



ASSCAT **DATA PRIVACY MANUAL**

Notice: Information contained in this document is classified as Agusan del Sur State College of Agriculture and Technology (ASSCAT) exclusive property. No person outside ASSCAT shall have access to the information contained in this document unless the College approves it. Otherwise, it is the responsibility of the person knowing the information contained in this document to ensure its confidentiality of it and to prevent unauthorized access to it.

Uncontrolled copy if printed/photocopied (unless specified otherwise)



AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY



VISION

The globally engaged Institution for sustainable agriculture and innovation.



MISSION

To serve humanity, the Institution will:

Further its excellence and values

Provide quality and inclusive instruction

Undertake vibrant research and innovation; and

Pursue responsive community services for sustainable development.



PHILOSOPHY

ASSCAT believes that the Higher Education should be anchored to the tenets of democracy; be guided by the continuing pursuit for relevance and excellence and; the mover and catalyst for development.

CORE VALUES





DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 2 of 20

TABLE OF CONTENTS

Contents	Page
Vision, Mission, Philosophy, and Core Values	1
I. INTRODUCTION	4
II. GENERAL DATA PRIVACY	4
III. DEFINITION OF TERMS	5
IV. SCOPE AND LIMITATIONS	7
V. PROCESSING OF PERSONAL DATA	7
1. GUIDELINES FOR PROCESSING OF DATA	7
A. Notification and Consent	7
B. Access of Authorized Personnel	8
2. COLLECTION OF PERSONAL INFORMATION	8
A. Types of Personal Information Collected	8
B. Provision for Specific Departments	9
Admission Office	9
Registrar's Office	9
Wellness and Health Clinic	10
Human Resource Management Office	10
Digital Transformation Center (DTC) Office	10
Other Offices	10
VI. ACCURACY OF INFORMATION	11
A. Verification of Personal Information	11
B. Correction or Update of Personal Information	11
VII. DISCLOSURE OF PERSONAL INFORMATION	11
A. Confidentiality	12
B. Internal Data Sharing	12
C. External Data Sharing	12
VIII. SECURITY OF PERSONAL INFORMATION	12
A. Organizational Measures	12
B. Physical Security Measures	14
C. Technical Security Measures	15
IX. BREACH AND SECURITY INCIDENTS	16
A. Creation of a Data Breach Response Team or Computer Emergency Response Team (CERT)	16
B. Incident Response Procedure	16
C. Notification Protocol	17
D. Documentation and Reporting	17
X. INQUIRY AND COMPLAINTS	18



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 3 of 20

XI. PRIVACY IMPACT ASSESSMENTS	18
XII. EFFECTIVITY	19
XIII. REFERENCES	19
XIV. ANNEXES	19





DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 4 of 20

I. INTRODUCTION

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act (DPA) of 2012, its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission.

It is the policy of Agusan del Sur State College of Agriculture and Technology (ASSCAT) to uphold data privacy rights and to ensure that all personal data collected from the students, alumni, providers, third parties, clients and customers, are processed in accordance to the general principles of transparency, legitimate purpose, and proportionality, while also enforcing stringent data security measures outlined in the DPA.

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

II. GENERAL DATA PRIVACY PRINCIPLES

ASSCAT adheres to process personal data in compliance with the requirements of the Data Privacy Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.

- a. **Transparency** - the data subject must be aware of the nature, purpose, and extent of the processing of his or her data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
- 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 information shall be adequate, relevant, suitable, necessary, and not excessive concerning a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.



III. DEFINITION OF TERMS

1. **Act** - refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012.
2. **ASSCAT** - refers to Agusan del Sur State College of Agriculture and Technology.
3. **Consent of the data subject** - refers to any freely given, specific, informed indication of will, whereby the data subject agrees to collect and process his or her personal, sensitive, or privileged information. The consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.
4. **Data subject** - refers to an individual whose personal, sensitive personal, or privileged information is processed.
5. **Data Privacy Officer or DPO** - spearhead the overall implementation and policies in protecting the personal information collected, stored and processed by ASSCAT as mandated by the Data Privacy Law.
6. **Data Privacy Response Team** - is a specialized group within the institution tasked with swiftly addressing and managing data privacy incidents and breaches.
7. **Data sharing** - the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controller/s.
8. **Personal Data** - refers to all types of personal information and sensitive personal information collected by ASSCAT.
9. **Personal data breach** - refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
10. **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.
11. **Personal Information Controller or PIC** refers to ASSCAT as the entity which controls personal data processing or instructs another to process personal data on its behalf.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 6 of 20

12. **Personal Information Processor or PIP**- refers to personnel within ASSCAT designated by a personal information controller to handle the processing of a personal data concerning a data subject.
13. **Privacy Impact Assessment or PIA**- refers to the process undertaken and used to evaluate and manage the impacts on the privacy of ASSCAT programs, projects, processes, measures, systems, or technology products. Such a process takes into account the nature of the personal data to be protected, the personal data flow. The risks to privacy and security posed by the processing, current data best practices, cost of security implementation, and where applicable, the size of the organization, its resources and complexity of operations.
14. **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.
15. **Privileged information** - refers to any form of data, which, under the Rules of Court and other pertinent laws constitutes privileged communication.
16. **Public authority** - refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions.
17. **Security incident** - an event or occurrence that affects or tends to affect data protection, or may compromise personal data's availability, integrity and confidentiality. It includes incidents that would result in a personal data breach, if not for safeguards that have been put in place;
18. **Sensitive personal information** - refers to personal information:
 - a. About an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations;
 - b. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence 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



AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- d. Specifically established by an executive order or an act of Congress to be kept classified.

19. **School Records** – refers to the records of the students of all acts, events, accomplishments, research and all documents from various activities. This includes but is not limited to the following:

- a. Personal and academic records of the students
- b. Birth Certificates
- c. Academic Reports
- d. Medical and Guidance Records
- e. Academic Financial Records

IV. SCOPE AND LIMITATIONS

This Manual applies to all personnel of ASSCAT, regardless of the type of employment or contractual arrangement, students, third parties, and administrators whose information or records must be kept and secured by ASSCAT. The data covered by this Manual is limited to personal information defined in this manual, collected and processed by ASSCAT.

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

V. PROCESSING OF PERSONAL DATA

1. GUIDELINES FOR PROCESSING OF DATA

To ensure that the rights of the data subjects are protected, all ASSCAT offices and Units are subject to the following policies:

a. Notification and Consent

Information will be collected only upon notification and with the consent of the Data Subjects (Students, Employees, and other parties). Consent may be in the form of physical forms validated and signed informing the data subject about the following:

- 1. Description of the personal information to be entered into the system;
- 2. Purposes for which they are being or are to be processed;
- 3. Scope and method of the personal information processing;
- 4. The recipients or classes of recipients to whom they are or may be disclosed;



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 8 of 20

5. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
6. The identity and contact details of the personal information controller or DPO;
7. The period for which the information will be stored; and
8. The existence of their rights, i.e., to access, correction, as well as the right to complain to the Commission.

b. Access of Authorized Personnel

Only authorized personnel can access and allowed to process the personal information collected from the students, employees, and other parties in accordance with the data privacy policy of ASSCAT.

Authorized personnel shall collect personal information which is reasonably necessary or directly related to the functions or activities of the institution. Personal Information shall not be collected in anticipation that it may be useful in the future.

The physical records or those which are not digital stored and secured in the database are stored in a safe and secured place at ASSCAT. Access is restricted, allowing retrieval solely upon explicit instructions from the office head for legitimate purposes and in accordance with the policies and procedures implemented by ASSCAT.

2. COLLECTION OF PERSONAL INFORMATION

A. Types of Personal Information Collected

The ASSCAT Personnel collects and processes only the type of personal information necessary to accomplish its core and auxiliary functions. ASSCAT operates its functions in Administration and Resource Generation, Academe-Industry Convergence, Student Affairs and Services, Research for Development and Extension, Innovation and Entrepreneurship, and Teaching and Learning and Faculty Development. Below is the common list of personal information that ASSCAT may collect from its customers.

1. Employees' personal information as required in the Personal Data Sheet provided by the Civil Service Commission.
2. Employees' academic information
3. Employees' work experience information
4. Financial Information



AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

5. Customer, Third-parties, Suppliers and other linkages' personal information
6. Students' personal information
 - Full name, gender, address, previous academic report card, birthdate, contact number, guardian's name, address and contact number, nationality, picture
7. Students' academic information
 - Grades, subjects, scholastic performance, faculty evaluation, academic program evaluation result
8. Adopted Barangays and Extension Activities information
 - Full name, age, gender, contact number, address
9. Visitors' personal information
 - Full name, contact number, address, identification card
10. Images for ID and via recording devices
11. Internet Protocol (IP) addresses
12. Alumni's personal information and current employment information

B. Provision for Specific Departments

Office of Student

The Office of Students Affairs and Services particularly the Admission Services collects the applicants' personal information to evaluate the eligibility of their submitted academic records for enrollment.

Registrar's Office

The Registrar's Office collects the academic report cards, and authenticated birth certificates of the students. The office also generated and released the students' academic reports during their entire duration in ASSCAT. These documents are processed and will be submitted to the Commission on Higher Education for compliance with the CHED Memorandum Order No. 30, series of 2009.

Wellness and Health Clinic

This office collects sensitive information relating to the medical condition and assessments of the students and employees of ASSCAT for health monitoring under its mandated function. Access to sensitive data is restricted only to the office's physician/doctor, dentist, nurse and staff. Disclosure of this



AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

information may not be released without the consent of the student or employee or authorized representative unless in some cases the life of the student or employee is at stake.

Human Resource Management Office

This office collects the personal information of the applicants and employees for evaluation of their eligibility, performance, benefits and the individual 201 files of the employees which are required by the Civil Service Commission. Personnel's personal information is confidential and restricted to authorized personnel only.

Digital Transformation Center (DTC) Office

The DTC Office is responsible for providing automated information systems to the different offices that collect and process personal information for its clients. The Admission, Registrar, Human Resource Management, Finance, Supply and Procurement Offices are the common offices that have Information Systems. The information gathered is then processed, stored and secured in the central data center of the College to maintain its confidentiality, integrity and accessibility.

Access to confidential information is restricted to authorized personnel according to their function. The customers, students, employees, applicants and other types of registered users have accessibility and can download their information in pdf or any format provided in the system.

Other Offices

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





DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 11 of 20

VI. ACCURACY OF INFORMATION

A. Verification of Personal Information

Whenever possible, the data entry must be done by the data subject to eliminate erroneous data gathering. Only official channels and systems shall be used in storing personal information and must only be conducted by officially designated personnel of a particular college or office.

The collected personal information from the clients, students, employees, applicants and third-parties are subject to verification for its eligibility and accuracy before processing.

For the manual collection of data, the form must be properly printed and elaborated by ASSCAT Personnel, if possible, provide a sample to eliminate erroneous entries. If data are gathered using automated information systems, they must provide clear instructions, formatting, validation, and proper algorithm to verify the accuracy of data.

B. Correction or update of Personal Information

Registered clients, students, employees, applicants and third parties may directly update their personal information in the information systems provided by DTC Office. ASSCAT Students and Employees are using Google Workspace for Education as their institutional account provided by the DTC office. Users may message the ASSCAT MIS Facebook Page or directly call the office for any issues and concerns about their user account.

VII. DISCLOSURE OF PERSONAL INFORMATION

All ASSCAT personnel and employees must exercise due diligence and utmost care in handling personal information. ASSCAT shall refrain from sharing or disclosing data to third parties without prior consent from the data subjects. In cases where data disclosure is essential and permitted, ASSCAT shall diligently review the privacy and security policies of authorized third-party service providers or external partners. Any disclosure of data by ASSCAT is made in compliance with legal or regulatory obligations when necessary.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 12 of 20

a. Confidentiality

Following an employee's contract termination with ASSCAT, it is imperative for them to uphold the confidentiality and secrecy of all personal information they have accessed. This obligation also extends to students, alumni, or any other individual officially authorized by ASSCAT to collect and process personal information for legitimate purposes (e.g., student council, campus organizations, etc.).

b. Internal Data Sharing

Internal sharing of personal information between ASSCAT offices, departments and units must adhere to a standardized data request procedure. This process guarantees that data is transmitted through official channels for valid purposes. The data request form, to be used in such procedure shall include details about the requesting entity, the data required, justification for the request, along with the date and signature of the requesting individual.

c. External Data Sharing

External data sharing shall only be allowed when it is expressly authorized by law and/or with the data subject's consent. In these instances, a Data Sharing Agreement is essential, to clearly specify the precise scope and manner of personal information disclosure while enforcing adequate safeguards. When engaging in partnerships or initiatives that involves sharing personal information, establish a clear Data Sharing Agreement approved by all involved parties. Prior to any external data exchange, ASSCAT will ensure strict compliance with the Data Privacy Act and related regulations.

VIII. SECURITY OF PERSONAL INFORMATION

The Agusan del Sur State College of Agriculture and Technology (ASSCAT) shall implement security measures to maintain the availability, integrity, and confidentiality of personal data collected from the data subjects.

A. Organizational Measures

1. The management appoints a Data Privacy Officer (DPO) to spearhead the overall implementation and policies in protecting the personal information collected, stored and processed by ASSCAT as mandated by the Data Privacy Law.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 13 of 20

The following are the roles and responsibilities of a Data Privacy Officer:

- 1.1 Monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, DPO may:
 - a. collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
 - b. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
 - c. inform, advise, and issue recommendations to the PIC or PIP;
 - d. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
 - e. advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensuring its compliance with the law;
- 1.2 Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- 1.3 Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- 1.4 Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- 1.5 Inform and cultivate awareness of privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
2. Creation of a Data Privacy Focal Person to support the DPO in the implementation of data privacy protection policies in the assigned office. They are responsible to monitor, mitigate and implement security measures in their respective offices.
3. Create an Information Security Incident Response Team to respond to data breaches and privacy complaints.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 14 of 20

4. Conduct Data Capacity Building Seminars/Webinars for all academic and administrative personnel to understand the requirements and their responsibilities in the Data Privacy Act, its IRR, issuances of the National Privacy Commission, and other related laws and issuances of data privacy and security.
5. Conduct a Privacy Impact Assessment of all information systems in the college and manual processes that collect personal information. Evaluate the security measurements the Information and Communications Office implemented to the current security vulnerabilities. Evaluate the current process for collecting information to prevent possible threats and propose security measures to address privacy risks.
6. All employees are required to sign a non-disclosure agreement. All employees, regardless of status, who have access to personal data must handle and maintain such information under strict confidentiality unless the data is intended for public disclosure.

B. Physical Security Measures

1. Firewall devices and information security policies are implemented in the ASSCAT Data Center.
2. Physical access to the ASSCAT Data Center is highly restricted to authorized personnel only. Door lock systems are installed for access control.
3. 24/7 security monitoring and CCTVs are provided to secure the Data Center.
4. Computers are properly positioned to maintain privacy and protect the processing of personal information.
5. Collection and processing of Personal Information may be in paper-based or digital/electronic format. All personal data processed in paper-based format are stored in locked filing cabinets or designated storage facilities, under the control of the Directors and heads of each unit. Files stored are categorized and properly filed by the PIPs. Sharing and disclosing personal information or any document from the storage facility must abide by the records transfer policy and the Data Privacy Act. On the other hand, digital/electronic files are stored and protected in a Data Center, Google Workspace, or cloud-based storage managed by ASSCAT.
6. Authorized ASSCAT employees with access to personal information and restricted facilities must adhere to privacy and protection protocols. They are required to log the date, time, duration, and purpose of each access.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 15 of 20

C. Technical Security Measures

1. Daily backup activities are implemented to secure copies of databases and virtual machines in case of hardware failure and data loss.
2. Information Systems are the common tools used for collecting personal information. The use of Google Authentication using the user's institutional accounts for data privacy and security is required for all systems. Hence, force enrollment to 2-Step Verification to all institutional accounts is implemented by the DTC Office.
3. Viewing of personal information of the data subjects is restricted to authorized personnel only. Information Systems are governed by the end-users as the system admin. Access to information systems is revoked for inactive employees.
4. Security policies must be evaluated and updated regularly.
5. Information Systems used for data collection and processing must have vulnerability assessments and perform penetration testing before deployment.
6. Whenever applicable, the DTC personnel shall evaluate the software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.
7. Clean Desk and Clear Screen Guidelines
 - a. Enable a password-protected screen saver.
 - b. Log off the computer when not in the workspace.
 - c. Log off and/or lock the computer at the end of the workday.
 - d. To prevent shoulder surfing, position the computer screen to protect the confidentiality of the Information. If moving the monitor is not possible, consider using a privacy screen or filter.
 - e. Lock the portable computing devices (e.g., laptops, tablets) in a drawer or cabinet when not at the workspace or at the end of the workday.
 - f. Secure portable media (e.g., CDs, DVDs, unencrypted USB or external drives) containing sensitive information with encryption or store the media in a secure location (i.e., locked drawer, locked cabinet).
 - g. Notify the IT Support technician and Information Unit immediately if any desktop, laptop, tablet, and/or portable media containing ASSCAT Protected or ASSCAT Sensitive information is missing.



AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

- h. Do not leave paper containing ASSCAT Protected Data and ASSCAT Sensitive Data unattended on your desk, especially if you are going to be away from your desk for an extended period.
- i. Do not leave cabinet or office keys in their locks.
- j. Do not leave keys used to access ASSCAT Protected Data or ASSCAT Sensitive Data at an unattended desk.
- k. Notify Security Services immediately if your access card or keys are missing.
- l. At the end of the working day, you should tidy your desk, put away all paper that contains ASSCAT Protected Data or ASSCAT Sensitive Data, and lock your office or drawers.
- m. Never write down passwords.
- n. Do not leave printouts on printers unattended.
- o. Shred sensitive documents when they are no longer required.

IX. BREACH AND SECURITY INCIDENTS

a. Creation of a Data Breach Response Team or Computer Emergency Response Team (CERT)

The CERT, comprised of the Supervisor as the Data Privacy Officer, the Chief Information Security Officer (CISO) as the Team Leader, the Analysts, Point of Contact (POC), and the Internal Auditor, operates under the direct supervision of the College President as the Personal Information Controller. The team is responsible for taking immediate action during a security incident or Personal Information breach. They assess and evaluate security incidents and take specific actions to restore integrity to the communications systems, mitigate and remedy resulting damages, and comply with reportorial requirements.

b. Incident Response Procedure

Any suspected data breach must be communicated to the Data Breach Response Team. The report may come from Firewalls, Students, Employees or external security agencies. The Data Breach Response Team shall conduct of Privacy Impact Assessment as needed to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. The team shall execute measures based on the conducted Privacy Impact Assessment to mitigate the adverse effects of the incidents.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 17 of 20

The general steps to mitigate the incident, irrespective of its type, are as follows:

1. **Containment** - limit the damage of security breaches and involve the affected personnel to resolve the issues. Perform necessary technical controls such as security forensic analysis if necessary.
2. **Remediation** - remove the cause and repair the security vulnerabilities that resulted in the security incident.
3. **Recovery** – restore backup configuration for network devices, firewalls, computer servers, virtual machines, databases, and other peripherals to recover the affected files
4. **Post-Incident Remediation** - conduct root cause analysis and prepare an action plan for the recommended changes to improve the security policies and controls in the institution.

The detailed incident procedure is specified in the Computer Emergency Response Team Manual.

c. **Notification Protocol**

The DPO shall report the data breach details to the National Privacy Commission (NPC), including the data subjects affected within 72 hours of knowledge thereof.

d. **Documentation and Reporting**

The Data Breach Response Team shall document details and actions taken of all the data breach incidents as well as the annual report to be submitted to the Vice President for Academic and Quality Assurance, the College President, and the NPC within the prescribed period. The reports should include the following:

1. Description of the personal data breach, its root cause, and circumstances regarding its discovery;
2. Actions and decisions of the incident response team;
3. Outcome of the breach management, and difficulties encountered; and
4. Compliance with notification requirements and assistance provided to affected data subjects



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 18 of 20

X. INQUIRY AND COMPLAINTS

Data subjects may inquire or file complaints regarding any matter relating to the processing of their personal information under the custody of ASSCAT, including the data privacy and security policies implemented to ensure the protection of their data. They may write to the ASSCAT Data Privacy Officer at dpo@asscat.edu.ph and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or emailed to dpo@asscat.edu.ph. The DPO shall coordinate with the Data Privacy Focal Person of the concerned unit to address the issue and shall liaise with all necessary third parties, including dealing with the complainant.

XI. PRIVACY IMPACT ASSESSMENTS

To assess the potential impacts on the privacy of a process, information system, program, software module, device or another initiative which processes personal information and in consultation with stakeholders of ASSCAT, privacy impact assessment shall be periodically conducted for taking actions as necessary to prevent and treat privacy risk.

The privacy impact assessment shall include the following activities in ASSCAT:

1. Description of the program, project, process, system or technology product and its context.
2. Assessment of the adherence by the PIC or PIP to the data privacy principles, the implementation of security measures, and the provision of mechanisms for the exercise by data subjects of their rights under the DPA.
3. Identifies and evaluates the risks posed by a data processing system to the rights and freedoms of affected data subjects, and proposes measures that address them.

The privacy impact assessment shall be evaluated by the DPO and shall be submitted to the College President for approval.



DATA PRIVACY MANUAL

AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY

Page 19 of 20

XII. EFFECTIVITY



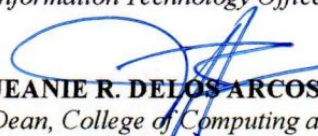

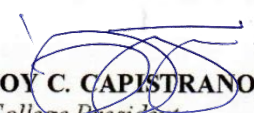
The provisions of this Manual are effective—upon approval by the ASSCAT Board of Trustees.

XIII. REFERENCES

1. Republic Act No. 10173
2. Implementing Rules and Regulations of RA 10173

XIV. ANNEXES

- Annex A – Privacy Impact Assessment Report
- Computer Emergency Response Team Manual
- Information Security Policies

Jointly Prepared by:	Reviewed by:	Approved by:
 Atty. SHIELA T. DELA VICTORIA <i>Data Protection Officer</i>  IRENE C. BALUIS <i>Information Technology Officer I</i>  JEANIE R. DELOS ARCOS, DIT <i>Dean, College of Computing and Sciences</i>	 CARMELO S. LLANTO, Ph.D. <i>Vice-President for Academic and Quality Assurance</i>	 JOY C. CAPISTRANO, Ph.D. <i>College President</i>
Date: <i>July 23, 2024</i>	Date: <i>August 06, 2024</i>	Date: <i>August 06, 2024</i>