INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

S. No.	Type of Information	Document Data
1.	Document Title	Information Security Management System (ISMS) Policy
2.	Date of Revision	Oct 21, 2022 20, 2020
3.	Document Version No.	V 1.7
4.	Document Owner	Cyber Security & S/W Compliance Team
5.	Document Author(s)	Program Manager - Cyber Security & S/W Compliance
6.	Document Approver	CTO

TABLE OF CONTENTS

1. PURPOSE

The purpose of this policy is as below:

- This policy serves as a guide to ensure the confidentiality, integrity and availability of Delhivery's information systems.
- To ensure the proper and lawful use of the Delhivery's Information Technology environment (IT environment)

2. SCOPE

This policy applies to all information, information systems, networks, applications, locations and users of Delhivery or supplied under contract to it.

3. POLICY STATEMENT(S)

Delhivery is committed to safeguard the Confidentiality, Integrity and Availability of all physical and electronic information assets of the organization to ensure that regulatory, operational and contractual requirements are fulfilled.

3.1 Information Security

3.1.1 Security goals

The overall goals for information security at Delhivery are the following:

- Ensure compliance with current laws, regulations and guidelines.
- Information is protected against unauthorized access and confidentiality of information is maintained.
- Ensure Integrity of information to maintain accuracy throughout the data lifecycle.
- Availability of information to authorized users when needed.
- Information security training is given to all employees to motivate them to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure business continuity even in case of a disaster.

3.2 Roles and Areas of Responsibility

Delhivery has established an Information Security Team to implement, maintain and continuously improve the Information Security Management Systems (ISMS).

Information Security Team:

- InfoSec Team includes :
  - Cyber Security and S/W Compliance team
  - IT Operation team

- Information Security team reports to C-Suite (Ex - CTO / CIO / CISO)

- **Infosec Team is responsible for:**

  - Establish policies, objectives and plans to achieve information security and data privacy and seek approval from the CTO / Steering Committee.
  - Ensuring the suitability, adequacy and effectiveness of the ISMS by conducting periodic reviews of Delhivery's security controls.
  - Identify and mitigate information security and data privacy risks at organization level.
  - Ensure that arrangements that involve external organizations having access to Delhivery's information and / or information systems are covered under contractual liabilities to secure Delhivery's information and information systems.

Information Security Steering Committee :

- Steering Committee includes :
  - CTO
  - CFO
  - COO
- **Responsibilities of Steering Committee:**
  - Review and approve strategic plans for information security.
  - Report Information Security risks to the board of directors.
  - Oversee major initiatives and allocate resources to achieve infosec goals.

4. Human Resource Security

- Screening or background checks must be performed at time of hire.
- Employees shall sign the organization's terms and conditions of employment that includes the employee's and the organization's responsibilities for information security, at the time of hire.
- Employees must take Information security and Data Privacy training at the time of hire and annually thereafter, or as per the business needs.

5. Asset Management

- Delhivery's information assets must be appropriately protected from theft, loss or any unauthorized access. Assets may include but not limited to :
  - Documented business processes and activities (electronic or physical)
  - Electronic information (data, spreadsheets, presentations, documents, notes, email, social media, etc.)
  - Physical information (papers, signs, posters, etc.)
  - Hardware (servers, laptops, desktops, printers, photocopiers, routers, switches, firewalls, mobile phones, tablets, computing devices, etc.)
  - Software (databases, applications, utilities, productivity software, cloud services, etc.)
  - Network (communication links, wired network, wireless network, etc.)
  - People (employees, contractors, interns, etc., as defined in this policy)
  - Facilities (offices, data centers, server rooms, wiring closets, storage facilities, studios, etc.)
- An accurate and up-to-date inventory of critical assets must be maintained. Critical assets are those, which if compromised or lost, could cause significant business disruption or revenue loss. An asset owner must be designated for each inventoried critical asset, though assets remain Delhivery's property.
- Refer "IT Asset Management Standard" for further details.

6. User access management

- Access to Delhivery's information, information systems (Infrastructure, applications, source code repositories) and information processing facilities shall be controlled to prevent unauthorized access.
- Access shall be granted considering least privilege principle and on need to know basis only.
- Logs should be maintained for access granted to critical systems.
- Refer 'User Access Management Process' for further details.

7. Cloud Infrastructure Security

- Delhivery's IT infrastructure is set up on AWS and ensures high availability, scalability and security of its application and data.
- All access to the servers and managed services is private, unless proxied through a public secure resource.
- Internal vulnerability assessment is performed at regular intervals.
- Only authenticated users are allowed to access Delhivery's Cloud Infra (AWS).
- All security best practices are adhered to, as advised by AWS.

8. Physical and Environmental Security

- Physical and environmental security requirements must be considered during design, buildouts or improvements of existing Delhivery facilities to protect against natural disasters, unauthorized access, malicious attacks and accidents.
- Access to Delhivery facilities must be restricted to authorized people only.
- Security barriers must be deployed at Delhivery facilities to protect the physical security perimeter consisting of walls, fences, doors, ceilings, floors, etc., to prevent unauthorized access, damage and interference.
- Where applicable or determined by business requirements, photo identification badges must be issued. People must wear or display badges when asked to do so.
- Visitors must be granted access to Delhivery facilities for business reasons only. Records of visitors to Delhivery facilities must be maintained. As appropriate, visitors must be escorted within Delhivery facilities by a Delhivery person and display temporary identification, if issued during their visit.
- The delivery and loading areas must be monitored for unauthorized access and incoming and outgoing materials must be registered
- Safeguards must be applied and regularly tested to prevent or mitigate damage to Delhivery facilities from fire, flood, earthquake, lightning and other natural and manmade disasters.
- Information processing facilities must be monitored for environmental conditions including temperature and humidity.
- Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference and damage, wherever possible.

9. EQUIPMENT SECURITY

- Equipment must be protected to minimize potential risks such as theft, fire, explosives, smoke, water, dust, vibration, electrical supply interference, electromagnetic radiation, vandalism and unauthorized access.
- Equipment must be protected from power failures and other disruptions caused by failures in electricity, telecommunications, ventilation, air conditioning, etc.
- Equipment supporting the business processes must be maintained and tested regularly according to manufacturer recommended service intervals. Maintenance records must be maintained.
- Equipment, except assigned portable/mobile devices such as laptops, mobile phones and tablets, must not be taken off site without approval. Records of incoming and outgoing equipment must be maintained and reviewed periodically.
- Appropriate protection must be applied to protect laptops, mobile phones, tablets, etc., while working remotely from home or other offsite locations.

10. APPLICATION SECURITY

- Application security testing shall be performed at regular intervals to find and fix any issues/vulnerabilities. Refer “Application Security Testing Policy” for further details.
- Changes to applications shall be performed through defined processes and requisite approvals to ensure security during change management activities.
- Only approved, tested and authorized changes shall be made to the applications.
- Changes shall be reviewed periodically by the respective Product manager/Engineering Manager to ascertain whether appropriate change management processes were followed or not.
- Refer ‘Change Management Process’ for further details.

11. VENDOR SECURITY MANAGEMENT

- Vendor's access to Delhivery’s information/information assets shall be restricted.
- Ensure a vendor risk assessment is performed to validate the adequate security controls of the vendor having access to Delhivery's critical data.

- Where third parties are involved in processing of Personal Data it must be ensured that due diligence is performed with respect to data security and privacy. It must also be ensured that data privacy obligations that are applicable to Delhivery are transferred to the third parties
- Refer “Tech Vendor Engagement Manual” and “Vendor - Security Audit Checklist” for further details.

12. Incident Management

- Delhivery shall implement procedures for detecting, reporting and responding to incidents. The incidents shall be reported in time to the appropriate regulatory authorities and corrective actions shall be taken immediately to avoid the recurrence of such events in future. All reported incidents shall be logged, analyzed and classified according to predefined criteria. Escalations and actions shall be as per the classification of incidents.
- All incidents shall be reported in a timely manner at infosec@delhivery.com and corrective actions shall be taken immediately as per procedures to avoid the recurrence of such events in future.
- Refer “Technology - Incident Response Process” for further details

13. Business Continuity management

- Delhivery shall plan for and implement the controls to mitigate the impact of disaster and timely resumption of business activities and information security.
    - Delhivery shall provide direction and support for business continuity
    - Set the organizational requirements and expectations for business continuity
    - Guide the implementation of appropriate policies, standards, processes, procedures, plans and controls necessary to recover functions within the organization
    - Define the roles and responsibilities of employees towards business continuity
- Perform annual mock drills of the business function to keep the Business Continuity measures up to date
- Refer “Business Continuity, Disaster Recovery Planning & Disaster Management” for further details.

14. Personal Data Protection

A. Privacy Notice

Where Delhivery collects Personal Data of an individual a privacy notice must be provided to the Data Subjects prior to collection. All privacy notices should be approved by the Cybersecurity team before being published.

B. Consent Management

Data Subjects should be required to provide an explicit consent (such as selecting a checkbox) prior to submitting their Personal Data to Delhivery. Consents provided by the Data Subject should be logged along with the date and timestamp.

C. Records of Processing Activities

When a team at Delhivery processes Personal Data for performance of their activities, they must ensure that details of such activities are captured in the Records of Processing Activities document. The records should be reviewed annually to ensure that updates to the data processing activities are accurately reflected.

D. Manual Data Handling Guidelines

Where possible Personal Data should not be processed manually . For activities where Personal Data needs to be processed manually an approval must be obtained from the Cybersecurity team

E. Privacy Impact Assessment

A Privacy Impact Assessment (PIA) should be performed for all processes and applications relying on Personal Data.. The risk levels of an activity must be determined by the Cybersecurity team.

F. Cookie Management

Individuals visiting Delhivery's websites/applications should be informed about the cookies being used to collect their information. Individuals should be allowed to reject the use of cookies.

G. International Data Transfer Guidelines

Where Personal Data of individuals is transferred from one country to another, it must be ensured that Data Privacy regulations of both countries are complied with, and appropriate data protection agreements are in place

H. Data Subject Rights Management

Delhivery may receive from the Data Subjects requests relating to their Personal Data and its processing. All such requests should be reported to the Cybersecurity team who are responsible for assessing the validity of the request and identifying teams who may be required to respond to the Data Subjects requests.

Where a Data Subject request is from an individual whose Personal Data has been provided to Delhivery by a client, notification should be provided to the client about the request and no communication should be made to the Data Subject until the same has been discussed with the client.

15. Related Standards, Policies and Processes

- Acceptable Usage Policy
- Information Classification Policy
- Password Policy
- Remote Access Policy
- Network Access Control Policy
- Clean Desk policy
- Risk Management Policy
- User access management process
- Change Management Process
- Application Security Testing Policy
- Vendor Engagement
- Technology - Incident Response Process
- Business Continuity, Disaster Recovery Planning & Disaster Management

16. Policy Violation

Failure to observe this policy may expose Delhivery to breaches of relevant laws, the loss of vital information or the impairment of business operations, and cause significant damage to the public image and reputation of Delhivery. The employees not complying with this policy may be subject to disciplinary action, up to and including termination of employment.