1.1 Objective: To protect Lee Pharma's information assets from unauthorized access, disclosure, alteration, or destruction, ensuring business continuity and regulatory compliance.

1.2 Scope: This policy applies to all employees, contractors, vendors, and third-party partners who access or manage Lee Pharma's information systems and data.

1.3 Commitment: Lee Pharma is committed to maintaining a secure digital environment through proactive risk management, employee awareness, and continuous improvement of security controls.

2. Governance & Roles

2.1 Information Security Governance: Oversight is provided by the Information Security team, which defines strategy, policies, and risk tolerance.

2.2 Roles & Responsibilities: All employees are responsible for safeguarding information. Specific roles such as IT, HR, and Compliance have defined responsibilities for implementing and monitoring controls.

2.3 Policy Enforcement: Violations of this policy may result in disciplinary action, including termination or legal consequences, depending on severity.

2.4 Third-Party Compliance: Vendors and partners must adhere to Lee Pharma's security standards as part of contractual obligations.

3. Data Classification & Handling

3.1 Classification Levels: Information is categorized as Public, Internal, Confidential, or Restricted based on sensitivity and impact.

3.2 Handling Guidelines: Each classification level has defined rules for storage, access, transmission, and disposal of data.

3.3 Labeling & Access: All sensitive documents must be labeled appropriately, and access must be restricted to authorized personnel only.

3.4 Data Minimization: Only the minimum necessary data should be collected, retained, and shared to reduce exposure.

4. Network & System Security

4.1 Perimeter Defense: Firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways are deployed to protect the network.

4.2 Endpoint Protection: All devices must have antivirus, encryption, and patch management tools installed and regularly updated.

4.3 Secure Configuration: Systems are hardened based on industry best practices and regularly reviewed for vulnerabilities.

4.4 Remote Access: VPNs and secure tunnels are required for accessing internal systems from external networks.

5. Data Protection & Privacy

5.1 Encryption: Sensitive data must be encrypted at rest and in transit using approved cryptographic standards.

5.2 Data Privacy: Personal and health-related data is handled in compliance with applicable data protection laws (e.g., GDPR, HIPAA).

5.3 Retention & Disposal: Data is retained only as long as necessary and securely disposed of when no longer needed.

5.4 Third-Party Data: Vendors handling sensitive data must demonstrate equivalent data protection measures.

6. Business Continuity & Disaster Recovery

6.1 Continuity Planning: Business continuity plans (BCPs) ensure critical operations can continue during disruptions.
6.2 Employee Awareness: Staff are trained on their roles during emergencies and participate in periodic drills.

7. Training, Awareness & Compliance

7.1 Mandatory Training: All employees must complete annual information security training and periodic refresher courses.
7.2 Policy Acknowledgment: Employees must acknowledge understanding of this policy and related procedures.
7.3 Audits & Reviews: Internal and external audits are conducted to assess compliance and identify improvement areas.

8. Review and Update

This information security policy is reviewed internally as per the review date mentioned for adherence and updated (if necessary) for applicability, relevance, and effectiveness.