INFORMATION SECURITY AND DATA PROTECTION POLICY

1. PURPOSE

The purpose of this policy is to safeguard the confidentiality, integrity, and availability of organizational information and personal data. It establishes measures for protecting information assets against unauthorized access, loss, misuse, disclosure, alteration, or destruction.

2. SCOPE

This policy applies to:

- All employees, contractors, vendors, and third parties handling company information.
- All information systems, applications, devices, and data (electronic or paper-based) owned, leased, or managed by **HMA Industries Pvt. Ltd.**

3. OBJECTIVES

- Ensure compliance with applicable data protection and privacy laws (e.g., GDPR, IT Act 2000, etc.).
- Protect personal, confidential, and sensitive information from breaches.
- Define roles and responsibilities for secure information handling.
- Build awareness among employees regarding data protection practices.
-

4. DEFINITIONS

- **Personal Data:** Any information relating to an identified or identifiable person.
- **Sensitive Personal Data:** Information such as financial details, health data, biometrics, passwords, etc.
- **Information Assets:** Any data, documents, systems, or applications critical to the company's operations.

- **Data Breach:** Unauthorized access, disclosure, alteration, or loss of data.

5. ROLES & RESPONSIBILITIES

- **Management:** Approve and enforce information security controls.
- **IT Department:** Implement technical safeguards, monitor systems, and respond to incidents.
- **Employees:** Handle information responsibly, follow security protocols, and report incidents.
- **Data Protection Officer (DPO):** Oversee compliance with data protection regulations.

6. POLICY STATEMENTS

6.1 Data Classification & Handling

- Classify data as **Confidential, Internal, or Public**.
- Handle personal and sensitive data with highest security controls.
- Share information only on a need-to-know basis.

6.2 Access Control

- Access rights are role-based and must be reviewed regularly.
- Strong passwords and multi-factor authentication must be used.
- Accounts must be deactivated immediately upon employee exit.

6.3 Data Protection & Privacy

- Collect only necessary personal data for legitimate business purposes.
- Obtain consent before collecting or processing personal data.
- Ensure secure storage (encryption, restricted access) and lawful use of data.

6.4 Data Storage & Retention

- Store data in secure servers or approved cloud systems.
- Retain data only for the legally required period or business necessity.
- Destroy or anonymised data when no longer needed.

6.5 Information Security Controls

- Use firewalls, antivirus, intrusion detection systems, and encryption.
- Regularly update and patch systems to prevent vulnerabilities.
- Prohibit unauthorized use of personal devices (BYOD) unless approved.

6.6 Incident Management

- Report all suspected data breaches immediately to IT/DPO.
- Investigate breaches promptly and notify relevant authorities/customers as required by law.
- Maintain incident records and corrective actions.

6.7 Physical Security

- Restrict access to server rooms and sensitive data storage areas.
- Use ID cards, visitor logs, and CCTV monitoring.
- Shred confidential paper records before disposal.

6.8 Third-Party & Vendor Management

- Vendors handling company data must sign confidentiality agreements.
- Ensure compliance with data protection regulations.
- Conduct periodic audits of vendor security practices.

7. TRAINING & AWARENESS

- Conduct annual training on data protection, cyber security, and phishing awareness.
- Provide role-specific training for employees handling sensitive data.
- Share regular updates on threats and prevention measures.

8. COMPLIANCE & DISCIPLINARY ACTION

- Non-compliance with this policy may result in disciplinary action, including termination of employment, contract cancellation, or legal action.
- Regular audits will be conducted to ensure compliance.

9. REVIEW & UPDATE

- This policy will be reviewed annually or as required due to changes in regulations, technology, or business processes.

APPROVED BY:

M. Zubair Rahman

Managing Director

Date: 25-04-2024