EPACK Durable Limited

Information Technology Security Policy

Objective

The objective of this Information Technology Security Policy ("IT Security Policy" or "Policy") is to ensure that EPACK Durable Limited ("Company", "EPACK", which term shall deem to include its subsidiaries) establish a comprehensive security framework to protect the organization's information assets, operations, and personal data.

Scope

The scope of this IT Security Policy encompasses all facets of the Company's technological and physical environment:

a) Personnel: It applies to all employees, contractors, partners, and any entity related to EPACK Durable including subsidiaries.

b) Systems and Devices: The Policy covers all accounts and systems, including network devices, standalone systems, application databases, and servers

c) Data and Information: It includes all personal data (electronic or non-electronic), business-critical information, software, and sensitive data such as PII and financial records

d) Physical and Virtual Locations: The scope extends to the physical office premises as well as virtual environments, including Work from Home (WFH) setups, VPN connections, and social media/Internet channels.

Definitions

a) "Information Assets" shall mean all data, systems, applications, devices, and infrastructure owned or used by the Company.

b) "Personal Data" shall have the meaning assigned under applicable data protection laws including the Digital Personal Data Protection Act, 2023.

c) "User" shall mean any individual accessing Company systems including employees, contractors, and third parties.

Roles and Responsibilities

a) The IT Head shall be responsible for implementation, monitoring, and enforcement of this Policy.

b) Department Heads shall ensure compliance within their respective functions.

c) All users shall comply with the requirements of this Policy and report any security incidents immediately.

d) The Management shall provide necessary resources to implement and maintain information security controls.

1. Physical Access Control

The objective of physical access control is to prevent unauthorized physical access, damage and interference to the organization's information, information processing facilities and prevent loss, damage, theft or compromise of assets or interruption to the organization's operations.

a) Physical access controls must be implemented to provide entry within the premises only on a need basis.

b) An access register or log must be maintained for recording the entry in and out of the office for the non-employees.

c) The above log must record the name, official address, purpose, signature, entry time and exit time for all non-employees entering the premises.

d) All visitors must wear visible visitor ID badges or passes and must be accompanied by the employee while on office premises.

2. Logical Access Control/User Role

The objective of Logical Access Control is to define key user life cycle management processes for physical and logical access control within the company. Any of the personal data stored in electronic or non-electronic form must be protected through suitable physical and logical access control mechanisms. Access to personal information must be provided on a need-to know basis.

a) It has to be ensured that all computerized systems must require minimum a username and password combination, before granting access to the system.

b) The passwords on all computer accounts must conform to the complexity requirements and it must be changed periodically. For every new employee, the Human Resources function must, initiate the user ID creation process by filling up the User ID Registration Form.

c) Forward the request for user ID authorization to the respective Functional Head for approval.

<u>On the designated last date of the employee/contractor, the IT Teams must</u>:

a) Change/disable passwords of accounts that the departing employee or third-party user had access to;

b) The user ID/Password must be retained first for a certain period. This period must be determined by the Functional Head of the concerned employee after considering the criticality of the concerned employee/role;

c) The data contained in the login must be backed up and handed over to the concerned Function Head;

d) Remove all access assigned to the respective user ID

e) Delete the entry in the user ID access list; and

f) Notify the respective Function Head, HR Functions about the successful revocation.

3. Password Protection

The password protection would be applicable for all users, accounts and systems including network devices and standalone systems. Passwords shall be a minimum of 12 characters in length and must include a combination of uppercase letters, lowercase letters, numbers, and special characters.

4. Cyber Security

Controls implemented on the information systems must be capable of addressing the latest vulnerabilities and insecurities that could bring the system down or result in information disclosure or destruction.

a) All systems within Organization must be configured with the Anti-virus software

b) Users must not have access to their anti-virus product's configuration

c) The anti-virus product configuration for all systems must be determined by the IT Department

d) Anti-virus products must be configured to update in a timely manner on all systems after the vendor has released a new definition file

e) Any file transferred electronically into the Organization's computer environment or from the Internet must be scanned for virus infection before, during or immediately after the transfer

5. Vulnerability and Patch Management

All systems shall be regularly updated with security patches. Critical patches shall be applied within 7 days, and others within 30 days of release. Periodic vulnerability assessments and annual penetration testing (VAPT) shall be conducted.

6. Digital Signature

The objective is to identify security controls for handling and protection of Digital Signatures. Whenever there is a business and/or legislative need, an employee must authenticate an electronic record by affixing a digital signature.

Emails that are very important or have financial or security implications should be sent with a digital signature for non-repudiation and should be encrypted.

Digital signature must be obtained after due approval of the IT Head/CEO and it must be attached on all documents/communications as approved by IT Head/CEO.

7. Social Media

The objective is to define the acceptable use Policy for use of social media communication channels by an employee, contractor, partner or any entity related to EPACK Durable, particularly in relation to how EPACK Durable related content is publicized and disseminated using social media and Internet channels.

a) Employees must be responsible, accountable and legally liable for any content that they may post on social media websites. Any views and posts must be understood to be the personal opinion of the individual and must in no way be construed as the opinion of the Company/Management.

b) Employees must not reveal any confidential information relating to EPACK Durable or pertaining to business including but not limited to that of clients, vendors and other associates.

c) Employees must not disclose any information – whether words, images, logos or videos – that are confidential or proprietary to EPACK Durable.

d) Unless expressly authorized, employees must not express opinions about company revenue, profits, future plans, clients or suppliers whether or not he / she has directly identified oneself as an employee of EPACK Durable.

e) Employees must not reveal any personal information of other employees/colleagues (e.g. DOB, Marital Status, Health Information, etc.) on social media sites.

8. Backup

The objective is to ensure that in the event of a disaster, all business-critical information or software can be restored within the recovery time objective.

a) EPACK Durable must have a documented backup and recovery procedures for critical information and information systems.

b) Business/ Unit IT department with relevant stakeholders must identify backup and restoration requirements for information within the Unit. The identification process must be in line with business requirements, legal requirements, contractual obligations, regulatory implications, vendor recommendations and other relevant factors.

c) All applications and operating systems software, data (including databases), application and operating system configuration information, hardware configuration information (where applicable) and log files/ logs from various systems that need to be backed up must be identified and documented.

d) The backup and recovery procedures must be monitored regularly.

e) Backups must be tested periodically to check data integrity of the backup and also the ability to restore data in the event of an actual emergency.

f) The Data backups must be performed at least every 12 hours. Disaster recovery mechanisms must be implemented and maintained to ensure timely restoration of data and minimize the risk of data loss.

9. Data Security

The Company shall implement technologies to monitor and detect the movement of sensitive data within the organization's network. This could involve network monitoring tools, endpoint protection security, and data loss prevention software.

a) Access Controls: Enforcing strict access controls to limit who can access sensitive data and under what circumstances. This includes user authentication and role-based access controls.

b) Employee Training Awareness: Educating employees about the importance of data security and providing training on how to handle sensitive data securely.

c) Incident Response Procedures: Establishing procedures for reporting and responding to data leakage incidents, including investigation, containment and remedy.

d) Restricted Access: No access of application databases and servers outside office premises without an approved VPN.

e) Identification of Sensitive Data: Classifying data based on its sensitivity level. For example, personally identifiable information (PII), financial data, intellectual property, etc.

f) Data Classification: Information shall be classified into categories such as Public, Internal, Confidential, and Critical based on sensitivity and impact.

g) Data Retention: Data shall be retained only for as long as necessary to fulfill business, legal, or regulatory requirements and shall be securely deleted thereafter.

h) Data Encryption: Sensitive and personal data shall be encrypted both at rest and in transit using industry-standard encryption protocols.

i) Personal Data Breach Notification: In the event of any personal data breach, as defined under the Digital Personal Data Protection Act, 2023, the IT Head shall ensure that the incident is reported to **Data Protection Board of India** and all affected Data Principals in the form and manner prescribed under the DPDP Act, 2023 and rules made thereunder. A record of all such breaches, mitigation measures taken, and notifications made shall be maintained by the IT Department.

10. Breach and Consequences:

Any employee, contractor, or third party found to be in violation of this Policy shall be subject to disciplinary action, which may include warnings, suspension, or termination of employment or contract, depending on the nature and severity of the breach. Violations involving criminal conduct, including unauthorized access, data theft, or deliberate sabotage, shall be referred to the appropriate law enforcement authorities. All users are required to cooperate fully in any investigation of a security breach.

11. Review and Amendments

This Policy shall be reviewed periodically to ensure its continued alignment with applicable laws, regulatory requirements, industry best practices, and the evolving information technology and cybersecurity landscape. The Managing Director of EPACK Durable Limited shall have the authority to amend, modify, or update this Policy, as may be necessary, from time to time.

12. Version Control

Version	Description	Date
Version 1	Information Technology Security Policy	August 11, 2026