Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential information of Alembic Pharmaceuticals Limited ("Alembic" or "the Company") and must be distributed to all the employees. All employees must read this document in its entirety and sign / electronically accept, confirming that they have read and understood this policy completely.

2. Scope of the Policy

This Information Security Policy ("the Policy") applies to all Employees, Contract workers, Business Partners, and all support members of the Company.

This Policy defines that all the users had to adhere to it, comply, and achieve a high level of IT security across all plants and locations.

3. Acceptable Use Policy & Compliance

The intentions for publishing this Policy is not to impose restrictions that are contrary to Alembic's established culture of openness, trust, and integrity. Management is committed to protecting employees, partners, and Alembic from illegal or damaging actions by individuals, either knowingly or unknowingly.

Any machine / equipment / instrument / network / software, which is generating any kind of computerized data is part of information technology. To install or implement any such devices / software / applications related to any kind of computerized data generation, it must be consulted and approved by the IT security cell.

An activity like hacking with computer systems; which includes destroying, deleting, or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously by any means; should be avoided.

All stakeholders shall carefully note that the foregoing acts are punishable offences under the law. If any such acts are committed by any employee of Alembic, Alembic shall have no alternative but to report the incident with full details to the law enforcement agencies including the police or any other cyber cell. In addition to reporting the incident to law enforcement agencies, Alembic reserves the right to take necessary disciplinary action against an erring employee, which may include summary dismissal without notice depending upon the gravity of the offence

It is a fundamental principle of the Company's security policy that all of the data and programs that are stored on or pass through the Company's computer and communication systems are the legal property of the Company and it should not copy / store / transmit information in any form outside of Alembic. If it is not for business purposes then appropriate approval shall be taken prior.

The Company intends that its computer and communication systems must be used for approved business purposes only. The Company may monitor your use of its computer and communication systems and other provided devices, including Internet access and sending and receiving email for compliance purposes and management has the right to access any data files stored on the Company's systems.

Postings of any blog or any content on any social media from a Companies email address or Company-related IDs to Newsgroups/Media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Alembic unless posting is in the course of business duties.

Do not install unauthorized software or hardware, including modems and wireless access unless or request approval from IT management before establishing any new software or hardware, third-party connections, etc.

All third-party companies providing critical services to Alembic have an agreed Service Level Agreement for the data management.

All third-party companies providing any support/assistance to Alembic IT, shall have to sign a Non-disclosure agreement.

4. Data Management

All data that we collect about the stakeholders will be, where applicable, recorded, used, and protected by us in accordance with applicable data protection legislation and/or this Policy. We may supplement the information that you provide with other information that we obtain from our dealings with you or which we receive from other organisations, for example, our sponsors and partners. Please note, if you don't choose to provide us with the requested personal data, we may not be able be offer you our products or services.

We may be required to use and retain personal information for legal and compliance reasons, such as the prevention, detection, or investigation of a crime; loss prevention; or fraud. We may also use personal information to meet our internal and external audit requirements, information security purposes, and as we otherwise believe to be necessary or appropriate for the business operations.

Alembic does not intend to store any data for a period which is beyond the intended purpose for which such data was collected or submitted, while also considering any applicable regulatory requirements and the data back-up and retention policy framed by Alembic.

All sensitive data stored and handled by Alembic stakeholders must be securely protected against unauthorized use at all times. Any sensitive data that is no longer required by Alembic for business reasons must be discarded in a secure and irrecoverable manner.

Alembic is not sharing or distributing any data including personal data to third parties without implementing appropriate safeguards. We shall use your personal data only if we have a proper reason for doing so. We may use available data for one or more of these reasons such as:

- To administer and provide products and services you request or have expressed an interest in and / or for the record-keeping purposes;
- Business requirements and have to share for completion of business operations;
- To respond to requests from law enforcement agencies and / or to public and government authorities, which may include such authorities inside / outside the country; or
- When it is in Alembic's legitimate interests and not harming others' interests.

5. Access to the Sensitive Data

Access to sensitive information in both hard and soft media formats must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

All Access to sensitive information should be controlled and authorized.

Access rights to privileged user IDs should be restricted to the least privileges necessary to perform job responsibilities.

Privileges should be assigned to individuals based on job classification and function (Role Based Access Control).

Alembic team shall ensure that there is an established process including proper due diligence in place before engaging with a Service provider.

Secure remote access must be strictly controlled and on a secure connection only with multifactor authentication.

Vendor accounts with access to the Alembic network will only be enabled during the period the access is required and will be disabled or removed once access is no longer required.

All hosts that are connected to Alembic internal networks via remote access technologies will be monitored as and when regularly depending on the activity.

All remote access accounts used are being reconciled at regular intervals and the accounts will be revoked if there is no further business justification.

6. Data Assurance

Alembic is committed for data security and taking all appropriate actions required and has deployed Next-Gen IT Security Tools & Technologies.

Alembic is doing due diligence to respect the privacy of all user's and customers' data. Alembic IT security cell is committed to maintaining a secure environment to ensure users' information meets a high level of security, with all possible and available tools and technologies.

Perimeter Firewall is installed to secured entire Network and Wireless Network is secured by enabling specific device ID and Managed through central Wireless Controller.

All Major security features are deployed including IDS, IPS, Sandboxing and IPSEC tunnelling for services providers.

USB Access is by default blocked in all the endpoints and as per the exceptional requirement and approval, specific system will be provided USB access for required period.

Email gateway is set up for SAPM management and E-Mail access with internal and external access provided to specific employees considering his / her work area and eligibility.

Next-Gen Antivirus is installed in all endpoints equipped with AI / ML enabled features.

Internet Access is provided to employee as per eligibility and his / her roles and responsibilities.

All user IDs for terminated users are deactivated or removed immediately.

All non-console administrative access will use appropriate technologies like SSH, VPN, SSL, etc. is required authentication.

System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.

Centralized Password policy is configured for all end points are required to use password for login and forcefully password change with complex password policy is implemented for users.

Alembic has already considered having appropriate insurance measures to protect the financial interest of Alembic and its stakeholders.

7. Store, Process, Secure Data

All sensitive data must be protected securely if it is to be transported physically or electronically.

To protect against physical attacks, all critical server are hosted in secured data center with access control system.

If there is a business justification to send very critical data via email, internet or any other modes then it is done using secure manner like https, IPSec, sftp, etc.,

Backup procedure is well defined and applicable to all data including GxP computerized systems where electronic data are generated and stored. Data for backup is categorized in different categories like SAP systems, DCS/ DMS systems, Chromatography Data Systems (CDS), and Non-Chromatography Data Systems (Non-CDS) and policies are defined as per the requirement for the retention.

Separate backup and retention policy is implemented to secure the data in case of any disaster.

All data are securely disposed of when no longer required by Alembic, regardless of the media or application type on which it is stored.

Hard Disks are manually destroyed when no longer required for valid and justified business reasons.

Alembic has procedures for the destruction of hardcopy (paper) materials for all critical location at the plants where it requires that all hardcopy materials are shredded and/or incinerated, as the case may be, so they cannot be reconstructed.

8. Disclosure on Data Sharing

Our businesses around the world are supported by different teams and functions and it may require to made personal information available to them if necessary for the provision of Services, account administration, sales and marketing, customer and technical support, and product development or for Human Resources perspective.

We may share data including personal with vendors, service providers and other trusted third parties based inside or outside of the country, so that they may process that data on our behalf as necessary, in connection with providing our products and services, and / or to fulfil contractual arrangements and legal or regulatory requirements.

Alembic reserves the right in its sole discretion to enlist a third party to audit contractor's findings and produce an independent report, and the contractor will fully cooperate with the third party. The contractor will also comply with Alembic policies and any other state and federal rules and regulations regarding security of information.

9. Incident Reporting & Response Plan

'Security incident' means any incident (accidental, intentional, or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money or just to damage our Company.

Stakeholders are expected to report any security-related issues IT Security Team. Incident Response and Management Policy is defined by IT as reported problem will be handled as per the incident severity which is defined in the policy

Incidents can be reported on: itsecurity@alembic.co.in

10. Contact Information

You can contact our IT security team for any question, suggestions and comments related to this document on itsecurity@alembic.co.in

11. Changes to Policy

This Policy shall be reviewed regularly and updated by the Board of Directors and persons duly authorised by it, as and when it is required to include newly developed security standards or to change any aspects of the existing policy, with a minimum review frequency of once every three years. The new policy / document may be published and / or distributed to the respective stakeholders as per the requirement.

*****

15/7/25
Head
IT

15/7/25
Mr. Manoj Desai
Chief Technology & Information Officer
(Head of Department-IT)
Alembic Group of Companies

J.K. Khuntia
15/07/25
Head
ESG