GOOD PEOPLE
for GOOD HEALTH

J.B. CHEMICALS AND PHARMACEUTICALS LIMITED

Information Security System & Cyber Security Policy

Information Security System & Cyber Security Policy

Information Security System & Cyber Security policy	Name	Date	Signature
Approved by: JB Pharma ESG Team	Mr. Jason Dsouza	22-11-2023	
Approved by: JB Pharma : President Operations	Mr. Kunal Khanna	02-12-2023	
Approved by: KKR ESG Team	Mr. Akshit Thaman / Ms. Erika Rodriquez	09-12-2023 / 12-12-2023	Approval on email
Approved by: JB Pharma CEO & Whole -Time Director	Mr. Nikhil Chopra	13-12-2023	

Nature of changes: New Policy

Reason: Given the concern around data privacy & cyber security we, we have follow global standard protocol to safe guard our system by enabling robust information network in place, which helps us to protect from any cyber threat or data breaches.

Table of Contents

Information Security

Information Assets

1. JB PHARMA in its normal course of business generates data and this data when assimilated constitutes information. This information, when analysed may give the reader, ample knowledge of the way we operate, the reasons for our success, and the key contributors to our market leadership position.

2. Over the years, the information ecology in which we operate has transformed. The complexity of systems to be managed has become greater. It is time to move to a new paradigm of information security management to protect our information assets in the new Information ecology.

3. Information assets are defined as media or systems that contain or carry information during its creation, processing, transmission, storage, and destruction. Information can exist in many forms. It can be printed or written on paper, stored electronically or in human memory as Knowledge, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

4. Information security is characterized as the preservation of

   4.1. Confidentiality: Ensuring that information is accessible only to those authorized to have access.

   4.2. Integrity: Safeguarding the accuracy and completeness of information and processing methods.

   4.3. Availability: Ensuring that authorized users have access to information and associated assets when required.

Policy

5. We at JB PHARMA recognize that Information is one of our most important assets. In an extremely competitive market, the achievement of our business goals depends on our ability to safeguard Information and ensure its Confidentiality, Integrity, and Availability.
6. Information Security at JB PHARMA is a management responsibility. All business heads/ department heads are directly responsible for ensuring compliance with our information security policies in their respective domains and the Group Management Committee has the overall responsibility for the implementation and maintenance of Information Security.
7. Information Security is not only a management concern and our ability to achieve high levels of security depends on all employees of the organization understanding the value of Information and appreciating that it is in their individual and collective interest to protect it in whatever they do.
8. All of us in JB PHARMA Industries and Associated Companies are committed to ensuring the Confidentiality, Integrity, and Availability of our information assets and to following the practices specified in our Information Security Policy.

Data Protection and Privacy

1. All the employees will be responsible to provide adequate safeguards to protect data and information within JB PHARMA. The Group Management Committee (GMC), will provide guidance to functional Heads on individual responsibilities towards data protection and privacy. The functional Heads will be responsible to inform the IT team about the storage requirements for information and controls required for protection and privacy of information.
2. We have incorporated information security/cybersecurity as an essential component of our employee performance evaluation process. This means that employees' adherence to information security policies and practices, including compliance with relevant regulations and standards, will be assessed, and considered during performance evaluations. Failure to meet the required standards may result in disciplinary actions, which could include retraining, warnings, suspension, or even termination, depending on the severity and frequency of the violations.
3. The objective of this is to ensure security and privacy of Personally Identifiable Information (PII), Sensitive Personal Identifiable Information (SPII) and Personal Health Information (PHI) gathered, stored and/or processed by JB PHARMA.
4. Business/ Unit Head must ensure that appropriate controls are applied while storing and handling PII.
5. Department heads within Businesses must identify list of PII being shared with third party/vendors.
6. Businesses must take into account local laws and regulations before sharing PII with any third party.
7. When data is shared with third party, a written agreement or contract between the Business and third party must be created.
8. Department head must ensure that only minimum required PII is disclosed to third parties.
9. Business/ Unit Head must ensure that strong encryption technology, is used while transferring PII within the organization or to third party as applicable.
10. PII must be securely disposed-off securely after the expiry of its retention period.

11. GMC must ensure that privacy trainings are imparted to all concerned users on a regular basis.

12. IT has ensured that data related to GMP applications, applications softwares, databases, end user files available on their machines and or on file servers are backed up regularly. SAP runs on a cluster environment in primary and secondary mode where as its DR instance is kept at Panoli.

13. GMP application databases are mirrored and that means if one fails other latest backup is available. It is the only recovery time that matters but there is no loss of data. GMP databases are backed up on the enterprise level CommVault server and local backup is also kept.

Visibility for ISMS Documentation

9. The ISMS documentation, which includes the policies, procedures, and standards, will be published with appropriate access controls as per need to know basis, on the company intranet.

10. The documents will be version controlled and the latest version of the documents will be published.

Scope

11. Applicable to all units of following Companies

    All operating sites of JB PHARMA

Responsibilities

12. The following administrative bodies and personnel along with other identified personnel will address and implement this ISMS initiative:

    12.1. Group Management Committee

    12.2. Corporate Information Security Officer

    12.3. Business Information Security Officer/Unit Information Security Officer

    12.4. Department Representative

    12.5. Corporate Quality Assurance

13. The roles and responsibilities of the above teams are described in the Information Security Organisation Policy.

Reporting Suspicious Activity

14. We established a clear escalation process for employees to follow if they notice something suspicious in the IT environment. Employees are encouraged to report any suspicious activities, security incidents, or potential breaches to their immediate supervisor and use the following reporting channels, Email: helpdeskit@jbpharma.com Hotline: 022 2439 5318 / 317.

Audit Checkpoints

15. The audit checkpoints for this policy shall be as following:

    15.1. Information Security Policy Document duly signed by the management

15.2. Information Security Policy communicated and published on the intranet 15.3. Minutes of the meeting for the ISMS review and discussion

Cross References

16. This policy is the first policy of ISMS. It will be supported by all other policies and procedures established in the ISMS. These polices are under development and will be finalised during the ISO 27001 implementation effort in Q3-Q4 of 2021-22.

16.1. Information Classification Policy

16.2. Information Security Organisation Policy

16.3. Information Security Verification & Validation Policy

16.4. Information Security Education & Training Policy

16.5. Handling of Classified Information Procedures

16.6. Risk Assessment Policy & Procedures

16.7. Incident Management Policy & Procedures

16.8. Acceptable Usage Policy

16.9. Physical Security Policy & Procedures

16.10. Photo/Access Badge Issue & Retrieval Policy & Procedures

16.11. Use of Electronic Office Equipment Policy & Procedures

16.12. Third-Party Access Policy & Procedures

16.13. Personnel Security Policy & Procedures

16.14. Coding Scheme Policy & Procedures

16.15. Internet Access Security Policy & Procedures

16.16. Email Security Policy & Procedures

16.17. System Access Control Policy & Procedures

16.18. Password Security Policy & Procedures

16.19. Capacity Planning Policy & Procedures

16.20. Log Monitoring Policy & Procedures

16.21. Systems Security Policy & Procedures

16.22. Application Security Policy & Procedures

16.23. Mobile Computing & Teleworking Policy & Procedures

16.24. Protection Against Malicious Code Policy & Procedures

16.25. Backup, Restoration & Media Handling Policy & Procedures

16.26. Network Security Policy

16.27. Software Copyright Compliance Policy & Procedures

16.28. Equipment Security Policy & Procedures

List of Records

17. The list of records for this procedure is as follows:

17.1. GMC minutes for discussion on Information Security

17.2. Information Security Policy Document signed by the management.

Glossary

18. Not Applicable

Guidelines

19. Not Applicable

Annexure

20. Not Applicable

Document History

Version	Approved by	Date of Approval / Amendment	Nature of changes
1	KKR ESG Team: Mr. Akshit Thaman / Ms. Erika Rodriquez	09-12-2023 / 12-12-2023	New policy*
	JB PHARMA CEO & Whole-Time Director: Mr. Nikhil Chopra	13-12-2023	