

**High Level Customer Centric Extracts from  
Data Privacy and Protection Policy**

**Tech  
Mahindra**

Sharda Centre, Off Karve Road, Erandwane,  
Pune, Maharashtra, India 411004

[www.techmahindra.com](http://www.techmahindra.com)

## 1. OBJECTIVE

Dependence on Data / Information is high in the present digitized and networked environment. At Tech Mahindra, (Here after it will be referred as TechM) this increases the risk of information being copied or stolen, or modified, hidden, encrypted, misused or destroyed. Although the defined controls provide an essential element of protection, these only deliver a percentage of the required protection, the most effective defense being achieved through awareness and good working practices.

This policy document forms TechM's **Data Privacy and Protection Policy** in support of the **Information Security Policy**. Compliance with this Policy will minimize the risk to information that is being compiled, used, transported, processed or held within/outside TechM premises and aligns with the Indian IT Act 2000, the EU Data Privacy Protection Directive, 1995, the UK's Data Protection Act 1998, the USA's Safe Harbor Principles and other related privacy principles and best practices.

The purpose of this policy is to define the requirements to safeguard personal data which includes Personal Information (PI) and Sensitive Personal Information (SPI), as defined below, related to TechM or its clients that are accessed or contained on any system, portable device and portable electronic storage media on or off TechM premises, and the procedures to be followed. This policy also explains how the most important PI and SPI which identifies TechM staff (also referred to as "associates" in this policy) will be used and processed by and on behalf of the TechM group.

In addition, the aim is to ensure that associates handling the PI or SPI are fully aware of the data privacy and protection requirements and handle it in accordance with the data protection procedures.

This policy must be read in conjunction with all other relevant Information Security policies, Data Security policies and HR policies as necessary. For the avoidance of doubt, nothing in this policy shall supercede the provisions regarding data protection and privacy contained in the data provided by the respective client or any related documents signed for the protection of such data including but not limited to:

- " In any Data Protection Policy provided by the Client to TechM;
- " Any Data Breach Policy provided by the Client to TechM;
- " In the agreement between the Client and TechM;

## 2. SCOPE

This policy covers PI or SPI held in (electronic & paper form) including that held in associated IT infrastructures such as software, networks, desktops, laptops, tapes (eg audio and CCTV) and servers at all TechM facilities.

## 3. APPLICABILITY

This policy applies to all business units and associates of TechM who create, store or access PI and/or SPI. This policy defines the minimum requirements for data privacy and protection which need to be complied with by TechM and its associates. Clients may adopt more stringent requirements depending on their in-country specific regulations and compliance on data privacy and protection. Whilst it is recognized that compliance with all aspects of this policy cannot be policed, those to whom it applies will be held accountable and responsible for any aspect of non-compliance involving them that subsequently comes to light under the Enforcement clause of this Policy.

### Definitions

**Business Requirements:** Requirements that can be traced back to the planning and execution of TechM's vision, mission, business goals and objectives, and its compliance to all relevant laws, regulations, policies and procedures.

**Personal Data - Or Personal Information (PI)** . (Also known as Personally Identifiable Information ) Any information that, when used alone or combined with other data, may be used to identify a living individual. This includes, but is not limited to:

- an individual's first and last name,
- an individual's Internet ID (not necessary his/her name)
- e-mail address,
- mailing and/or residential addresses,
- telephone number,
- title,
- birth date,
- gender,
- occupation,
- contact information,
- credit card or bank information,
- biographical information (where it is combined with information that identifies someone).

**Sensitive Personal Information (SPI)** - means any personal information like:

- password, (note even if applicable law may not categorise passwords as sensitive TechM does and you should treat them accordingly),
- national insurance number,
- social security numbers,
- race
- ethnic origin
- sexual orientation
- political opinions
- religious or philosophical beliefs
- trade union memberships that contains individual's health-related records (e.g. patient records, medical photographs, diet information, hospital information records, biological traits and genetic material),
- criminal records
- legal investigations and proceedings, etc.

**Processing** - is obtaining, using, holding, amending, disclosing, destroying deleting, transferring and any other activity with personal data. This includes some paper based personal data as well as that kept on computers.

**Data Subject** - is an individual who is the subject of personal data

**Data Controller** . :The Legal entities alone or with others, control the Purpose and manner in which the personal data are used, for example TechM in its role as Provider of employment and other related services/benefits to the employees

**Data Processor** - is someone who provides services to its clients and processes personal data on behalf of a data controller.( for example TechM in its role as a service provider to its clients)

**Portable Devices:** Electronic computing and communications devices designed for mobility, including laptop, desktop, tablets, smart phones, in-vehicle personal computers, personal data/digital assistants (PDAs), cellular phones, and other devices that have the ability to store data electronically.

**Portable Electronic Storage Media (Portable Storage):** Includes floppy disks, CDs, DVDs, optical platters, flash memory drives, backup tapes, USB HDDs, and other electronic storage media or devices that provide portability or mobility of data.

**Secured Storage Environment:** Data storage devices and support systems, such as direct attached server storage and Storage Area Network (SAN) devices, managed by our TIM team or provided explicitly under contract, and are secured by physical and logical means consistent with data storage best practices and TechM's Information Security Policy recommendations ensuring Confidentiality, Integrity and Availability (CIA).

#### 4. HIGH LEVEL POLICY

Personal/Sensitive Personal Data (PI or SPI) that is held or processed in any form including paper/electronic form within/outside TechM premises, related to TechM or its clients, must be protected appropriately and always in line with TechM's and its clients policies and procedures

Such data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in each case in line with the provisions of TechM policies and client senior manager directions. Physical access to and transmission and storage of PI or SPI shall be restricted to only those who require such access as part of their day to day job function.

TechM is committed to protect the PI or SPI of its associates as well of its customers, no matter where it is collected, transported, processed or retained within the scope of the applicable contractual as well as regulatory requirements.

#### 5. DETAILED POLICY

**If you require more detailed Policy, Procedure information on how TechM assures and ensures Data Privacy and Protection please write email to:**

[Corporateombudsman@techmahindra.com](mailto:Corporateombudsman@techmahindra.com).

#### Compliance

1. Associates shall note and comply with the applicable data protection and privacy laws and take note of the relevant guidelines and industry codes of practices and standards.
2. Compliance shall be indicated by individual and organizational adherence to the requirements and procedures of this policy and Data Privacy and Protection Directives of the Client.
3. In addition, associates need to undergo regular trainings on Data security and Privacy and be aware of the security procedures and control requirements as mentioned in the agreement and/or the regulatory requirements provided by the Client.
4. The internal Information security team to regularly audit and assess the compliance to the security and Privacy requirements and report it through Online Audit Management tools
5. All the Information Security and Privacy related incidents to be reported immediately through an Online Incident Management portal. Such incidents will be further escalated depending on the type of the incidents and the contacts for the relevant locations as defined in the TechM Incident Management Policy and procedure
6. With regard to breach of Security and Privacy policies, the organisation and individual may be liable for costs incurred as a result of loss, theft or unauthorised use of PI or SPI and remedy measures as relevant. The actions will be taken based on HR policy and Legal team's opinion regarding the issue.
7. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our IT and telephone systems including devices which we allow our staff to access and use are monitored. Further, TechM reserves the right to retrieve the contents of messages sent and searches made by and to inspect content stored on company owned devices. Monitoring is only

carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. If evidence of misuse of TechM and its group's IT systems is found, TechM may undertake a more detailed investigation in accordance with its disciplinary policy. If necessary, the matter may be referred to the Police Authority for criminal investigation. Investigations and disclosure of information to the relevant authorities shall be carried out in terms of the applicable laws.

8. In order to fulfil the Data Privacy laws and regulations , TechM reserves the right to disclose an individual's PI and SPI to law enforcement agencies, regulatory bodies and, government agencies as required by law or for statutory compliances .