Data Privacy & Cyber Security Policy

Tatva Chintan Pharma Chem Limited

Plot No. 353, Makarpura GIDC, Vadodara,

Gujarat – 390 010, India

1.Objective

At Tatva Chintan Pharma Chem Limited (hereinafter may be referred as "The Company" or "Tatva Chintan"), we recognize that all people have fundamental privacy rights and freedoms, and the company is committed to responsibly using Personal Information as reflected in the Code of Ethics. To help the company protect these rights and freedoms, recognize when you are collecting, handling, sharing or otherwise using Personal Information. This policy establishes company data privacy & information security principle.

2.Scope

This policy is applicable to:

I. All employees, contractors, third-parties, outsourced partners and personnel associated with Tatva Chintan whether in India or out of India.

II. All information Assets which include, but are not limited to: software assets, physical assets, paper assets, service assets, people assets and assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.

III. Tatva Chintan Pharma Chem Limited and Associate Companies.

3. Definition

3.1 Data Subject

I. All individuals whose personal information is either collected, received, processed, stored, dealt or handled by Tatva Chintan shall hereinafter be referred to as "Data Subject".

3.2 Information

I. Personal Information of a Data Subject collected by Tatva Chintan under this Policy shall hereinafter be referred to as "Information". Such Information includes, interalia, Sensitive Personal Data or Information as defined under the Indian Information Technology Act, 2000 and the

Aadhaar number and/or the biometric information associated with an Aadhaar number.

3.3 Information Security

I. Information Security is the protection of Information and Information Assets, from a wide range of threats in order to safeguard business and profits. It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

4.Principles

4.1. Be transparent

I. Describe in clear and simple language what Tatva Chintan does with Personal Information and communicate this at an appropriate time. By doing so, Tatva Chintan builds trust with whom we exchange data society.

4.2. Requirements

I. Explain what Personal Information will be collected, who is collecting it, why it is being collected, how it will be used, and who it will be shared with Communicate this at the time when Personal Information is collected (if possible) in a format that is easily accessible Consider whether it is appropriate (or required) to empower individuals with choices regarding what information they provide and how Tatva Chintan uses it.

4.3. Collect only what is necessary

I. Collect the minimum necessary Personal Information to further a specific, and legitimate, business purpose.

4.4. Requirements

I. Identify the specific purpose(s) for collecting Personal Information Ensure Personal Information is collected only for such purposes.

II. Consider whether the business purpose could be achieved with less Personal Information, and only collect the minimum data needed.

4.5. Use responsibly

I. Use Personal Information responsibly, meaning only in ways compatible with the purposes for which it was collected, and as communicated. This includes ensuring that the company only transfers such information across country borders where it is appropriate to do so.

4.6. Requirements

I. Use Personal Information only in ways consistent with any notice Presented.
II. Include appropriate data privacy protections in contracts where Personal Information will be handled by a third party.
III. When handling sensitive Personal Information, such as health data, recognize that enhanced data privacy protections may be needed.
IV. Honor individuals' preferences and privacy requests, including to access, delete, or correct their Personal Information, subject to local laws and requirements.
V. If local law allows transferring Personal Information across country borders, follow local requirements when transferring to third parties.

4.7. Protect and be vigilant

I. Follow applicable information security guidelines. Be on the lookout and immediately report any unintended use or disclosure of Personal Information.

4.8. Requirements

I. Classify Personal Information and store it according to the Information Security Risk Management
II. Prevent Personal Information from unintended modification, use, or disclosure
III. Keep Personal Information accurate and up to date
IV. Report any security incident or other unauthorized sharing, receipt, or handling of Personal Information at go/security incident

4.9. Retain only as long as necessary

I. Collect Personal Information only for specific business needs. Once the Personal Information is not necessary, it should not be kept unless needed to comply with legal obligations

4.10. Requirements

I. Follow records retention schedules for specific time frames for maintaining Personal Information
II. Delete Personal Information when no longer needed (unless otherwise required for legal reasons)
III. In some situations, anonymization may be used as an alternative to deletion

5. Internal Controls

Internal controls for this policy are closely monitored by Head-IT & Head-HR.

6. Breach of this Policy

Breaches of this policy can result in remedial, corrective, or disciplinary actions up to and including termination of employment. Actual or suspected incidents of misconduct should be reported. Tatva Chintan guarantees non-retaliation and confidentiality, to the extent legally possible, for good-faith reports of such breaches.

7. Exceptions

There are no exceptions to this policy.

8. Adaptations

There are no adaptations to this policy.

9. Data Privacy & Cyber Security Policy

I. **Network security**

At its simplest, network security refers to the interaction between various devices on a network. This includes the hardware and the software.Network security is a critical field of computer security that focuses on protecting the integrity, confidentiality, and availability of data and resources within a computer network. It encompasses a wide range of technologies, processes, and practices designed to safeguard a network infrastructure from various threats, vulnerabilities, and attacks. These threats can come from both internal and external sources and include things like hackers, malware, viruses, and unauthorized access.

II. **End-Point Security**

End-point protection software may include privileged user control, application controls, data controls, intrusion detection, and encryption. Encryption ensures the integrity of data being transferred, while application security controls protect against dangerous downloads on the user's end. Furthermore, security departments typically install such software not only on the device in question, but also on the company's server. When a security update occurs, the central server pushes the update to all end-point devices, thus ensuring a certain level of security uniformity. Likewise, having a central sign-in page allows enterprises to monitor who logs on and tracks any suspicious behavior.

III. **Internet Security**

In particular, Secure Sockets Layer (SSL) and Transport Layer Security (TSL) are forms of encryption and authentication commonly used by business for their online platforms. They create public and private keys when interactions with customers take place, ensuring the integrity of the data during transactions. Sites using such encryption methods will usually have *https* in the address bar along with a small lock icon. Other common security measures for the Internet include firewalls, tokens, anti-malware/spyware, and password managers.

Beyond network, end-point and Internet security, the introduction and expansion of the cloud and the extensive application market also warrants attention. Cloud security parallels on premise security procedures in that the goals are generally the same – to protect stored date and data in transfer. The main difference lies in the expansion of the security "border."

IV. DLP Security

Data Loss Prevention (DLP) refers to a range of measures, including strategies, tools, and processes, created with the purpose of averting the unauthorized disclosure, leakage, or loss of sensitive data within an organization. The fundamental objective of DLP solutions or Data Loss Prevention solutions is to safeguard data from being accessed, shared, or stored in an insecure manner, which could potentially result in security breaches, non-compliance with regulations, or harm to an organization's reputation.DLP systems typically encompass a blend of software, hardware, and policies that assist organizations in identifying, monitoring, and safeguarding sensitive data at every stage of their existence.

V. USB Security

USB blocking or USB endpoint protection is a data loss prevention (DLP) technique which aims at preventing the loss or leakage of crucial organizational data from various devices connected to USB ports. DLP USB blocking essentially allows the controlling and blocking of unwarranted access to removable storage media and prevents data theft via USB devices.

VI. E-Mail Security

We are establish Microsoft 365 Defender is a monitor and manage security across your enterprise. With the integrated alerts across identities, endpoints, data, apps, email, and collaboration tools - investigating and responding to threats now happen in a central.

VII. **Firewall Security**

Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet.

VIII. **Remote work**

Employees to work at home. Not only is this option cheaper for them, as it reduces overhead costs, but it also appeals to both young and old workers (e.g., less time in traffic appeals to older generations and less traffic is better for the environmental which appeals to younger generations). However, remote work expands the threat environment and makes it more difficult for IT departments to control.

There are a few steps every company can take to improve the safety of remote work.First, educate employees on the difference between suspicious emails and password protection. Likewise, emphasize the importance of utilizing a work computer only for work; the more programs (not work related) downloaded onto the computer, the more vulnerable the machine becomes.Second, provide a VPN for remote workers to help mitigate Wi-Fi breaches of your WiFi security having been krack'd and install the ability to remotely wipe the computer in the event the device falls into the wrong hands.

IX. **Application Security**

Concerned with securing software applications and preventing vulnerabilities that could be exploited by attackers. It involves secure coding practices, regular software updates and patches, and application-level firewalls.

The app must be installed from a trust-worthy platform, not from some 3rd party website in the form of other software.

X. **Cloud Security**

As organizations adopt cloud technologies, it's crucial to ensure that cloud providers offer robust security measures and to configure cloud services securely. Implement encryption, access controls, and other security features.

XI. **Data Backup and Disaster Recovery**

Reliable backup and disaster recovery solutions to ensure that data can be restored in the event of data loss, system failures, or security incidents.

XII. **Cyber security awareness & Employee Training**

Employee Training and Awareness: Educate your employees about data protection best practices and security policies, as human error remains a common source of data breaches. Cyber security awareness program and training for an organization's users is crucial to help protect against cyber threats and ensure that employees understand their role in maintaining security.

XIII. **Regular Auditing and Monitoring**

Continue audit and monitor IT systems for security vulnerabilities and incidents, and promptly address any issues that arise.

Thank You