DATA PRIVACY POLICY

TABLE OF CONTENTS

DOCUMENT CONTROL

DOCUMENT NAME: Data Privacy Policy

AUTHORIZATION:

Issue Date/Review Date	Version	Prepared By	Approved By	Description
	1	(Internal) MIND Infotech ??	Krishna	Data Privacy Policy

SECURITY CLASSIFICATION: Internal

VERSION HISTORY

Issue Date	Version	Change	Requested By	Approved By

1 Introduction

Apty collects and processes personal information of its employees, contractors, clients, partners and visitors. Consequently, Apty is committed to ensure that privacy of personal information is maintained during its entire lifecycle. Given the sensitivity of Personal Information (PI) /Sensitive Personal Information (SPI) being handled, Apty recognizes the need to protect the information against unauthorized disclosure and misuse. Apty Data Privacy Policy provides management the direction and support for protecting PI / SPI handled and processed within Apty business processes**.** Ensuring privacy is also imperative for enhancing confidence and avoiding litigations, thus ensuring an increase in Apty's credibility.

1.1 Objectives

This document defines Apty's procedures to collect, access, process, collect, store, transmit or destroy PI/ SPI and its intent and commitment to protect the same. The policy presents guidance for various functions within Apty to protect privacy of employees, contractors, clients and partners, and also critical organizational information through technical, managerial and procedural controls. The guidelines contained within the document are based on leading practices prevalent across the globe and comply with various regulatory and legal requirements of Apty Information Security Policy and Standards.

1.2 Scope

This Policy shall be applicable to PI/ SPI of employees, contractors, clients and partners, which because of the manner in which it is collected, or because of its nature or the context in which it is processed or stored, poses a threat to the privacy of an entity (individual, group of individuals or organization).

Apty Data Privacy Policy shall be applicable to all employees and third parties of Apty. As a reference for this document, a third-party is a service provider, contractor or partner associated with Apty(through direct contracts) involved in handling, managing, storing and processing of PI/ SPI at Apty. Apty Data Privacy Policy is also applicable across all business functions of Apty and across all geographies of Apty across the globe.

1.3 Definitions

Term	Definition
Privacy	Privacy is the right of an entity to control the collection, use, retention, disclosure and disposal of its PI/SPI consistent with its interests and values
The Organization	Apty

Client Organization	Client organization is a term used for the clients
Third – party staff	The term 'third party vendor' mentioned in this document refers to the employees, agents, skill based contractors, auditors, consultants and representatives, of all third parties, who are in any way accessing, processing, storing or transmitting any PI/SPI on behalf of Apty.
Personal Information (PI)	Personal Information is any information relating to an identified or identifiable natural person. Examples include, but not limited to, Name, Address, Date of Birth, Telephone Number, Fax Number, Email Address, Government Identifier (e.g. PAN Number, PF account number, etc.), Driving License Number, IP Address, Photograph or Video Identifiable to an Individual and any other unique identifying number, characteristic or code
Sensitive Personal Information (SPI)	Sensitive Personal Information is any information relating to an identified or identifiable natural person. Examples include Financial Information, Mental Health Condition, Physical/ Physiological Condition, Sexual Orientation, Medical Records and History, Biometric Information
Chief Privacy Officer	The Apty Chief Privacy Officer shall oversee all ongoing activities related to the development, implementation, maintenance of; and adherence to the Apty's policies and procedures covering the privacy of; and access to, end customer's personal information in compliance with the privacy regulatory and contractual requirements. **Head IT is taking over role Privacy Grievance Officer to start with.
Privacy Principles	Privacy guidelines followed at Apty to ensure compliance to the legal regulatory and contractual privacy requirements.
Information Privacy or Data Privacy	To protect privacy of personal information from unauthorized use, disclosure, modification or misuse. Privacy is the right of an individual to control the collection, use, retention, disclosure and disposal of his/ her personally identifiable information consistent with his/ her interests and values.
Explicit Consent	Explicit consent is the documented consent obtained directly from the individual, for example, by requiring the individual to check a box and/or sign a form.
Systems	Includes operating systems, databases, and applications.

1.4 Policy Owner

The owner of Apty Data Privacy Policy is the Chief Privacy Officer (hereinafter referred to as CPO). The CPO shall be responsible for the maintenance and update of the Apty Data Privacy Policy document.

1.5 Responsibility

Chief Privacy Officer (CPO): The CPO, as defined in the section 2.4.2 of Apty Data Privacy Policy, shall be responsible for ensuring that Apty Data Privacy Policy is current and reflects the requirements of Apty Limited.

**Chief Information Security Officer will take over role of CPO to start with.

All Employees: It is the responsibility of all employees, temporary staff and third party staff to read, understand and adhere to Apty Data Privacy Policy & other IT Policies.

Chief Information Officer: Implementing controls for electronic data is responsibility of IT department. Enforcing and monitoring for electronic data is also with IT only.

Eg. Data available in computer workstations, servers, Mobile phones, removable media, backup and Archive data, Printing technologies, etc.

Head of Department: Business unit head is responsible for enforcing controls for both electronic and soft data.

1.6 Policy Objective

Personal information collected by Apty is of utmost importance and privacy of personal information shall be maintained at all times by abiding to the privacy principles as described in section 3 of this document through controls commensurate with the sensitivity of personal information.

The management shall take steps including, but not limited to, the following in order to ensure privacy of personnel information:

a. Devising the data privacy policy for the organization;

b. Aligning the privacy framework with the business objectives;

c. Ensuring that policy of Apty is regularly updated to include the latest regulatory, contractual and organizational changes and to ensure swift and effective implementation of privacy controls;

d. Deploying appropriate technology, processes, resources and infrastructure for timely implementation of privacy controls to comply with latest privacy laws and regulations and incorporate industry best practices;

e. Taking appropriate actions including consequence management for any violations of Apty Data Privacy Policy; and

f. Increase privacy awareness in the organization.

1.7 Consequence Management for Non-Compliance

a. All employees and third party staff shall be required to comply with the Apty Data Privacy Policy.
b. Non-compliance with Apty Data Privacy Policy shall lead to disciplinary action, up to and including termination. The relevant HR processes shall be invoked for carrying out the disciplinary action.
c. If it is ascertained that the action is inadvertent or accidental, first violation(s) may result in a warning. A relevant warning letter would be placed in the involved person's records. Subsequent violations could result in termination.
d. Deliberate violation of Apty Data Privacy Policy by any individual or entity may involve disciplinary and/or legal action as appropriate. Such legal action may be initiated by Apty and may consist of criminal and/or civil proceedings.

1.8 Unanticipated Situations

This Policy does not anticipate every situation that may arise within APTY. Therefore, all users are encouraged to consider carefully the actions they take and to contact the Chief Privacy Officer (CPO) if they have any questions, concerns or suggestions relating to this Policy.

1.9 Exceptions

Apty Data Privacy Policy is intended to be a statement of information privacy requirements that need to be met at Apty. If legal/ regulatory restrictions prevent application of any aspect of this policy, the risk arising from it shall be formally recorded in Apty Risk Exception Form (Refer Appendix 2) with a detailed description explaining reason for not implementing the control, alternative mitigating controls implemented, and the residual risk. The management should take appropriate steps to ensure mitigation of this residual risk.

However, exceptions against individual controls in specific policy domains should be discussed with CPO and the business should seek his approval for the same. Following this, the exception shall be formally documented in the SOD, which shall include, at a minimum, the following:

a. Justification for the exception;

b. Risk due to the exception;

c. The mitigation controls to manage the risk;

d. The plan of action to manage the risk;

e. The validity period of the exception; and

f. Details of assets/ PII containers/ information on which the SOD is applicable.

The exception request, validation and management shall be performed as prescribed in Apty Information Security Policy.

2 Information Privacy Organization

2.1. Introduction

The Information Privacy Organization has been defined by Apty with representation from all business functions in order to provide management direction for information privacy and to coordinate and control the implementation of information privacy within Apty.

2.2. Objective

The objectives of Information Privacy Organization are to:

1. Establish a privacy framework to implement, monitor, manage and improve organization-wide information privacy controls;
2. To define and assign privacy roles and responsibilities at all levels ensuring that the individuals understand them;
3. To create information privacy awareness among employees;
4. To review privacy framework and controls at regular intervals and updated to incorporate latest legal and regulatory requirements and industry best practices.

2.3.1. Chief Privacy Officer (CPO)

The Chief Privacy Officer shall be an information privacy liaison who shall be responsible for the establishment and maintenance of the Apty Data Privacy Policy and Framework. The CPO shall have following additional roles pertaining to Information Privacy:

1. Ensure alignment of information privacy objectives to the organization's strategic plan;
2. Ensure regular review of Apty Data Privacy Policy in order to ensure compliance to latest privacy laws and regulations.
3. Ensure training and awareness programs are regularly organized to inculcate privacy awareness amongst the employees;
4. Guiding privacy representatives to ensure effective implementation of Apty Data Privacy Policy and Framework.
5. Review exceptions against Apty Data Privacy Policy and approve/suggest mitigating controls to ensure information privacy; and
6. Oversee investigations/forensics of privacy breaches.
7. Manage overall discrepancies and grievances reported by information providers as per the Data Privacy Policy;

2.1 Third-party Security

All third parties (contractors, partners and service providers) should comply with the privacy requirements laid down in Apty Data Privacy Policy. Apty shall ensure that the privacy

requirements as laid down in Apty Data Privacy Policy are communicated to all the third parties having access to PI/ SPI in any form. The contracts with third parties shall incorporate these requirements as part of the legal contract. Further, third parties shall submit their consent to comply with these requirements before any PI/ SPI is shared with them;

1. Privacy requirements from third party perspective shall be included in the Code of conduct for business associates which need to be signed off by the third party on an annual basis;
2. The third parties handling PI/ SPI shared by Apty shall establish a data privacy policy to incorporate the privacy requirements as laid down by the contract as well as all the applicable legal and regulatory requirements;
3. Before sharing any PI/SPI with a third party, Apty must ensure that there is an NDA signed with the third party backed with a legal contract or Letter of Intent (LOI);
4. If the third parties sub-contract any service/ work involving PI/ SPI shared by Apty, the subcontracted parties and their employees shall also adhere to Apty Data Privacy Policy;
5. It shall be the responsibility of the third party to ensure implementation of controls as per Apty Data Privacy Policy in their organization as well as at sub contracted organization;
6. The third parties as well as their sub contracted organization shall not disclose any PI/SPI shared by Apty without explicit consent of CPO;
7. Third-parties shall be subject to independent reviews of their compliance with Apty Privacy Policy;
8. Any PI/ SPI to be shared with a third party must be shared through a secure communication channel and data should be encrypted wherever possible.

3 Privacy statement

Apty values the privacy of any individual's PI/ SPI and therefore, is committed to ensure complete protection to the PI/ SPI it accesses, creates, receives, maintains or otherwise uses on behalf of its clients, relating to an individual.

This privacy policy demonstrates Apty's commitment to privacy and outlines how the organization intends to handle PI/ SPI for employees, contractors, clients, partners and visitors.

3.1 Privacy Principles

Apty shall adhere to the following privacy principles:

3.1.1 Management

Policy Objective: Apty shall define, document, assign accountability, regularly update and communicate Apty Data Privacy Policy to the various stakeholders in a timely manner.

3.1.1.1 Communication to Internal Personnel

Apty Data Privacy Policy shall be made readily available to all the employees of Apty and its associated entities.

a. The policy shall be hosted on the intranet for easy reference by employees;
b. The policy shall be enforced by the CPO, through regular information privacy related training and awareness campaigns; and
c. Trainings shall be conducted for the employees on their roles and responsibilities towards ensuring privacy of personal information on an annual basis.

3.1.1.2 Responsibility and accountability for policies

a. Chief Privacy Officer (CPO) shall be responsible for developing, documenting, enforcing, monitoring, and updating privacy policy and privacy related controls; and
b. The contact details of the CPO shall be communicated to all the employees of APTY.

3.1.1.3 Consistency of Privacy Policies and Procedures with Laws and Regulations

The privacy laws, regulations and standards that are applicable to Apty shall be identified. The review of the policy shall be carried out on an annual basis to ensure that policy is consistent with the applicable laws, regulations, and appropriate standards.

3.1.1.4 Personal Information Identification and Classification

a. Users, processes, systems and third parties handling personal information shall be identified; and
b. The personal information shall be classified based on the sensitivity of the information.

3.1.1.5 Risk Assessment (Privacy assessment)

Privacy assessment of all the functions shall be carried out initially for all processes to identify the risk of leakage of personal information and its criticality. Thereafter, such assessments shall be carried out whenever there is a change in the process or governing laws and regulations. PST shall carry out the privacy assessment of all the business functions of Apty across all locations.

3.1.1.5 Consistency of Commitments with Privacy Policies and Procedures

Contracts and Service Level Agreements shall be reviewed and updated on periodic basis by the business functions to ensure consistency with Apty Data Privacy Policy.

3.1.1.6 Infrastructure and Systems Management

a. The Team shall assess the impact of new and significantly changed products, services, business processes, and infrastructure on privacy of personal information;
b. Documented systems development and change management process shall be used for all information systems and related technology (including manual procedures, application programs, technology infrastructure, organizational structure, and the responsibilities of users), used to collect, use, process, retain, disclose, and destroy personal information;
c. Potential effect on privacy shall be assessed for new systems and changes;
d. Changes to system components shall be tested to minimize the risk of any adverse effect on the privacy of personal information. A controlled test database shall be maintained for full regression testing to ensure that changes to one program do not adversely affect other programs that process personal information;
e. All test data involving personal information shall be anonymized;
f. Procedures shall be implemented to ensure integrity and protection of personal information during migration from old to new or changed systems;
g. Documentation and approval by the CPO, business function manager, and IT management shall be taken before implementing changes to systems and procedures that handle personal information, including those that may affect its security. Emergency changes shall maintain the same level of protection of personal information; however, they may be documented and approved post implementation;
h. The IT and Network function shall maintain a listing of all applications / software that process personal information and the respective level, version, and patches that have been applied;

i. Where systems are involved, appropriate procedures shall be followed, such as the use of separate development, test, and production libraries to ensure that access to personal information is appropriately restricted; and

j. Personnel responsible for initiating or implementing new systems and changes, and users of new or revised processes and applications shall be provided training and awareness sessions related to privacy.

3.2. Notice

Policy Objective: Apty shall provide notice to the information providers about its privacy policies and practices, purposes of collecting personal information, usage, retention, dissemination and destruction, the identity and location in Apty where the personal information resides and , information on whom to contact at Apty on privacy related issues.

3.2.1 Communication to Individuals

All business functions shall ensure that while collecting any personal information the information providers are informed about the purpose of collection of the information. The privacy notice provided to the information provider shall include following points:

a. If any personal information is collected, the purpose for collection of such information and whether this purpose is a part of a legal requirement;

b. Consequences, if any, of not providing the requisite information. The consequences of information provider's refusal to provide the consent or, at a later date, withdrawal of the consent with regard to collection, processing, retention and disclosure of his/her personal information;

d. The process to be followed by the information provider to exercise the choices available to them with respect to their personal information (for example signing the consent clause or checking the opt in box for giving consent);

e. The options with information provider to change the contact preferences and withdraw consent with regard to processing, retention, dissemination and destruction of the personal information at any later date;

f. The retention of personal information for only as long as necessary to fulfil the stated purposes, or for a period specifically required by law or regulation and thereafter is disposed of securely;

g. The procedure to be followed by information providers to update and correct their personal information (for example, in writing, by phone, by email, or by using the entity's website);

h. Communication of the method of resolution of disagreements related to personal information;

i. Information may be disclosed to the authorized third parties for providing service(s) to the information providers;

j. Information may be transferred to entities located within or outside India for the purposes of providing service(s) on explicit consent from the information provider or if it is necessary for the performance of the lawful contract between Apty and the information

provider and post ensuring the same level of data protection is being adhered to by such entity;

k. Notification about the web tools such as web cookies and web beacons which are used by Apty to collect information providers' personal information while they are on Apty's website and about their choice to turn off cookies and beacons and as a result not provide such information to Apty;
l. Notification that reasonable physical and logical access controls are implemented to ensure privacy of their personal information; and
m. Description of the procedure of registering complaints regarding their personal information including the contact information of the CPO.

3.2.2 Provision of Notice

a. Notice shall be provided to the information providers in a timely manner (that is, at or before the time personal information is collected) to enable them to decide whether or not to submit personal information; and
b. Notice shall be dated to allow information providers to determine whether the notice has changed recently.

3.3. Choice and Consent

Policy Objective: Apty shall communicate to the information providers, the choices available to them and obtain explicit consent with regard to collection, processing, retention, dissemination and disclosure of the information.

3.3.1 Implicit or Explicit Consent

The business functions shall ensure that:

a. The information provider's consent is obtained in a timely manner and properly documented and retained till the time the information provider is associated with Apty or as mandated by the local laws (whichever is longer); and
b. Any changes to the information providers' preferences with respect to their consent are recorded and are implemented within seven working days of obtaining them.

3.3.2 Consent for New Purposes and Uses

The business functions shall ensure that: -

a. When personal information is to be used for a purpose not previously specified, the individual is notified and the new purpose is documented. The business function shall obtain and document consent or withdrawal of consent to use personal information for the new purpose; and
b. The use of personal information provided by the information providers is in accordance with their preferences.

3.3.3 Explicit Consent for Sensitive Information

Any sensitive personal information shall be collected only after explicit consent of the information provider.

3.4. Collection

Policy Objective: Apty shall collect personal information only for the purposes communicated to the information providers furthermore, any such information shall be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the end customer concerned.

3.4.1 Collection Limited to Identified Purpose

In case the business function needs to collect the personal information, the business function shall:

a. Clearly indicate the fields of personal information which are essential for the purpose of providing product or service and differentiate it from the non-essential fields of personal information; and
b. Periodically review the business' necessity of collection of personal information and ensure that the fields of information being requested are consistent and limited to those required for providing the product or service. Also, it shall be ensured that all personal information mandated by the applicable laws and regulations is collected before conducting business.

3.4.2 Collection from Third Parties

a. Contracts signed with the third parties shall include provisions requiring them to collect personal information fairly and lawfully and in accordance with Apty Data Privacy Policy requirements; and
b. Collection methods adopted by the third parties responsible for collecting personal information of the information providers shall be reviewed. Business shall ensure that information providers are provided with the choice and their consent is obtained before collecting such information.

3.5. Use and Retention

Policy Objective: The information provided by an individual to Apty shall be used only for the purposes for which it was provided and consented by the individual and shall be retained for only as long as necessary to serve the purpose or as required by the applicable laws or regulations. Personal information shall be securely disposed of to prevent its retrieval and mishandling post the retention period.

3.5.1 Use of Personal Information

While using personal information, the concerned business function shall ensure that:

a. The information is used in accordance to the purposes intimated to the information provider while collecting the information; and
b. The applicable laws and regulations are adhered to all times.

3.5.2 Retention of Personal Information

For retention of the personal information, adherence to following controls shall be ensured:

a. Retention period shall be defined and implemented as per the business requirement or legal requirements, whichever is later;
b. Retention periods of different types of records of personal information shall be defined;
c. The interception communication recorded through lawful interception, if any, shall be retained for a period of two months from the date of issue;
d. Third parties should define and implement the "retention policy" for personal information, which should be aligned to the Apty's retention policy. This policy should clearly define the retention period for various records containing personal information; and
e. Any personal information not required for conducting business or mandated by law and captured by Apty's systems is removed in a timely and secured manner to prevent mishandling;

3.5.3 Disposal and Destruction of Personal Information

While disposing of personal information, following privacy controls shall be adhered to:

a. Information is disposed of in accordance with the timelines defined in the retention policy of Apty or its third parties depending upon the ownership of the information;
b. Time of disposal is documented to include the details of the disposed-off records containing personal information. For example, document the name of the record owner, date created, date destroyed, method of destruction, fields of personal information contained by it and primary purpose for the creation of the record;
c. Destruction of personal information which is no longer required for providing the services or as per applicable laws and regulations; and
d. Any information retained by Apty after the expiry of its retention period is retained only after obtaining consent of the information provider.

3.6. Access and Correction

Policy Objective: Information providers, at all times, shall be able to access their personal information available with Apty. Apty shall provide the information providers with an option to update their personal information.

3.6.1 Access by Individuals to their Personal Information

Any business function, while maintaining personal information, shall ensure that:

a. All information providers are intimated of different means of accessing their personal information as part of the notice;
b. Information providers are able to access their own personal information only. No individual, who is not an authorized personnel to access personnel records, shall be provided with access to personal information of any other information provider;
c. All such requests of information providers to access their personal information are processed within seven working days from the date of request; and
d. All such requests for access to personal information along with action taken by Apty are recorded. If Apty is unable to provide the requisite information or in case of unresolved complaint or dispute, the reasons for not complying with the request shall also be documented.

3.6.2 Confirmation of an Individual's Identity

a. Identity of the information providers shall be verified before allowing them access to their personal information; and
b. Communication with the information provider about updating his/her personal information shall be carried out only over email or at the postal address provided by the information provider. In case of change of postal address, such communication shall be sent to both, the new postal address and the old address.

3.6.3 Updating or Correcting Personal Information

a. Information provider shall be communicated of the procedure for updating personal information;
b. Personal information shall be updated in a time bound manner after receiving the request for change;
c. Personal information shall be updated only after verification of the identity of the information provider; and
d. Procedures for resolving the discrepancies related to the personal information shall be communicated to the information providers.

3.6.4 Internal Access to Personal Information

a. All functions handling personal information shall be identified and the relevant processes within these functions shall be reviewed for adequacy of privacy controls of personal information;
b. Access to personal information shall be provided to a Apty employee (part time/ full time), contractual employee or third party employee only after authorizations of the functional

head of his/her function. All such authorizations shall be obtained over mail or in hard copy format; and

c. Any changes to an individual's personal information shall be efficiently updated in all the systems of Apty. If any third party is facilitating in updating this information on Apty's behalf, it shall be the responsibility of the third party to accurately update the records.

3.7. Disclosure to Third Parties

Policy Objective: Any information shared with the third parties shall be shared only after obtaining explicit or implicit consent from the information provider.

Additionally, Apty shall ensure that the third-party adheres to all applicable privacy principles and regulations.

3.7.1 Disclosure of Personal Information

Following points shall be kept in mind while disclosing personal information to the third parties or any other agencies:

a. Business functions shall disclose the personal information to Government agencies only after verifying that such agencies are lawfully authorized to seek such information. Further, all such requests shall be obtained in writing clearly mentioning the purposes and the powers of such agencies to seek personal information from Apty ;

b. Personal information shall be disclosed to third parties of Apty on need basis only for the purpose of executing business. Further, business function shall ensure that all such third parties have signed a Non-Disclosure Agreement (NDA) with Apty to ensure privacy of personal information of information providers. Also, the contracts with such third parties shall be updated to include a clause on privacy of personal information of Apty's information providers available with them; and

c. Business functions shall document the nature and extent of personal information disclosed to the third parties.

3.7.2 Protection of Personal Information

a. The purpose, for which information is collected, shall be communicated to the third parties with whom the information is being shared, as part of the legal contracts signed with them and they shall be instructed not to use this information for any other purposes. The third parties shall further disclose the personal information to their sub-contractors only if such disclosure is necessary for providing service(s) to the information providers; and

b. All third parties shall provide periodic statement of compliance stating that they are compliant with Apty Data Privacy Policy requirements. Apart from this, audits shall be conducted by Apty or representatives appointed by Apty to ensure compliance of third parties with Apty Data Privacy Policy requirements.

3.7.3 Non-compliance to protection of Personal Information

Non-compliance of any third party with the privacy practices followed at Apty, is ground for disciplinary actions up to and including termination of the contract. The third party will establish a procedure to ensure that the associates are made aware of their personal liability of personal information and that any deviation to the policy may lead to the associate's services being discontinued/ terminated.

3.8. Security

Policy Objective: Apty shall ensure protection of personal information against unauthorized access, usage and dissemination.

3.8.1 Information Privacy Program

Following shall be taken into consideration while handling personal information:-

a. Periodic vulnerability assessment of the physical and technical environment shall be carried out to gauge effectiveness of privacy controls implemented. Apart from this, penetration testing shall be carried out periodically to assess the resilience of websites and other systems of Apty accessible through internet;
b. Adequate authentication parameters and access controls, as described in Apty Information Security Standards, shall be implemented at all access points of personal information;
c. Access rights of all the employees handling personal information shall be periodically reviewed, at least once every quarter;

3.8.2 Logical Access Controls

a. Employees shall not divulge the security procedures followed at Apty to mitigate the risk of compromise of personal information; and
b. Access controls, as defined in the Apty Information Security Standards, shall be applicable at all points from where personal information is accessible.

3.8.3 Physical Access Controls

a. Apty shall provide adequate protection to its information systems containing any personal information and facilities against unauthorized physical access and environmental threats using measures as described in Apty Information Security Standards;
b. Hard copy of any form or any other document containing any personal information shall be secured physically by adopting adequate security measures as described in Apty Information Security Standards; and

c. Apty shall log and monitor access areas hosting personal information. Any attempted breach and unauthorized destruction of information shall be dealt with in accordance with Section 1.7 Consequence Management for Non-Compliance.

3.8.4 Environmental Safeguard

Privacy of personal information of any information provider shall be ensured, even at the time of disaster. Business continuity and disaster recovery plans shall be updated to ensure privacy of personal information in such an event.

3.8.5 Transmitted Personal Information

All personal information transmitted to external networks shall be transmitted through secure lines. Any remote access to Apty systems containing personal information shall be according to the Apty Information Security Standards.

3.8.6 Personal Information on Portable Media

a. Personal information shall not be stored on portable media or device unless it is required by business. Even if required, an approval shall be taken from the business head and the CPO. If it is stored, care should be taken to mitigate the risk of its leakage by encrypting it and protecting it using password; and
b. Mechanisms shall be defined by each business to report loss of media containing personal information and ensure timely documentation of all such incidents. In case of loss of media, business, in consultation with PST and PT shall take mitigating steps to minimize the risk arising from any such incident. To proactively prevent future occurrence of similar incidents, all such incidents shall be investigated and action points from such investigation acted upon.

3.9. Accuracy

Policy Objective: Apty shall strive to maintain the completeness and accuracy of the personal information of information providers available with it.

3.9.1 Accuracy and Completeness of Personal Information

To maintain the accuracy of the personal information available with Apty, following points shall be taken into consideration:-

a. Apty shall maintain complete and accurate personal information of information providers, as provided by them, as long as Apty retains it;
b. It shall be communicated to the information providers at the time of collection, that:
    - They are responsible for providing complete and accurate personal information;

- Methodology to contact Apty in case their personal information needs to be updated;

c. If any changes to their personal information are requested by the information providers, such requests shall be processed in a time-bound manner and the record of all such change requests shall be maintained.

3.10. Monitoring and Enforcement

Policy Objective: Apty shall incessantly monitor the compliance of employees, third parties and other direct stakeholders with this policy and shall address privacy related complaints, queries and disputes appropriately.

3.10.1 Inquiry, Complaint and Dispute Process

a. The steps to contact Apty management in case of privacy related complaint or queries shall be clearly defined and also be published on Apty's official website;
b. It is the duty of all employees and third parties of Apty to cooperate with CPO for effective and timely resolution of information provider's complaints and queries;
c. The information provider shall be intimated of any breach of personal information with all relevant details as per the last communication address shared by the information provider;
d. All complaints and queries shall be periodically reviewed to ensure their timely resolution (within 20 days) and the unresolved disputes and complaints, pending for more than 20 days, shall be reviewed by CPO for appropriate resolution;
e. It shall be ensured by the CPO that all complaints and queries are resolved within 30 days; and
f. Information provider's complaints records shall be periodically reviewed by the CPO to identify trends and Apty Data Privacy Policy and relevant processes shall be updated to address those specific issues.

3.10.2 Compliance Review

a. Annual reviews shall be carried out by the CPO to ensure organization's compliance with Apty Data Privacy Policy, other privacy procedures, applicable data privacy laws and regulations and privacy standards adopted (if any); and
b. Management shall address the vulnerabilities, cited in the annual review, in a timely manner and it shall be the responsibility of CPO to ensure remedial controls are implemented at the earliest to prevent any information privacy related incidents;

3.10.3 Ongoing Monitoring

a. All employees of Apty shall complete the online information privacy training post joining the organization;
b. Employees and third parties shall inform CPO if they observe any privacy vulnerability or security breach; and

c. Whenever an employee's roles and responsibilities change, his access to personal information shall be reviewed and appropriately modified within 72 hours of such change. If an employee is leaving the organization, his access to the personal information shall be immediately revoked.

3.11 Privacy Awareness and Training (PAT)

Apty shall formalize a privacy awareness and training program to address the continuous training of all the personnel involved in handling the PI/SPI, including employees, contractors and individuals.

Objectives

a. To ensure that the employees/ contractors/ third party vendors understand their responsibilities and roles towards protection of PI/SPI and privacy requirements;
b. To establish awareness amongst Apty employees and third party vendors regarding:
    i. Privacy Principles;
    ii. Data protection regulations;
    iii. Legal liabilities of the organization and its employees;
    iv. Do's and Don'ts for privacy;
    v. Principles of due care;
    vi. Privacy specific incident reporting;
c. To ensure timely detection and reporting of privacy incidents thereby minimizing the impact from such incidents; and
d. To achieve compliance with Apty's privacy policies;

4 Review and Evaluation

The Apty Data Privacy Policy document shall be reviewed at the time of any major change(s) in the existing environment affecting privacy policies and procedures or once every year, whichever is earlier. The Apty Data Privacy Policy document shall be reviewed by the Privacy Grievance Officer and approved by the Privacy Steering Committee.

5 Appendices

5.1 Appendix 1

Online Privacy Policy	apty's privacy statement.docx

5.2 Appendix 2

Apty Risk Exception Form	Exception Form V1.0.docx