Data Protection Policy

Denave

REVISION HISTORY

Title	Data Protection Policy
Version Number	1.1
Last Document Change (DCR)	Update Data Subject Rights

Approved By:		**Sumit Malaviya**	
Version	**Release Date**	**Significant Changes**	**Author**
1.0	21-Dec-2017	First Formal Issue	Arjun Singh Chauhan
1.1	21-May-2018	Update Data Subject Rights	Arjun Singh Chauhan
1.1	23-May-2019	No Change	Arjun Singh Chauhan

CONTENTS

1. POLICY STATEMENT

Denave is committed to respecting the privacy and distinguishes the need for appropriate safety of any personally identifiable information ('Personal Information') of its employees, customers and vendors. The authenticity of the Personal Information is the sole responsibility of the provider and that Denave shall not be held accountable for the same. Denave strives to comply with applicable laws that are designed to protect individual privacy.

2. PURPOSE

The purpose of the policy is to stipulate how Denave shall have a systematical approach when working with Privacy/Data Protection in order to ensure the following objectives:

- that employees feel safe and secure in how Denave handles their Personal Information (Denave's Data Controller Role),
- that clients feel safe and secure in how Denave handles the Personal Information of their end customers (Denave's Data processor Role) ,
- to ensure compliance to relevant Privacy/Data Protection regulations and to minimize the risk of penalties and fines.

3. OBJECTIVE

- Denave is committed to meeting its obligations under the applicable Privacy/Data Protection laws. Denave will strive to observe the laws in all collection and processing of subject data, and will meet any subject access request in compliance with these rules.
- Denave will only use data in ways relevant to carrying out its legitimate purposes and functions as an IT Service Provider in a way that is not prejudicial to the interests of individuals.
- Denave will take due care in the collection and storage of any sensitive data.
- Denave employees and, where appropriate, representatives, will do their utmost to keep all data accurate, timely and secure.
- All Denave employees and representatives, whether permanent or temporary, must be aware of the requirements of the Data Privacy Rules when they collect or handle data about an individual.
- Denave employees and representatives must not disclose data except where there is subject consent, or a legal requirement. Data sent to outside agencies must always be protected by a written contract. All collection and processing must be done in good faith.
- The Data Protection Officer will keep records of all complaints by data subjects and the follow up. He/she will also keep a record of all data access requests. There will be a repository of Denave statements of Data Privacy Rules compliance. This information will be available to relevant employees and data subjects on request.
- Denave shall keep all notifications up to date.

4. SCOPE

The document applies in relation to all processes, both from corporate and delivery side, at Denave. Further, all the data subjects such as employees, prospective employees and individual contractors (whether temporary or permanent), Clients and client's customers hereafter referred as 'data subjects' are covered under this policy.

5. DEFINITIONS

- **Individual:** Individual shall mean any natural person, which include Denave Global Employee, Client, Client Customers, Suppliers and Vendors.
- **Personal Information/ Personally Identifiable Information (PI/PII) is** any data that could potentially identify a specific individual directly, or indirectly. It includes, but not limited to names, date of birth, social security number, Government/National Identifiers, address, telephone numbers, employee ID numbers, credit card numbers, passwords etc. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered Personal Information.
- **Sensitive Personal Information (SPI)** is any data that could potentially identify a specific individual's racial or ethnic origin, political opinions, religious beliefs, physical or mental health etc.
- **Data subject:** An individual who is the subject of Personal Information. In other words, the data subject is the individual to whom Personal Information/information belongs.
- **Data Controller** is an entity that has the authority over the processing of personal information. It controls the use of Personal Information by determining the purposes for its use and the manner in which the data will be processed. The Data Controller may be an individual or an organization that is legally treated as an individual, such as a corporation or partnership.
- **Data Processor** is an individual or organization that processes data on behalf of the data controller. A Data Controller can also be a data processor.
- **Data Processing** is any operation or set of operations which is performed on Personal Information, such as collecting; recording; organizing; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission, dissemination or otherwise making the data available; aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means.
- **Privacy Incident** shall be defined as any activity performed in contravention to applicable privacy and data protection laws and regulations of the country.
- **Privacy Breach** - Privacy Incident can result in a Privacy Breach when the information compromised reveal any type of Personal Information. Privacy breach may occur due to unauthorized access, unauthorized disclosure, misuse, theft or loss etc.

6. DENAVE'S APPLICABILITY

- **Data Controller**

  Denave collects, uses, stores, transfers and deletes Personal Information relating employees (both full and part time) for its business purposes. Such Personal Information includes, but is not limited to: name, address, date of birth, Permanent Account number, National insurance number (or equivalent government issued social welfare numbers), salary details, designation, medical details, passport number, residential and alternate personal telephone numbers, photographic image, bank account number and signature.

As Denave collects this Personal Information from Data Subjects and defines the terms of processing, it attains the position of a Data Controller for employee Personal Information.

Business Role	Activity	Privacy Role
Denave as an employer, Consumer of Third party contractors/Service providers	Collects, uses, stores and disposes Personal Information of the data subjects for business purposes	Data Controller

- **Data Processors**

  Denave processes its client's and client customer's Personal Information as per Client's instructions, thus Denave's role is limited to that of a Data Processor.

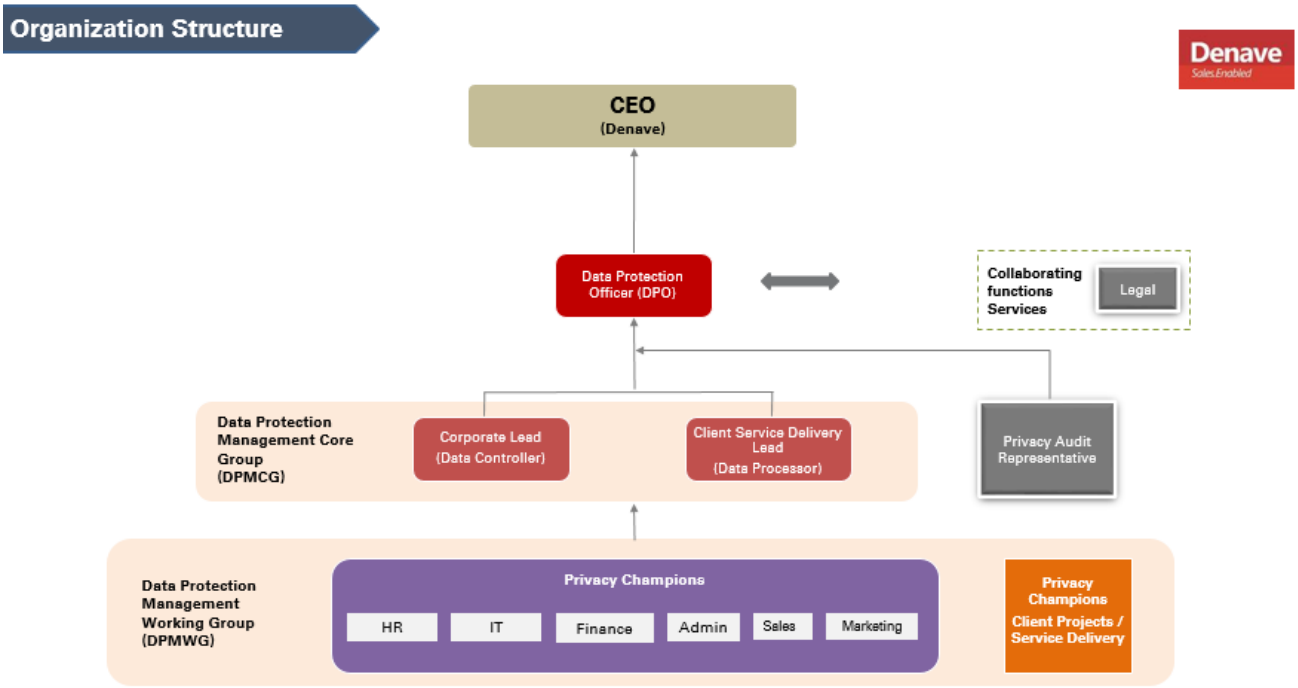
Business Role	Activity	Privacy Role
Denave as a third party processor	Uses, stores and disposes of Personal Information as agreed in agreement or related Statement of Work	Data Processor

7. APPROACH TO DATA PROTECTION

Denave is willing and committed to adapt to changes in the internal organization and the external environment. In order to achieve this Denave shall work with the below standardized approach:

- **Identify Risks & Requirements:** Identify internal and external risks and requirements and handle them in a sufficient way.
- **Updated Standards & Guidelines:** The input form the risk and requirement identification will lead to updates of the standards and guidelines and/ or creation of new ones.
- **Communication**: The new standards need to be communicated effectively and to the right audience.
- **Implementation:** The organization need support and time in order to implement new requirements.
- **Audit & Compliance:** Follow up on the requirements need be done on different level (external and internal audit) in order to ensure compliance. The audit result will be the input for the next risk and requirements identification.

8. DATA PROTECTION ORGANIZATION STRUCTURE



- **Roles and Responsibilities**

  Board of Director (Denave)

  - Approve Privacy/ Data Protection (P/DP) framework;
  - Approve roles and responsibilities for implementing the P/DP framework;
  - Approve suitable budget and resources to design, implement, validate, and optimize the P/DP framework;
  - Review and approve new initiatives proposed by Data Protection Officer (DPO); and
  - Communicate the importance of meeting P/DP objectives and conforming to P/DP policies, organization's responsibilities under applicable laws and the need for continual improvement.

  Data Protection Management Group (DPMCG)

  - Develop P/DP policies and procedures.
  - Develop procedures on complaints, disputes, and P/DP related incidents;
  - Review organization's clients', vendors', and legal entity subsidiaries' P/DP policies and governance documents to ensure adherence and conformity to organization's P/DP policies and procedures.
  - Review requests for exemptions from organization's P/DP policies and implementing procedures.

- Review privacy issues identified in compliance testing, control assurance, internal/external audits, regulatory examinations, and other business/functional area monitoring or self-assessment and develop mitigation plans for open risks.
- Review privacy incident reports and recommend corrective action to DPMWG.
- Review updates in global P/DP regulatory expectations, pending regulatory changes, and emerging trends as they relate to P/DP and recommend actions to ensure future compliance.
- Develop P/DP training materials and the ensure effectiveness of enterprise-wide training programs.
- Present initiatives for new projects or changes to existing technology or business processes that relate to collection, marketing, sharing, and/or disclosure of PII / Personal Information, or otherwise introduce P/DP risk to the DPO.
- Report enterprise-wide P/DP matters to the DPO. This includes, but is not limited to:
  - Testing and monitoring results for high risk areas;
  - Material compliance issues or escalated issues;
  - Status of remediation efforts and corrective actions;
  - Status of findings from internal/external reviews and examinations;
  - Exceptions granted to privacy/data protection policies and implementing procedures; and
  - New privacy/data protection initiatives.

Data Protection Management Working Group

- Follow and ensure compliance with organization's P/DP policies, procedures and standards;
- Conduct DPIA and remediate necessary risks, based on the recommendations provided by DPO and DPMCG;
- Report any P/DP concerns to DPMCG, within reasonable time;
- Coordinate with internal business functions to respond to any requests and/or complaints on Personal Information processing;
- Provide support to follow P/DP breach response policies and procedures whenever a breach is discovered or suspected;
- Participate in and conduct necessary P/DP training activities for respective business functions;
- Unless delegated, represent the business activities, during audits, assessments and investigation;
- Support DPMCG and DPO with necessary metrics from time to time;
- Send necessary internal communications to respective business functions, based on corrective actions provided by DPMCG and be accountable to track them to closure

Privacy Audit Representative

- Develop a privacy audit calendar and ensure compliance with established privacy framework by examining records, reports, operating practices, and documentation.
- Report the findings to the DPMCG and communicate the mitigation plan/corrective actions to DPMWG.

- Co-ordinate with DPMWG to track the implementation of the suggested mitigation plans/ correction actions.
- Maintain audit work papers by documenting audit tests and findings.

Collaborating functions (Legal)

- Collaborate with DPO and provide inputs from legal aspects to ensure development and sustenance of a robust Privacy framework in the organization.
- Remain up to date on legal requirements specified in applicable P/DP regulations and provide guidance to DPMCG in incorporating these requirements in P/DP policies and procedures.

9. DATA PROTECTION PRINCIPLES

All processing at Denave shall rely on and follow the below mentioned Privacy/ Data Protection principles.

- **Lawfulness, fairness and transparency:** Lawfulness and fairness mean that at least one of the legitimate processing criteria to process Personal Information is met to and fulfilled in a fair manner. The legitimate processing criteria applicable for Denave are:
  - Contractual necessity – processing is needed to provide the service e.g. billing, order intake, provisioning, trouble shooting, transmission
  - Legal obligation – processing is needed to fulfill legal requirements e.g. financial reporting, Tax/VAT, lawful intercept
  - Legitimate interest – processing is allowed after weighing the interests of Denave and the Data Subjects, e.g. processing for direct marketing, debt collection, revenue assurance
  - Consent – The Data Subject (Customer, Employee) has given consent, e.g. to process data for profiling (including marketing), selling/sharing data with third parties

  Transparency means that it should be clear to the individual which Personal Information is processed, for what purposes and to which extent. The information should be easily accessible and easy to understand (clear and plain language used).
- **Purpose limitation:** Purpose limitation means that Personal Information must be collected for a specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- **Data minimization:** Data minimization means that Personal Information that are processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed.
- **Accuracy:** Accuracy means that Personal Information must be accurate and, where necessary kept up to date. So ensuring the data quality of the Personal Information Denave has.
- **Storage limitation:** Storage limitation means that Personal Information must be kept in a form which permits identification of the data subject for no longer than necessary for the purposes for which the data are processed.
- **Integrity and confidentiality:** Integrity and confidentiality means that the Personal Information must be processed in such a way that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical and organizational measures.

- **Accountability:** Accountability means that Denave is responsible for compliance to the relevant Privacy/Data Protection regulations and that Denave is able to demonstrate how compliance is achieved.

10. DATA SUBJECT RIGHTS

Denave is sensitive towards the freedom of the Data Subjects and is committed towards valuing their rights as per applicable laws/regulations. Denave has developed internal policies and processes to ensure that the Data Subjects can easily exercise their rights. For more details please refer the 'Data Subject Request handling guidelines'. Below are the rights provided to Data Subjects under the General Data Protection Regulation (GDPR).

- **Right to information** - Denave as a Data controller and Data Processor must provide information notices to Data Subjects to ensure fair and transparent processing of their Personal Information.
- **Right to access** - Denave must on request from any verified individual confirm if Denave processes any Personal Information of the individual, and provide supporting /detailed information (as applicable)
- **Right to erasure** ("Right to be forgotten")- A Data subject should have the right to have his or her Personal Information erased, i.e. the Right to be forgotten, and no longer processed.
- **Right to rectification**- The data Subject has the right to rectify his/her Personal Information provided to Denave to ensure that his/her Information is processed based on correct information.
- **Right to restriction of processing** - For Denave's purposes the right to restriction would normally only mean restrictions for marketing purposes (i.e. processing based on consent) of non-anonymized data. The fact that the processing of Personal Information is restricted should be clearly indicated in the Denave systems/records.
- **Right to data portability** - A Data subject shall have the right to receive the Personal Information concerning him or her, which he or she has provided to Denave (e.g. name, address, email-address, etc.), in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller
- **Right to object** (opt-out) to processing- The Data subject shall have the right to object (unless Denave otherwise has compelling legitimate grounds), on grounds relating to his or her particular situation, at any time of processing of Personal Information concerning him or her, including profiling based on those provisions.

11. DATA INVENTORIZATION

A data inventory is a record of the Personal Information attributes processed for performing one or more operations (e.g. while processing employees' Personal Information to elaborate pay slips or processing client's information to provide a specific service). The Data Inventory shall act as a record of processing activities performed by Denave, both as a Data Controller and Data Processor.

Among others, the Data Inventory shall provide information regarding the type of data processed, where and how it is processed (e.g. generated, edited, deleted, transferred) by which Denave's functions and why.

Further, Denave has created Records of Processing and Data Flow Diagrams to identify the flow of Personal Information of the Data Subjects within Denave, in its capacity as a Data Controller and Data Processor.

For more details on how Denave creates and manages data inventory please refer to 'Data Inventory guidelines'.

12. DATA PROTECTION IMPACT ASSESSMMENT

Denave performs Data Protection Impact Assessment (DPIA) to determine the maturity level of its Privacy/Data Protection framework. Where processing of PII/SPI by Denave is likely to result in risk to the rights and freedoms of Data Subjects, taking into account the proposed nature, scope, context and purposes of the processing, a DPIA should be carried out.

DPIA is performed at two levels;

- **Enterprise level** (Corporate functions like HR,Finance, Admin, IT, Sales and Marketing etc. as part of Denave's Data Controller Role) to determine the overall Data protection maturity of Denave;
- **Project level** (Client projects as part of Denave's Data Processor Role) to determine the project specific Data Protection maturity level.

For more details on how Denave performs DPIA, please refer the 'DPIA guidelines'.

13. THIRD PARTY MANAGEMENT

Denave shall notify Data Subjects prior to disclosing Personal Information to any Third Parties. Denave shall ensure that any such disclosure made shall be for the purposes indicated in the privacy policy provided to the Data Subject.

Denave must take reasonable steps and exercise due diligence during selection of Third Parties who handle Personal Information. Denave must execute written contracts with Third Parties mandating strict compliance with this Data protection Policy and applicable laws and, at a minimum, shall retain audits rights to monitor Third Parties' usage of Personal Information during performances of services by such Third Parties. Denave shall further ensure that any Third Party processing such Personal Information shall:

- not disclose the Personal Information without Denave's prior written consent;
- where applicable, sign a Non-Disclosure Agreement with Denave before Personal Information is disclosed;
- enter into a Master Services Agreement with Denave to ensure the protection of Personal Information that is disclosed to the Third Parties as per Denave privacy practices; and
- take adequate measures and comply with all applicable laws while Personal Information is transferred to another entity or country, and to facilitate such transfers.

Denave shall ensure that cross border transfers of Personal Information to a Third Party or to any business affiliate are accompanied with adequate level of protection and compliance with applicable laws and regulations. For more details kindly refer 'Third part Data Protection guidelines'.

Managing Sub-Contractors

When acting as a Data Controller, Denave may share Personal Information with Third Parties and/or vendors who may further engage with another organization (sub-contractor) to process Personal Information. In such scenarios, Denave shall undertake at least the following measures:

- Denave shall maintain a list of sub-contractors to whom Personal Information is being shared;
- Denave shall assess the adequacy and appropriateness of security controls as part of due diligence before any sub-contractor is engaged by the vendor or Third Party;

- Denave shall specifically require, within the Master Services Agreement, that the vendor flow down to the sub-contractor its requirements to always deploy appropriate technical and organizational security measures for Personal Information; and
- Denave shall ensure that when a contract between a Third Party vendor and its sub-contractor is terminated, Personal Information is either destroyed or passed on to Denave as per Denave's requirement. No copies of Personal Information should be retained by a sub-contractor on the termination or expiry of its appointment.

Denave is committed to identify and assign appropriate accountability which shall ensure effective implementation, policy development, adherence, evaluation and refinement of privacy protection throughout the organization.

14. INFORMATION DISCLOSURE

- Requests for the disclosure of any personal and sensitive personal information will only be processed once Denave is fully satisfied that the enquirer or recipient is authorized to receive the information. Care must be taken to ensure that any disclosure has a lawful basis. A criminal offence under the Data Privacy Rules may be committed if the information is obtained or used in any way outside the notified purposes.
- Denave may transfer sensitive Personal Information or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by Denave. The transfer may be allowed only if it is necessary for the performance of the lawful contract between Denave on its behalf and provider of information or where such person has consented to data transfer.
- Denave shall not allow data collected from subjects to be disclosed to third parties except in circumstances, which meet the requirements of the Data Privacy Rules. This will be either:
  - The subject has consented to the disclosure.
  - Denave is legally obliged to disclose the data.
  - There is a business requirement to disclose data that is within the remit of the Data Privacy Rules and is not prejudicial to the interests of the individual.
- The disclosure of any data collected by Denave will only take place where the subject has been informed about this use of their data and offered the chance to opt out.
- Occasionally information relevant to an enquiry must be sought from other organizations. In these circumstances an organization may request an official from Denave stating what specific information is sought and why. Personal and sensitive Personal Information may be exempt from the provisions of the Rules in cases where the disclosure is required for the following purposes:
  - the prevention and detection of crime;
  - the apprehension or prosecution of offenders
- These exemptions only apply to the extent that if the data were not disclosed, it would be likely to prejudice the investigations.
- An appropriate entry must be made on the source document for each transaction.
- Other government organizations may serve a notice on the company to access information held. Normally such use will be by organizations that have the authority to investigate and/or prosecute offences.

Procedure on Disclosures

- All employees must ensure any general disclosure is recorded, and each class of disclosure includes a clear rationale as to why this is taking place.
- Any new disclosure to be made must be checked for suitability with the DPO/DPMCG. This may be referred to the Legal for advice.
- Any request for data based on a legal requirement, e.g. from Police or other body, must be put in writing and be checked against the advice of the DPO and the Legal before data is disclosed.
- All employees and representatives have a duty to protect individual's data from accidental disclosure:
  - Do not give out passwords to other people, who will then have access to the data you are entitled to view.
  - Do not recycle reports that contain Personal Information.
  - In particular, take due care to ensure that data is not left about on laptops or in files out of the office where they can be accessed by other people who are not Denave employees or representatives.
- In cases where sets of data are disclosed to non- Denave employees, for example external consultants carrying out specific reviews, employees must ensure that subjects have been informed of this use of their data, and why this is done. They must have had an opportunity to opt-out.
- Where sensitive data is involved, employees or representatives should not disclose data to outside agents except in cases agreed by the DPO.

15. SECURITY FOR PRIVACY

In order to safeguard privacy information, both electronic and physical, Denave shall have appropriate security safeguards such as

- Denave shall ensure that any Personal Information is appropriately and adequately secured, against loss, unauthorized access, use, modification or disclosure, and other misuse while at rest, in motion, and in process.
- Personal electronic data shall be subject to appropriate stringent controls, such as passwords, encryption, access logs, back-ups, etc.
- Screens, printouts, documents and files showing Personal Information must not be visible to unauthorized persons.
- Personal manual data must be held securely in locked cabinets, locked rooms, or rooms with limited access.
- Subject to retention guidelines, personal manual data shall be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PC, Denave personnel shall ensure the hard drive is cleaned by IT Team.
- Special care will be taken where laptops and PCs containing Personal Information are used outside the Company premises.
- Denave, on disclosing Personal Information to a Data Processor, shall do only under a written contract specifying the security rules to be followed.

The company's approach to Information Security Management is contained in separate policy/guidance documents.

Surveillance at Work

- Denave has a legitimate interest in monitoring the behavior of its employees. For instance, Denave may wish to carry out monitoring in order to:
  - Detect harassment or other inappropriate behavior;
  - Monitor performance of its staff where this is appropriate;
  - Monitor and detect the outward transmission of confidential information;
  - Prevent and detect theft of Denave property;
  - Prevent or detect any unlawful act.
- Monitoring can take several forms. It can involve monitoring by way of Closed Circuit Television (CCTV), e-mail and Internet monitoring.
- More detailed information about the monitoring of Internet and e-mail activity can be found in the 'Acceptable Use Policy'.
- CCTV Cameras
  - In carrying out such monitoring, Denave may use CCTV cameras in what are considered to be "public" areas of the workplace or in the work area's.
  - Denave may use the footage in disciplinary or other proceedings where appropriate.

16. DATA RETENTION AND DISPOSAL

Denave is committed to keep personal information for a minimum length of time as per the contract signed with client or timelines specified by regulatory body or only as long as it is needed to achieve the identified purposes.

Personal Information collected by Denave is destroyed when the use of Personal Information is no longer necessary for the purposes of processing. Destruction shall

- be in a manner sufficient to prevent unauthorized access to that Personal Information; or
- ensure that the Personal Information is anonymized

Reviews of personal and sensitive Personal Information shall be carried out at appropriate intervals to ensure cancellation or amendment of superfluous or out-of date material.

All print-out material, magnetic tape, diskettes, manual files, hand-written notes etc., which contain personal and sensitive Personal Information and are no longer required, will be treated as confidential waste and disposed of in accordance with the 'Policy on Record Management'.

Internal audit(s) is performed on a periodic basis to ensure that Personal Information collected is used, retained and destroyed in compliance with the 'Policy on Record Management' and other applicable policies and procedures to comply with applicable laws and regulations.

17. PRIVACY BREACH AND INCIDENT RESPONSE

Denave is determined to ensure that untoward privacy events/breaches associated with information, information assets and other business/ IT operations are communicated and managed in a manner allowing timely corrective actions to be taken. Denave has established a consistent and effective approach to the management of Privacy breaches/incidents within Denave.

Data Protection Officer (DPO) along with Data Protection Management Core group (DPMCG) shall respond to, analyze, and manages privacy incidents within Denave.

- **Individual Responsibility for Privacy Incident and breach**
  - Individual shall be made aware of their responsibilities in the event of a suspected Privacy weakness such as individuals will not attempt to prove (or test) the same. Such action on part of users shall be interpreted as a potential non-compliance to Denave policies and individuals found doing so may be liable to disciplinary action.
  - Individuals shall be responsible for reporting any observed (or suspected) privacy incidents, privacy breaches or any other incident immediately and shall not share such information with internal or external parties.
  - Individuals shall not include any personal data other than what is necessary to complete the initial reporting process.
- **Management of Privacy Breach and Incident**

  Privacy Breach and Incident Management shall comprise of five stages, which can be categorized as:
  - **Identify** : Report and Analyze.
  - **Handling:** Categorize, Notify and Document.

Identifying a Privacy Incident/ breach

A privacy incident is any successful or unsuccessful loss of control, compromise, or unauthorized disclosure, acquisition, access of personal information (PI)/personally identifiable information (PII) or electronic personally identifiable information (ePII).

A privacy breach is any successful compromise of protective controls, or unauthorized acquisition, disclosure, access of use of PI/PII or ePII which triggers reporting obligations under federal and/or state law to those individuals whose information was compromised.

Handling a Privacy Incident/ breach

Based on initial assessment of reported privacy incident/breach and analysis performed DPMWG, DPMCG and DPO shall work in conjunction to ensure successful closure of reported privacy Incident/breach.

- **Categorize**

  DPMCG shall categorize the Privacy Incident based on the level of potential harm to Denave. The categories are as follows:

Privacy Impact Level	Definition
Low – 1	Limited effect or consequences on business operations of Denave or on affected individuals.

Privacy Impact Level	Definition
Moderate - 2	Adverse effects on Denave's Global business operations, assets, and/or affected individuals.
High – 3	Serious adverse effects on Denave's Global business operations, market reputation, affected individuals.

For Privacy Incidents, not qualified as "Privacy Breach," measures should be taken up internally by DPMCG and DPO and the relevant stakeholders to address the violations through conduct of privacy impact and risk assessments and deploy remediation measures.

- **Notify**

  Wherever, the Privacy Incident qualifies to be a Privacy Breach, notification to affected individual(s) and/or client(s) and/or supervisory authority is the responsibility of DPMCG. DPMCG shall ensure that all the affected stakeholders are appropriately notified. Further, any notification shall be duly approved by the DPO.

  Some considerations that shall determine whether to notify individuals affected by Privacy Breach, include but not, limited to:

  - Legislations and data breach laws;
  - Contractual obligations;
  - Risk of physical harm;
  - Reputational Risk;
  - Risk of Identify Theft or Fraud;
  - Risk of loss of confidence among client, third party vendors and employees; and
  - Obligations as Data Controller or Data Processor

  Breach Notification shall also be dependent on the below roles that Denave plays:

  - **Denave as Data Controller**: Wherever applicable, under breach notification laws and regulations, Denave may notify the Data Protection Authority/Supervisory Authority and/or Data Subjects about the Privacy Breach, unless exempted.
  - **Denave as Data Processor:** Wherever applicable, Denave may require to notify the Client as per contractual commitments or applicable laws and regulations, unless Denave can reasonably conclude on the basis of investigation that misuse of the Personal Information compromised is unlikely to cause harm, and appropriate steps are taken to safeguard the interests of affected Data Subjects.

- **Document**

  DPMWG and DPMCG will work with relevant stakeholders to document all corrective action taken, including any steps to mitigate the harm. It is the responsibility of DPMCG to maintain a privacy incident log and track necessary action items with relevant stakeholders.

For a detailed procedure please refer the 'Privacy Incident and Data Breach management process'

18. TRAINING AND AWARENESS

Denave shall conduct periodic training and awareness sessions on privacy for employees, vendors and/or contractors who access and process the Personal Information of Data Subjects and Drive importance in meeting compliance with this Privacy and Data Protection Manual.

Below are the training requirements for ensuring consistent implementation of Privacy/Data Protectin framework across the organization:

- Induction training for Denave employees should carefully explain Denave's applicable Privacy/Data Protection policies;
- Appropriate questions on Privacy/Data Protection would be included in the annual ISMS Test.
- It is the responsibility of all the Privacy Champions to train and educate their respective teams in the Principles of Data Protection through training sessions.
- All project and function Privacy Champions will maintain records of these trainings. A brief capsule on Data Privacy would be conducted during the Denave's Induction Program.
- Periodic privacy policy training for vendors;
- Increase awareness of privacy and data protection using a variety of communication methods (such as, mailers, posters, website); and
- The process to identify and report privacy incidents, queries, grievances, and disputes should be clearly and consistently communicated to Denave employees.
- Employees should also be made aware of the contact details of the individual (DPO/DPMCG/DPMWG) to whom privacy related incidents, queries, grievances, and disputes shall be reported.

19. COMPLAINT/ GREVIENCE HANDLING

Denave is committed to monitoring and enforcing compliance with its privacy policies, applicable privacy laws, regulations and obligations. Denave is committed to:

- Addressing and resolving data privacy grievances in a timely manner (and always within the time lines prescribed by applicable laws);
- Implementing a comprehensive remediation process for data privacy breaches that fully addresses the symptoms which caused the data privacy breach;
- Identifying a Third Party arbitrator for dispute resolution, if applicable; and
- Conduct annual compliance audits of privacy policies, procedures, applicable laws, regulations, contracts and standards.

Denave has established and follows a formal process to address all such complaints and provide resolution in a timely manner. For more details please refer the 'Compliant handling procedure'. Further, if for any questions/suggestions about Denave's Data Protection Policy, please e-mail at privacy@denave.com.

20. EXCEPTIONS

All exceptions to this policy shall be directed to the Data Protection Management Core Group (DPMCG). DPMCG shall ensure that the exception request is formally recorded (using MyDen) with substitute controls which shall be put in place.

The exception shall be reviewed by Data Protection Officer (DPO) - and DPO shall take a decision to formally approve/reject the exception request. The validity of the exception shall be defined and shall not exceed one year. An annual review of all accepted exceptions shall be carried out by DPO and DPMCG team to identify any changes to the risk posed by the exception or to identify any alternate controls that may be implemented to reduce the risk.

21. ASSOCIATED DOCUMENTS

- Data Protection Organization Structure
- Information Security Policy
- Data Subject Request handling guidelines
- Data Inventory guidelines
- DPIA guidelines
- Third Party Data protection guidelines
- Acceptable Use Policy
- Policy on Record Management
- Privacy Incident and Data Breach Management process
- Compliant handling procedure