



TANGENT SOLUTIONS, INC.

DATA PRIVACY POLICIES AND PROCEDURES

Policy Manual (PLM)

CORPORATE COMMUNICATIONS, INTERNAL AUDIT,
RISK MANAGEMENT AND COMPLIANCE OFFICE [CCIARCO]

EOD-CCIARCO-PLM-037-V2.0
REV. NO. 2.0 [01 JANUARY 2025]

This document is **Proprietary** and **Confidential**.

I. INTRODUCTION

A. Purpose

The purpose of this Data Privacy Policies and Procedures is to ensure that the organization protects data subjects’ personal data physically, organizationally, and technologically. This policy demonstrates Tangent’s commitment to collect, process and store personal data in accordance with the Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations [IRR], and other relevant policies, including issuances of the National Privacy Commission [NPC].

This policy explains how Tangent seeks to adhere to the general privacy principles of transparency, legitimate purpose, and proportionality to safeguarding personal data, fostering trust among customers, partners, and employees.

B. Scope and Coverage

The scope of this policy covers all types of personal data and to any natural or juridical person involved in personal data processing.

Data Subject			
Employees	Customers	Partners	Stockholders
organic agency personnel contractors/consultants applicants previous employees	individual corporate prospects	vendors/suppliers third-party service providers visitors	Past and Present: Shareholders Board of Directors

This policy defines the range and boundaries of these policies within the organization. It outlines what data, processes, systems, and personnel are covered, as well as the extent of compliance requirements.

This encompasses the following:

Data Types	covers all categories of data that the organization collects, processes, or stores, including personal data [such as names, addresses, financial information] and sensitive information [like health data, social security numbers, biometric data].
Data Processing Activities	encompasses all actions taken on data, such as collection, storage, use, sharing, and disposal. It also addresses data transfers within and outside the organization, particularly to third parties or affiliates.
Systems and Technology	identifies the platforms, applications, databases, and devices involved in data processing, including cloud services, POS systems, mobile devices, and employee laptops.
Third-Party Interactions	outlines the handling of data shared with vendors, partners, and service providers, along with the organization's policies for ensuring third parties also comply with data privacy requirements.

C. Definition of Terms

1. **Data Subject.** Includes the individuals whose data [personal, sensitive personal, or privileged information] is being processed, such as customers, employees, contractors, and third parties. This could also extend to any individual whose data might be indirectly gathered or stored by the organization.
2. **Personal Data.** Any data that makes it possible to recognize or distinguish one person from another.
3. **Personal Information [PI].** Any regular information that identifies or can identify an individual.
4. **Sensitive Personal Information [SPI].** Refers to personal data that includes highly confidential information with greater risks to individuals should their data be disclosed which requires stricter handling and protection measures.
5. **Privileged Information [PRI].** Refers to all forms of data that constitute privileged communication under the Rules of Court e.g. communication between a client and his/her lawyer, penitent and priest, patient and doctor.
6. **Personal Information Controller or PIC.** Refers to the organization or individual which controls of the processing of personal data or instructs another to process personal data on its behalf.
7. **Personal Information Processor or PIP.** Refers to the organization or individual that processes personal data on behalf of the data controller, typically a third-party service provider. Data processors must follow the instructions of the data controller.
8. **Person.** Any natural or juridical person.
9. **Consent.** The explicit, informed, and voluntary agreement from a data subject allowing the collection and processing of their personal data. Consent must be specific, informed, and revocable.
10. **Privacy Notice.** A statement provided to data subjects that explains how their personal data is collected, used, shared, and protected. Privacy notices are often legally required and aim to foster transparency.

II. GOVERNANCE AND ACCOUNTABILITY

A. Data Protection Officer [DPO]

Responsibilities	<ul style="list-style-type: none">• Monitor the PIC/PIP compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies.• Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC/PIP.• Advise the PIC/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.• Ensure proper data breach and security incident management by the PIC/PIP, including the preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period.• Inform and cultivate awareness on privacy and data protection within the organization, including all relevant laws, rules and regulations and issuances of the NPC.• Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC/PIP relating to privacy and data protection, by adopting a privacy by design approach.• Serve as a contact person of the PIC/PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC/PIP.• Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security.• Perform other duties and tasks that may be assigned by the PIC/PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.
Qualifications	<ul style="list-style-type: none">• DPO shall possess specialized knowledge and demonstrate reliability necessary for the performance of his/her duties and responsibilities.• DPO should have expertise in relevant privacy or data protection policies and practices.• DPO should have sufficient understanding of the processing operations being carried out by the PIC or PIP, including the latter's information systems, data security, and/or data protection needs.
Contact Information	<p>Name: Kaye P. Alagao Email : dpo@tangentsolutionsinc.com Mobile No.: 0917-113-0801 Address: 15/F Suite 1507-A Tektite East Tower, Exchange Road, Ortigas Center, Pasig City 1605 Philippines</p>

B. Privacy Management Framework

Privacy by Design is a concept where privacy management cannot be assured only by compliance with regulatory requirements but a default mode of operation to assure personal data are protected. Privacy considerations is proactively considered and prioritized throughout the entire lifecycle of a project or system, operation, and management.

Planning	Privacy is an integral, embedded consideration when developing any priorities, activities, initiatives and operations.
Security and Control	Reasonable security and privacy protection measures are developed and implemented to prevent and/or mitigate the unauthorized collection, access, use, disclosure, and destruction of personal data.
Openness	Information pertaining to privacy management and how personal data is collected, accessed, used, disclosed and destroyed must be readily available to data subjects.
Accountability	Governance must be in place to ensure personal data is protected.

C. Roles and Responsibilities

Management	
By integrating these steps into the operations, management can ensure that the organization not only complies with the DPA but also established a robust foundation for protecting personal data	
<ul style="list-style-type: none"> Establish governance and leadership Develop and implement policies Conduct regular risk assessments Implement security measures Provide training and awareness Monitor third-party compliance 	<ul style="list-style-type: none"> Create data inventory and processing record Enable data subject rights Develop an incident response plan Monitor and audit compliance Engage with regulatory authorities Promote continuous improvement
Employees	
By adhering to these practices, employees actively contribute to the organization's compliance with the DPA and the broader goal of protecting personal data.	
<ul style="list-style-type: none"> Understand and follow policies Handle personal data responsibly Protect data security Be cautious with data sharing Report incidents promptly Respect data subject rights 	<ul style="list-style-type: none"> Avoid risky practices Attend training and stay informed Practice data minimization Maintain confidentiality Securely manage data Be vigilant
Third Parties	
By adhering to these practices, third parties ensure compliance with the DPA while contributing to the overall security and privacy posture of the organizations they serve.	
<ul style="list-style-type: none"> Understand legal and contractual obligations Establish privacy policies and procedures Appoint a Data Privacy contact Limit data use to authorized purposes Implement security measures Maintain confidentiality Perform risk assessments 	<ul style="list-style-type: none"> Support data subject rights Monitor and audit data handling Handle data breaches responsibly Ensure subprocessor compliance Retain and dispose of data securely Stay updated

III. DATA PRIVACY PRINCIPLES

The processing of personal data and shall be allowed, in accordance with the requirements of the DPA of 2012 and other laws allowing disclosure of information and in 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 personal data, including the risks and safeguard involved, the identity of PIC, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to processing of personal data should be easy to access and understand, using clear and plain language. The following are its core elements:

Clear Communication	Provide clear, concise, and accessible information about data practices in privacy policies, terms of services, and consent forms.
Purpose Specification	Clearly explain why personal data is being collected and how it will be used.
Consent Management	Obtain informed consent, ensuring data subjects understand what they are agreeing to and providing them with the ability to opt-out or revoke consent easily.
Data Sharing Disclosure	Clearly state if data will be shared with third parties and for what purpose, including any international data transfers.
User Rights Information	Inform data subjects of their rights, such as the right to access, correct, delete, or restrict processing of their data.
Regular Updates	Keep privacy policies updated and notify users of any significant changes in data handling practices.

B. Legitimate Purpose

Personal data must be collected and processed only for lawful, specific, and clearly defined purposes. The following are its core elements:

Lawful Basis	Ensure that data collection and processing are based on a valid legal ground, such as: [a] Consent: The data subject has given clear consent [b] Contractual necessity: Data is required to fulfill a contract. [c] Legal obligation: Processing is necessary to comply with the law. [d] Legitimate interests: The organization's interests do not override the data subject's rights and freedom.
Purpose Specification	Clearly define the purpose of data processing at the time of collection, ensuring it is: [a] Specific: Focused and well-defined [b] Explicit: Clearly communicated to the data subject [c] Legitimate: Compliant with applicable laws and regulations.
Purpose Limitation	Data should only be used for the original purpose unless further processing is compatible with that purpose, or the data subject provides additional consent.
Transparency and Accountability	Inform data subjects about the purpose of data processing in privacy policies or consent forms and demonstrate compliance through records and audits.

C. Proportionality

The amount and type of personal data collected must be adequate, relevant, and limited to what is necessary for the intended purpose. The following are its core elements:

Data Minimization	Collect only the data strictly necessary for the specific purpose. Avoid excessive or irrelevant data collection.
Purpose Limitation	Use the data only for the stated purpose and ensure any further processing is necessary and justified.
Balanced Approach	Ensure that the benefits of processing the data outweigh any potential risks to data subject's privacy. Avoid intrusive or unnecessary data practices.
Retention Limitation	Retain personal data only for as long as necessary to fulfill the purpose. Implement clear data retention and deletion policies.

IV. DATA COLLECTION, PROCESSING, AND STORAGE

A. Data Collection and Consent Management

Collection of information is done with the consent of Data Subjects which consent is included in the forms filled out. Employees are also asked to sign the Data Privacy Consent and Agreement during their onboarding period ensuring that they are informed about why their data is and will be collected, how it will be used, and who will have access to it.

- a. Notify data subjects of data collection purposes and obtain explicit consent if required.
- b. Provide a privacy notice that details data usage, storage, and sharing practices.
 - i. When to Provide a Privacy Notice

A privacy notice must be provided at the time the data is obtained from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, but not later than 24 hours from obtaining the data. The privacy notice must be provided at the latest when the first communication takes place. If disclosure to another recipient is expected, then the privacy notice must be provided to the data being disclosed.

- ii. What to Include in a Privacy Notice

Privacy notices must be concise, transparent, intelligible, conspicuous and easily accessible. They are provided free of charge and must be written in clear and plain language.

- c. Document and maintain records of consent.

B. Data Processing Guidelines

Processing means any activity pertaining to the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data.

1. Data Storage

These guidelines outline the proper methods and locations for storing data securely.

When data is stored on paper, it should be kept in a secure location where it is not visible to unauthorized individuals. These guidelines also apply to data that is normally stored electronically but has been printed out:

- a. When not in use, paper or files should be kept in a locked drawer or filing cabinet.
- b. Employees should ensure that paper and printouts are not left in areas where unauthorized individuals could see them, such as on a printer.
- c. When no longer needed, data printouts should be shredded and disposed of securely.

To protect electronic data from unauthorized access, accidental deletion, and malicious hacking attempts, the following measures must be taken:

- i. Data should be protected with strong passwords that are changed regularly and never shared among employees.
- ii. If data is stored on removable media [such as USBs or hard disks or DVDs], these should be kept locked in a secure location when not in use.
- iii. Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- iv. Servers containing personal data should be in a secure location, separate from general office space.
- v. Data should be backed up frequently and those backups should be tested regularly according to the standard backup procedures.
- vi. Data should never be saved directly to laptops or other mobile devices such as tablets or smartphones.
- vii. All servers and computers containing data should be protected with approved security software and a firewall.

2. Data Processing

- a. The data subject has provided explicit consent for the processing of personal data.
- b. Processing pertains to personal data that has been clearly made public by the data subject.
- c. Processing is necessary for fulfilling obligations and exercising specific rights of the controller or data subject in the fields of employment, social security, etc.
- d. To protect the vital interests of the data subject or another natural person when the data subject is unable to give consent due to physical or legal incapacity.

3. Data Access

a. Onsite and Online Access

- i. No employee of Tangent shall have access to sensitive personal information on company property or through online facilities unless the employee has received a security clearance from the head of the department.
- ii. A head of the department shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online access.
- iii. The online access allowed shall be subject to the following conditions:
 - o An IT governance framework has been designed and implemented.
 - o Sufficient organizational, physical and technical security measures have been established.
 - o The company can protect SPI in accordance with data privacy practices and standards recognized by the information and communication technology industry.
 - o The employee is only given online access to SPI necessary for the performance of official functions.

b. Offsite Access

- i. A request for such transportation or access shall be submitted to and approved by the department head. The request must include proper accountability mechanisms in the processing of data.
- ii. Where a request is approved, the department head shall limit the access to not more than one thousand [1,000] records at a time.
- iii. Any technology used to store, transport or access SPI for purposes of offsite access, shall be secured using the most secure encryption standard recognized by NPC.

4. Data Use

Tangent uses personal data collected for purposes of the following:

- a. Complying with the laws, rules and regulations
- b. For purposes of its operations as POS terminal services provider
- c. For documentation processes

C. Data Retention and Disposal

To ensure fair processing, personal data will not be retained by Tangent for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which Tangent services need to retain personal data is set out based on identified retention period. This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

1. Unauthorized destruction should be reported to the DPO pursuant to the procedure.
2. Personal data must be retained safely for the purposes of evidence or where retention is mandated by any law or where such personal data is subject to a civil or criminal investigation.

Type of Data	Personal Data Type	Retention Period
Personal Data	Personal Data	5 years after resignation date
CCTV	Footage	90 days to 1 year
Visitor's Log	Personal Data	1 year following visit
Financial Records	Tax Regulations	5 years
Emails and Viber Group	Operational Messages	1 year or shorter
Phone Conversations	Operational Messages	1 year or shorter
Emails and Viber Group	Complaints/Legal Issues	3 years
Employee Records	Contracts, Performance Reports, Disciplinary Records	5 years following resignation date

V. DATA SUBJECT RIGHTS

A. Right to be Informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, conspicuous, free of charge, that are written in clear and plain language.
- Keeping a record of how Tangent uses personal data to demonstrate compliance with the need for accountability and transparency.

B. Right to Access

- Enabling data subjects and their authorized person to access their data.
- Allowing clients to be aware of and verify the data protection policy of the processing activities.

C. Right to Rectification [if data is being maintained by Tangent]

- Tangent must rectify or amend the data of the data subject if requested in the event it is inaccurate or incomplete as reported by data subject.
- This can be with permission from the Data Protection Officer [DPO].

D. Right to Erasure/Removal/Blocking

- Tangent has a right to have its data erased and for processing to cease in the following circumstances:
 - i. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed.
 - ii. Where consent of data subject is withdrawn.
 - iii. Where the data subject objects to processing and there is no overriding legitimate interest for continuing the processing.
 - iv. Where the personal data was unlawfully processed or otherwise in breach of data protection laws.
 - v. To comply with a legal obligation.

E. Right to Data Portability [if only requested by the data owner]

- Tangent must provide data subject with their data so that they can reuse it for their own purposes or across different services upon authorization by parties involved.
- Tangent must provide it in a commonly used, machine-readable format, and send it directly to the requested party only.
- Tangent should only provide data as mentioned above to only authorized person[s] after verifying their authority to receive such data.

F. Right to Object

- Tangent must respect the right of data subject to object to data processing on legitimate interest or the performance of a public interest task.
- Tangent must respect the right of data subject to object to processing their data for scientific and historical research and statistics.

G. Rights in relation to Automated Decision-Making

- Data subjects have the right not to be subjected to a decision when it is based on automated processing and has a legal effect on them.
 - i. The choice is completely based on automatic means like there is no human intervention in the decision-making process.
 - ii. The decision has legal consequences or has a substantial impact to the data subject.

VI. DATA SHARING AND THIRD-PARTY ACCESS

A. Third-Party Agreements

1. Using Third Party Controllers and Processors

As a data controller and data processor, Tangent must have written consents in place with any third-party data controllers and data processors that Tangent uses. This consent must contain all parties' liabilities, obligations, and responsibilities.

As a data controller, Tangent must only appoint processors who can provide sufficient guarantee that the rights of data subjects will be respected and protected.

As a data processor, third-party data processors and controllers must only act on the documented instructions of a controller. Tangent acknowledges responsibilities as a data processor to protect and respect the rights of data subjects.

2. Consents

Our consent must comply with the standards set out by the DPO and, where possible, our consent with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

B. Cross-Border Data Transfer Mechanisms

1. Adequacy Decisions

Ensure that certain country's data protection legislation provides acceptable safeguards for personal data. Tangent can freely transfer data to a jurisdiction with an adequacy ruling without any additional precautions.

2. Appropriate Safeguards

Transfers to countries that do not have an adequacy determination must include adequate measures to guarantee the data is protected to the same level as it would be within the Philippines. These precautions may include the following:

- Standard Contractual Clauses: contracts between the sender and the receiver that include specified data protection requirements.
- Binding corporate rules are internal data protection rules within a multinational corporation that have been approved by the DPO.
- Derogations: limited exceptions to the general transfer ban, such as contractual necessity or consent.

3. Binding Corporate Rules

Binding corporate rules [BCRs] are a complicated but potentially efficient method of transferring data throughout a multinational corporation group. However, obtaining approval from DPO takes a significant amount of time and effort.

VII. SECURITY MEASURES

To maintain data security within Tangent, proper security procedures must be implemented. These safeguards serve to keep personal data safe from unauthorized access, loss, alteration, or disclosure.

A. Physical Security

Format of Data	Personal data in the custody of Tangent may be in digital or electronic format and/or paper-based/physical format. Management or employees are responsible for providing reasonable security for all information, documents and property entrusted to them.
Storage Type and Location	All personal data being collected and processed by Tangent shall be stored in a secured facility, whether virtual or physical. Papers or physical documents bearing personal data shall be stored in locked filing cabinets/room, access keys to which shall be entrusted only to authorized personnel. Digital or electronic documents containing personal data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by passwords or passcodes. Computers, portable disks and other devices used by Tangent and its PIPs in processing personal data shall be encrypted with the most appropriate encryption standard, but which should not be lower than AES250 encryption.
Access and Security Clearances	Only authorized personnel issued with security clearance by CCIARCO may access the personnel data stored by Tangent. The clearance shall be issued to personnel whose performance of official functions directly depends on such access or cannot otherwise be performed without such access.
Monitoring of Access	Access of personal data by all authorized personnel and employees whose request to access personal data were approved shall be monitored by the DPO. All those who enter and access the storage/archive room of Tangent must fill out and register in the logbook, which shall indicate the date, time, duration, and purpose of each access. Access to Tangent's data centers shall be restricted to personnel who have the appropriate security clearance. Access to records and procedures shall be reviewed by DPO regularly.
Design of Office Space	All offices specially those rendering front line services shall arrange their computers and tables with considerable spaces between them and a countertop positioned to prevent entry of visitors to maintain privacy and protect the processing of personal data. Posting of the appropriate signage "Restricted Area," "No Entry," "Unauthorized Person Not Allowed," "Deposit your Firearm[s], Camera, and Mobile Phone with Camera at the Assigned Lobby Guard[s]," etc. and installation of CCTVs at strategic locations are essential to minimize risk of personal data breach and other security incident[s].
Use of Gadgets and Storage Devices	Confidentiality shall be observed and maintained at every stage of the data processing systems. Employees, whether authorized personnel or not, shall not be allowed to bring, connect and/or use their own gadgets or storage devices of any form when processing personal data. Only prescribed devices properly configured to Tangent's security standards are authorized to access personal data.
Modes of Transfer of Personal Data within Tangent or other Parties	Transfer of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Tangent shall ensure that the uses of portable media such as disk or USB drive to store or transfer personal data is encrypted. Personal data stored in paper files or any physical media shall be transmitted only through registered mail or, where appropriate, authorized parcel post service. As much as possible, facsimile technology shall not be used to transmitting documents containing personal data.

B. Organizational Security

Contracts with PIP	The PIC through appropriate contractual agreements, shall ensure that its PIP, where applicable, shall also implement the security measures required by the Act and its Rules. It shall only engage those PIP that provide sufficient guarantees to implement appropriate security measures specified in the Act and its Rules and ensure the protection of the rights of the data subject.
Privacy Impact Assessment [PIA]	A PIA should be undertaken for every processing system of Tangent or its PIP that involves personal data. It may also be carried out vis-à-vis the entire organization with the involvement or participation of the different process owners and stakeholders. A PIA should be conducted for both new and existing systems, programs, projects, procedures, measures, or technology products that involve or impact processing personal data. For new processing systems, it should be undertaken prior to their adoption, use or implementation. Changes in the governing law or regulations, or those adopted within the organization, or its industry may likewise require the conduct of a PIA, particularly if such changes affect personal data processing. A PIC may require a PIP or a service provider to conduct PIA. For this purpose, the report prepared by the PIP of the service or product provider may be considered by the PIC in determining whether the former is able to provide a comparable level of protection to the processing of personal data.
Control Framework	A control framework is a comprehensive set of measures intended to address the risks identified in the privacy impact assessment. It includes organizational, physical and technical measures that maintain the confidentiality, integrity and confidentiality of personal data and protect the latter against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination. It includes nature of the personal data to be protected, risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and costs of security implementation.
Privacy by Design	Tangent shall consider data privacy in the design of its processing systems considering the following: <ul style="list-style-type: none"> ○ Purpose Specification – seeks to ensure the maximum degree of privacy by ensuring that personal data are automatically protected in IT systems and business practices. ○ Collection Limitation – the collection of personal data must be fair, lawful and limited to that which is necessary for the specified purpose. ○ Data Minimization – the collection of SPI should be kept to a strict minimum; by the design or programs, IT, and systems should begin with non-identifiable interactions and transactions, as the default; and whenever possible, identifiability, observability and linkability of personal data should be minimized. ○ Use, Retention and Disclosure Information Limitation – the use, retention and disclosure of personal data shall be limited to the purposes for which the individual has consented [unless required by law]. Personal data shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.
Employee Training and Awareness	Employees should receive extensive training on data security best practices, such as data handling, secure communication, password management, and spotting and reporting any security events or breaches. Reinforce awareness on a regular basis through continued training and communication.
Incident Response Plan	Create a solid incident response strategy that describes what to do in the event of a data breach or security incident. This plan should include protocols for reporting events, containing the breach, assessing the impact, alerting affected parties, and executing corrective actions.

Vendor Management	When working with third-party service providers or vendors, be sure they follow relevant data security standards. Establish specific contractual responsibilities and evaluate their security policies on a regular basis to ensure the security of personal data provided with them.
Compliance Monitoring	Continuously monitor compliance with DPA of 2012, to ensure continued legal compliance. Review and update policies, processes, and controls on a regular basis to keep up with growing security standards and regulatory changes.

C. Technical Security

Access Control	Implement strong access control systems to ensure that personal data is only accessed by authorized personnel. This includes creating unique user accounts, requiring strong passwords, adopting multifactor authentication when applicable, and reviewing and changing access privileges on a regular basis.
Encryption	Use encryption techniques to protect personal data in transit and at rest. This includes encrypting data during network transmission and storing sensitive data in an encrypted manner to prevent unauthorized access.
Data Minimization	Apply the data minimization principle by collecting and retaining just the personal data required for the intended purpose. Avoid collecting too much data and frequently review and delete old or unnecessary data.
Data Backup and Recovery	Setup frequent data backup methods and test data recovery processes to ensure that personal data can be recovered in the case of a data loss disaster. Backups should be kept in a secure location, and restoration methods should be recorded and validated on a regular basis.
Regular Security Audits and Assessments	Conduct frequent security audits and assessments to examine the effectiveness of security measures in place and identify any vulnerabilities or areas for improvement. Penetration testing, vulnerability scanning, and security assessments by internal or external experts.

VIII. BREACH MANAGEMENT

A. Incident Reporting

Any breach of this policy must be reported as soon as practically possible. This means that as soon as an employee become aware of a breach, he/she has a legal obligation to report any data breaches to the DPO within 48 hours.

All members of Tangent staff have an obligation to report actual or potential data protection compliance failures. This allows the organization to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the DPO of any compliance failures that are material or as part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed Tangent's reporting standards and procedures will be liable to disciplinary action.

B. Breach Response Plan

A structured strategy that the organization uses to identify, manage, and mitigate the impact of data breaches. It ensures timely action; limits damage and complies with DPA of 2012.

1. **Data Mapping:** understand where the data resides and how it flows through the organization. This knowledge is critical to identifying potential vulnerabilities and planning containment strategies. Then determine what data that require protection. Inventory digital assets to understand where vulnerabilities may exist.
2. **Defining the Output Format:** Plan should be easily accessible and understandable. Opt for a format that can be dynamically updated and shared across organization.
3. **Assembling Response Team:** this may be composed of the legal counsel, human resources, or with an external consultant.
4. **Notification Channels:** this includes internal notifications to executives and teams, and external communications to affected customers and regulatory bodies.

Key Components of a Data Breach Response Plan

Preparation	The cornerstone of any response plan. This involves identifying your critical assets, understanding potential threats, and training your response team.
Detection and Analysis	Implementing tools and procedures to detect breaches quickly and accurately assess their impact.
Containment, Eradication, and Recovery	Steps to limit the breach's spread, eliminate the threat, and restore systems to normal operations.
Post-Incident Activity	Reviewing and learning from the incident to bolster future defenses.
Communication Plan	Establishing protocols for internal and external communication, including regulatory bodies and affected parties.

C. Notification of Affected Parties

1. Notifying the NPC
 - a. Notification to the NPC may be done through email at complaints@privacy.gov.ph or through delivering a hard copy to the NPC office.
 - b. Upon receipt of the notification, the NPC shall send a confirmation message or email to the PIC.
2. Notifying the Data Subject[s]
 - a. Notification may be made on the basis on available information within 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.
 - b. May be supplemented with additional information at a later stage based on further investigation.
 - c. Notification to affected data subjects may be done electronically or in written form but must be done individually.
 - d. The notification must not involve a further, unnecessary disclosure of personal data.
 - e. If individual notice takes disproportional effort, NPC authorization is required for alternative means.
3. Contents of Notice
 - a. Nature of the breach
 - b. Personal data possibly involved
 - c. Remedial measures to address breach
4. Nature of Breach
 - a. Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach.
 - b. Chronology of the events leading up to the loss of control over the personal data.
 - c. Approximate number of data subjects or records involved.

- d. Description or nature of the personal data breach.
- e. Description of the likely consequences of the personal data breach.
- f. Name and contact details of the DPO or any other accountable persons.

IX. TRAINING AND AWARENESS

Employees shall receive adequate training on provisions of this policy specific to their role and shall ensure completion of all required trainings. If an employee moves role or responsibilities, he/she is responsible for requesting new data protection training relevant to his/her new role or responsibilities.

If additional training is required, employee must contact the DPO.

Not receiving necessary awareness/training shall not excuse an employee from liability for violating the policy.

X. MONITORING AND AUDITING

A. Data Audits

Regular data audits to manage and mitigate risks will be based on the data register that contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. A regular data audit is conducted as defined by the DPO and other relevant procedures.

B. Monitoring

All employees must adhere with this policy fully. The DPO has overall responsibility for this policy. Tangent will keep this policy under annual review and amend or change it as required. The DPO must be notified of any breaches of this policy.

XI. POLICY REVIEW AND UPDATES

Tangent takes compliance with this policy very seriously. Failure to comply puts the organization at risk. Failure to comply with any requirement may lead to disciplinary procedures, which may even lead to dismissal from employment.

HISTORY LOG			
Version No.	Date	Author	Summary of Change
1.0	01 October 2020	KPA, HAA	new
1.0	25 January 2021	LTC	same; no change[s]
1.0	24 January 2022	LTC	same; no change[s]
1.0	24 January 2023	KPA, LTC	same; no change[s]
1.0	13 November 2024	KPA, LTC	same; no change[s]
2.0	01 January 2025	KPA, LTC	Complete rewrite

XII. CONTACT INFORMATION


Any data subject may approach the Data Protection Officer [DPO], at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. All concerns and complaints will be handled confidentially.

If the immediate department head in question cannot resolve a complaint or remedy a breach of the policy for data protection, the DPO must be consulted immediately. Decisions made by the DPO to remedy data protection breaches must be upheld by the management of the company in question. Inquiries by supervisory authorities must always be reported to the DPO.

Contact details for the DPO are as follows:

Data Protection Officer
CCIARCO Office
dpo@tangentsolutionsinc.com

XIII. APPROVALS



KAYE R. ALAGAO
Deputy Director
CCIARCO



LYNDEL T. CIRILOS
COO



JOSE MARI ALDEGUER
President and CEO