, such as accidental loss or destruction, and human dangers, such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

The DPO, with the assistance of the COP/s, and the Data Privacy Response Team, shall monitor SSCT's compliance with the security Measures specified in this Article.

SECTION 1. PHYSICAL SECURITY MEASURES

1.1 **Format of Data**. The Personal Data in the custody of SSCT may be in digital/electronic format and/or paper-based/physical format.

1.2 **Storage Type and Location**. All Personal Data being processed by SSCT shall be stored in a secure facility, whether virtual or physical. Papers or physical documents bearing Personal Data shall be stored in locked filing cabinets, access key to which shall be entrusted only to Authorized Personnel. Digital or electronic documents containing Personal Data shall be stored in computers, portable disk, and other devices, provided either the documents or the device where it is stored is protected by password or passcodes. Computers, portable disk, and other devices used by the College and its PIP/s in Processing Personal Data shall be encrypted with the most appropriate encryption standard.

1.3 **Access and Security Clearances**. Only Authorized Personnel and PIP/s may access the Personnel Data stored by SSCT, subjects to the rules prescribed on access in Article IV, Section 4.2 hereof.

1.4 Monitoring of Access. Access of Personal Data by all Authorized Personnel and employees whose request to access Personal Data were Approved pursuant to Article IV, Section 4.2 of this Manual shall be monitored by the DPO/COP concerned. All those who enter and access the Archive Room of SSCT must fill and register in the logbook, which shall indicate the date, time, duration, and purpose of each access.

1.5 Design of Office Space and/or Work Station. Computers shall be positioned with considerable spaces between them to maintain the privacy and protect the Processing of Personal Data. Authorized Personnel shall be assigned to office space

and/or work stations with the least volume of foot traffic to minimize risk of Personal Data Breach and other Security Incident/s.

1.6 Maintenance of Confidentiality. Confidentiality shall be observed and maintained at every stage of the Data Processing System. Employees, whether Authorized Personnel or not, shall not be allowed to bring, connect, and/or use their own gadgets or storage devices of any used for transmitting documents containing Personal Data.

1.7 Modes of Transfer of Personal Data within the Company or to Other Parties. Transfer of Personal Data via electronic mail shall use a secure email facility with the encryption of the data, including any or all attachments.

1.8 Retention and Disposal Procedure. SSCT shall retain Personal Data in its custody following the Retention Period indicated in Data Processing Systems.

SECTION 2. TECHNICAL SECURITY MEASURES

2.1 Monitoring for Security Breaches

2.1.1 SSCT shall cause the monitoring of access to Personal Data so as to minimize the risk of Personal Data Breach and other Security Incident/s. For this purpose, SSCT shall maintain and keep up-to-date its Data Privacy Tracker, which shall contain a log of all privacy-related incident/s, complaint/s and/or request/s from Data Subjects, access request/s.

2.1.2 SSCT shall cause the monitoring of its information and Communications System/s through the employment of File Integrity Monitoring (FIM).

2.1.3 SSCT shall run vulnerability scans periodically, to detect outdated versions of software and misconfigured networks, among others.

2.1.4 SSCT shall regularly read the firewall logs to monitor security breaches and alert itself of any unauthorized attempt to access SSCT network.

2.2 Security Features of Software/s and Application/s Used

2.2.1 SSCT shall procure and install an antivirus software in all College devices where Personal Data are Stored, including tablets and smartphones, that regularly access the Internet. The DPO/COP/s shall ensure that the antivirus software is updated and a system check is done periodically.

2.2.2 SSCT shall use web application firewall to protect its servers and database from malicious online attacks.

2.2.3 To ensure compatibility and data security, the DPO/COP/s shall first ensure that the software applications have been reviewed and evaluated by an Authorized Personnel or PIP/s concerned, if any, before the utilization thereof in College computers and devices

2.3 Regular Assessment and Evaluation of Effectiveness of Security Measures

2.3.1 SSCT, through its Authorized Personnel or PIP/s concerned, shall conduct periodic penetration testing of the firewall appliance from outside the College premises and from within to conduct vulnerability assessment of the same.

2.3.2 If the use of any software application is found to be a security risk such as that it may disturb or interrupt the normal operations of the SSCT's network, the College, through its Authorized Personnel or PIP/s, shall notify the end user of such risk and the software application shall immediately be uninstalled. Such circumstances must be logged, and must be included in the SSCT's Annual Security Incident Report.

2.4 Encryption, Authentication, and Other Technical Security Measures

2.4.1 **Encryption.** As much as possible, Personal Data, most especially Sensitive Personal Data, processed by SSCT shall be encoded into scrambled text using algorithms that render it unreadable unless a cryptographic key is used to convert it.

2.4.2 **Authentication.** Each employee with access to Personal Data shall verify his/her identity using a secure encrypted link and multi-level authentication. passwords or passcodes used to access Personal Data should be of sufficient strength to deter password attacks.

2..4.3 **Other Technical Security Measures.** SSCT shall use such other technical Security Measures to keep its software security tools up-to-date.

SECTION 3. ORGANIZATIONAL SECURITY MEASURES

3.1 Key Personnel. SSCT shall appoint a DPO and/or COP/s in accordance with Article II, Sections 1 and 2 hereof, and shall constitute a Data Privacy Response Team in accordance with Article IV, Section 1 hereof.

3.2. Continuing Education on Data Privacy. All Employees of SSCT shall be required to read this Manual upon employment, and/or upon the effectivity of this Manual, whichever is applicable. All new employees shall be briefed of their obligations under the Data Privacy Act. SSCT shall hold trainings on privacy and date protection at least once a year for employees handling Personal Data. Intra-office memoranda shall be distributed to inform employees of the most current government issuances on data privacy, as well as of any update of this Manual.

3.4 Confidentiality and Data Privacy Protection Clauses and/or Non-Disclosure Agreements. A confidentiality clause sustainability shall be incorporated into the employment contracts of employees, particularly Authorized Personnel. All employees with access to Personal Data shall operate and hold such Personal Data under strict confidentiality, unless the same qualifies as Public Personal Data. This obligation shall apply even after the employee has left SSCT for whatever reasons. Alternatively, a non-disclosure agreement may be executed by the College to protect confidential information and/or Personal Data given to an employee or any other party. Where SSCT has to collect and process the Personal Data of a Data Subject under any contract with such Data Subject, it shall ensure that a Data Privacy Protection Clause

is contained in its contract with such Data Subject. Alternatively, the Company shall require the Data Subject to fill out a Consent Form.

3.5 Institutional Records. Adequate records of SSCT's Personal Data Processing activities shall be maintained at all times. The DPO shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum, general information about the Data Processing Systems of SSCT.

3.6 Review of Data Privacy Manual. This manual shall be reviewed and evaluated annually, Privacy and security policies and practices within SSCT shall be updated to remain consistent with current data privacy best practices.

ARTICLE VI

PERSONAL DATA BREACH AND SECURITY INCIDENTS

SECTION 1. DATA PRIVACY RESPONSE TEAM

A Data Privacy Response Team, consisting of the DPO, and all COPs of SSCT shall be responsible for ensuring immediate action in the event of a Security Incident or Personal Data Breach. SSCT may also designate other key personnel of the college to form part of the Data Privacy Response Team. The DPO shall lead the Data Privacy Response Team.

SECTION 2. DUTIES OF THE DATA PRIVACY RESPONSE TEAM

The Data Privacy Response Team shall, among others:

a) ensure the implementation of this Manual;
b) ensure the management of Security Incidents and Personal Data Breaches, if any:
c) ensure the SSCT's compliance with relevant provisions of the Data Privacy Act, its IRR, and all related government issuances on personal data breach management:
d) assess and evaluate the occurrence of a Security Incident or Personal Data Breach, if any:
e) execute measures to mitigate the adverse effects of any Security Incident or Personal Data Breach, if any: and
f) comply with reporting and notification requirements.

SECTION 3. PREVENTION OF SECURITY INCIDENTS AND PERSONAL DATA BREACH

The Data Privacy Response Team shall periodically conduct a Privacy Impact Assessment to identify risks in the Data Processing Systems. The Data Privacy Response Team shall likewise periodically review the existing policies and procedures of SSCT with regard to data privacy, including this Data Privacy Manual and its implementation.

SECTION 4. PROCEDURE FOR RECOVERY AND RESTORATION OF PERONAL DATA

SSCT shall always maintain a backup file for all Personal Data under its custody. In the event of a Security Incident or Personal Data Breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the Security Incident or Personal Data Breach.

SECTION 5. DOCUMENTATION AND REPORTING PROCEDURE FOR SECURITY INCIDENTS AND/OR PERSONAL DATA BREACH

Within twenty-four (24) hours from the Security Incident or Personal Data Breach, the Data Privacy Response Team shall log every Security Incident encountered into the Data Privacy Tracker to be submitted to the SSCT's Management. The log shall contain the following:

a) description of the nature of the Security Incident or Personal Data Breach, its root cause, chronology of events, estimate of the number of Data Subjects affected, and circumstances regarding its discovery:
b) measures undertaken by the Data Privacy Response Team to address the breach and reduce the harm or its negative consequences:
c) outcome of the breach or incident management, and difficulties encountered;
d) assistance provided or to be provided to the affected Data Subject.

SECTION 6. COMMISSION NOTIFICATION PROTOCOL

6.1 Annual Security Incident Report. The Annual Security Incident Report that must be submitted to the Commission annually shall be prepared by the Data Response Team.

6.2 Mandatory Notification of the Commission. Upon knowledge of, or reasonable belief that a Personal Data Breach has occurred, the Data Privacy Response Team shall notify SSCT's management within twenty-four (24) hours, and the Commission within seventy-two (72) hours, of such occurrence. Notification to the affected Data Subjects should substantially contain the details, while notification to the Commission shall substantially be in the same form.

6.2.1 Conditions. A Personal Data Breach must be reported to the Commission when the following circumstances.

a) There is a breach of Sensitive Personal Information or other Personal Data that may, under the circumstances, be used to enable identity fraud;
b) The Personal Data is reasonably believed to have been acquired by an unauthorized person; and
c) Either SSCT or the Commission believes that the Personal Data Breach is likely to give rise to a real risk of serious harm to the affected Data Subject.

6.2.2 Doubt as to Necessity of Notification. If there is doubt as to whether the Commission has to be notified, the Data Privacy Response Team shall consider the following:

a) The likelihood of harm or negative consequences on the affected Data Subjects;
b) How notification, particularly of the Data Subjects, could reduce the risks arising from the Personal Data Breach reasonably believed to have occurred; and
c) If the Personal Data involved:
   i Information that would likely affect national security, public safety, public order, or public health;
   ii At least one hundred (100) individuals;
   iii Information required by all applicable laws or rules to be confidential; or
   iv Personal Data of vulnerable groups.

ARTICLE V
NOTIFICATIONS, REQUESTS, INQUIRES AND COMPLAINTS

SECTION 1. NOTIFICATION ON USE OF PERSONAL DATA FOR MARKETING AND PROFILING

A Data Subject must be notified within forty-eight (48) hours before entry of his/her Personal Data into the Information and Communications System/s of SSCT, whenever such Personal Data shall be used for direct marketing, profiling, or historical or scientific purpose/s. Notification shall be made through electronic mail to the address of the Data Subject found in SSCT Records.

SECTION 2. REQUESTS AND INQUIRES PERTAINING TO DATA PRIVACY ISSUES

A Data Subject may access and recommend corrections to his/her Personal Data being processed by SSCT by accomplishing the Data Privacy Right Form. Any person, including an employee who is required by his/her functions within the College to access Personal Data of Data subjects, may request access thereto through accomplishment of the Access Request Form.

SECTION 3. PROCEDURE FOR COMPLAINTS

The procedure to be observed in case of complaints for data privacy violation shall be as follows:

(a) Any suspended or actual violation of this Manual, the Data Privacy Act, and/or other government issuances related to data privacy, or any breach, loss, or unauthorized access or disclosure of Personal Data in the possession or under the custody of SSCT must be reported immediately to any member of the Data Privacy Response Team who shall reply within twenty-four (24) hours to acknowledge receipt of the complaint.
(b) In case of complaint for violation of this Data Privacy Act, and/or other government issuances related to data privacy, or any breach, loss or unauthorized access or disclosure of Personal Data in the possession or

under the custody of SSCT, the DPO, the COP, if, any or two (2) members of the Data Privacy Response Team shall:

i. Verify the allegations of the complaint;
ii. If warranted, conduct an official investigation in case of serious security breach as provided under the Data Privacy Act its IRR; and
iii. report the Security Incident or Personal Data Breach to the Commission following the procedure laid down in Article VI, Section 6 of this Manual.

The Data Privacy Response Team may also convene 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 Company or any of its Data Subjects. Such recommendation shall be submitted to the management of SSCT for approval.

ARTICLE VIII

EFFECTIVITY

This Manual was approved by the SSCT Board of Trustees on __ July 2020, and shall take effect immediately.