Information Security and Data Privacy Policy

Note:

The procedures listed here, are a facilitator to smooth functioning and a means of spreading common processknowledge and understanding across the business units / departments.

Table of Contents:

1.0 Purpose

The purpose of this policy is to state the organization's directive towards data confidentialityand to ensure adequate safeguards to prevent misuse or loss of information. Compliance to this policy shall ensure that our legal, business and regulatory obligations are fulfilled.

2.0 Audience

This policy applies to all ARVIND employees, contractors and retainers, interns, temporary workers, partners/third parties and related ("users"), to perform tasks related to design, engineering, operational maintenance andmanagement on ARVIND's information. It is also applicable to users in all business verticals of ARVIND GROUP, but not limited to, Textiles, Garmenting, Advanced Materials, Brands & Retail, Telecom, Agribusiness, Real Estate, Internet, CSR, Engineering, Water business and Finance.

3.0 Scope

ARVIND recognizes that all key information are vital and strategic and must be protected from unauthorized access, loss, contamination, or destruction. Proper management and protection of information / communication systems is characterized by ensuring the confidentiality, integrity, and availability of the system.

ARVIND recognizes "Information" is an extremely valuable and important asset to them. "Information", in anyform, requires protection against risks that would threaten its confidentiality, integrity and availability. Suitable information security controls shall therefore be selected and implemented. ARVIND, therefore, shall take appropriate steps towards providing reasonable level of security and privacy for information and information processing operations.

Failure to comply with the requirements of this document, any applicable data protection policies and procedures, the acceptable use policy, or any applicable ARVIND information security policies, procedures, orstandards, could result in the removal of privileges of allocated device, and result in an imposition of disciplinary action by ARVIND management.

4.0 Policy

ARVIND shall take adequate precaution for the protection of data.

ARVIND shall ensure that, information related to its employees, is secure and appropriate controls are in place to prevent unauthorized disclosure or modification.

- **Information Classification and Ownership:**

  Information created by users, is the exclusive property of ARVIND. In order to prevent unauthorized disclosure or misuse.

  All information shall be classified according to its sensitivity and confidentiality. The data owner shall appropriately classify the information according to the following guidelines.

  Restricted: Information that is extremely sensitive and intended for use only by named individuals within the organization. Restricted information may not be shared with external parties unless its in compliance with legal requirements or there is a strong business justification.

Confidential: Information that is sensitive within the organization and is intended for use only by specified groups of employees. Such information shall be shared within a specific department and access by personnel of other departments is restricted.

Internal: Non-sensitive information available for usage within ARVIND. Information classified as Internal isnot suitable for release outside the organization.

Public: Non-sensitive information available on public domain that can be accessed by anyone.

When information of various classifications is combined, the resulting collection of information or latest information must be classified at the most restrictive level among the sources.

If any information is not specifically classified it shall be treated as ‘**Internal**” by default.

- **Data Retention**

  Retention period shall be determined based on the contractual, statutory or regulatory requirements. ARVIND shall ensure that data, that is retained, is secured (logically and physically) and its integrity is maintained.

- **Legitimate and Fair Use**

  ARVIND shall only collect, use, or disclose ‘Personal Information’ by lawful and fair means, in accordance with applicable laws, and fully observing the legal rights of individuals. ARVIND shall only obtain or use ‘Personal Information’ in order to fulfill ARVIND’s legitimate business purposes, such as (but not limited to) evaluating applications for membership with ARVIND (including any of its individual programs), maintaining ARVIND membership accounts, maintaining regular communications with ARVIND members, furnishing services to members, complying with applicable legal and regulatory requirements, and protecting ARVIND’s legal rights and interests. ARVIND shall use the minimum amount of ‘Personal Information’ necessary and, whenever possible, should rely instead upon anonymous or aggregated information to accomplish its business objectives. ARVIND prohibits any unauthorized use of ‘Personal Information’ by ARVIND personnel or its agents.

- **Individual Choice**

  ARVIND believes individuals should be able to decide how ARVIND collects and uses their ‘Personal Information’ to the greatest extent possible. Whenever possible or required by law, ARVIND shall obtain the consent of an individual before collecting or processing their ‘Personal Information’ and, where an individual withholds or later withdraws their consent, respect their indicated wishes. ARVIND will strive in particular to obtain the consent of individuals where ARVIND collects and processes ‘Sensitive Personal Information’, while recognizing it may in some instances be necessary to process such Information to protect adequately ARVIND’s legal rights and interests. When seeking an individual’s consent, ARVIND shall provide the individual with sufficient information to allow the individual to make an informed decision, allow the individual to later withdraw their consent, and refrain from penalizing the individual for withholding their consent. For the avoidance of doubt.

a) ARVIND shall ensure that any benchmarking surveys, questionnaires, and related research tools capturing ‘Personal Information’ contain a mechanism for securing the consent of the respondent, and that the relevant individual has affirmatively indicated their consent.

b) ARVIND shall allow individuals to decide whether their ‘Personal Information’ will be used for other purposes besides those appearing in any notices furnished to the individual, other than where necessary to protect ARVIND’s legal rights and interests.

c) ARVIND shall respect an individual’s decision not to receive marketing and promotional communications from ARVIND.

- **Information Integrity**

  ARVIND shall only use ‘Personal Information’ in accordance with any notices furnished to or consents obtained from individuals, and should not later process ‘Personal Information’ for any additional, incompatible purposes unless it has re-notified the individual or where required or expressly permitted by law. ARVIND shall only collect ‘Personal Information’ that is relevant in light of the business purposes the ‘Personal Information’ is meant to serve and employ reasonable means to keep the ‘Personal Information’ accurate, complete, up-to-date and reliable. ARVIND materials and forms used to collect ‘Personal Information’ should be prepared in such a manner that only pertinent ‘Personal Information’ is captured.

- **Information Security**

  ARVIND shall implement appropriate administrative, technical, and organizational measures to safeguard the ‘Personal Information’ under its control or in its possession against loss, theft, misuse, unauthorized access, modification, disclosure, or destruction. ARVIND shall ensure that any ‘Sensitive Personal Information’ it holds is subject to safeguards reflecting the correspondingly greater harm that would arise from its unauthorized use or disclosure.

- **Sharing information**

  a) Internal

  Within the organization, information shall be made available only, on need basis and an appropriate approval shall be obtained from the data owner, as deemed necessary, while information is to be shared with other departments / functional units.

  b) External (Third Parties/Partners)

  ARVIND may share the confidential information with Third Parties/Partners for evaluating a possible business arrangement.

  “Confidential Information” means any and all information that is disclosed by Discloser to the Recipient relating to and in connection with the Business Purpose.

  Confidential Information and any and all intellectual property rights relating to Confidential Information is the sole and exclusive property of Discloser ARVIND.

  A Non-Disclosure Agreement shall be signed with the third parties before information is shared with them. Sharing of business information with external parties, requires a valid justification and approval from BU Heads/CEOs. In case of any breach actions against the third parties/partners shall be taken as per Non-Disclosure Agreement.

Care shall be taken to ensure that, information shared, is not intercepted, copied and modified. In order to protect the interest of the organization, approved disclaimer shall be included in all the e-mails that are sent from the company email account.

- **Reporting Cyber security incidents**

It needs to be ensured that any cyber security incidents needs be reported immediately to the concerned Cybersecurity Grievance Officers. Below are some of such security incidents that needs to be reported:

a) Targeted scanning/ probing of critical networks/ systems
b) Compromise of critical systems/information
c) Unauthorized access of IT system/ data
d) Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites etc.
e) Malicious code attack such as spreading of virus/worm/Trojan/Botnets/spyware
f) Attack on servers such as Database, mails and DNS and network devices such as routers
g) Identify theft, spoofing and phishing attacks
h) Denial of service (DoS) and distributed Denial of Service (DDoS) attack
i) Attacks on Critical infrastructure, SCADA (Supervisory control and data acquisition) system and wireless network
j) Attacks on applications such as E-Governance, E-Commerce etc.

Above reporting shall be intimated to Grievance Officers via **email: cybercell@arvind.in.**

- **Cybersecurity Incident Response Plan**

a) Preparation

- Determine the exact location, sensitivity and relative value of all information of organization that needs to be protected.
- Identify cybersecurity regulatory requirements of the organization across all functions and develop guidance on how to interact with law enforcement and other governmental authorities in the event of an incident.
- Develop and maintain a list of preferred technology vendors for forensics, hardware replacement, and related services that might be needed before, during or after an incident.
- Establish procedures for IT teams to receive clear, actionable alerts of all detected malware.
- Employee’s need to report suspicious emails and activities that might compromise network security.
- Establish a comprehensive and integrated communications plan to inform both internal and external audiences on incidents in a rapid, accurate and consistent fashion.

b) Detection & Analysis

- Develop a proactive detection strategy based on tools that can automatically scan your physical and virtual hosts, systems, and servers for any vulnerable applications, identities, or accounts.
- Conduct compromise assessments to verify whether a network has been breached and quickly identify the presence of known or zero day malware and persistent threats active or dormant — that have evaded your existing cybersecurity defense.

c) **Response & Remediation**

- Inform cybersecurity grievance team about the incident.
- Inform cybersecurity cell about the incident.
- Inform cybersecurity partner about the incident.
- Isolate Data Center/Sever Zones from the Network.
- Identify and Isolate infected locations from the network.
- Determine if any sensitive data has been stolen or corrupted.
- Eradicate infected files and, if necessary format the systems/servers and restore last good known backup.
- Restore the Network Connectivity between infected locations and Data Center.
- Keep a comprehensive log of the incident and response, including the time, data, location and extent of damage from the attack.
- Preserve all the artifacts and details of the breach for further analysis of origin, impact, and intentions
- Update any firewalls and network security to capture evidence that can be used later for forensics.
- Engage the legal team and examine compliance and risks to see if the incident impacts any regulations.

d) **Recovery**

- Eradicate the security risk to ensure the attacker cannot regain access. This includes patching systems, closing network access and resetting passwords of compromised accounts.
- During the eradication step, create a root cause identification to help determine the attack path used so that security controls can be improved to prevent similar attacks in the future.
- Perform an enterprise wide vulnerability analysis to determine whether any other vulnerabilities may exist.
- Restore the systems to pre-incident state. Check for data loss and verify that systems integrity, availability and confidentiality has been regained and that the business is back to normal operations.
- Gather logs, memory dumps, audits, network traffic statistics and disk images.
- Complete an incident response report and include all areas of the business that were affected by the incident.

- **Dishonest and Fraudulent Intentions are prohibited**

  Below mentioned activities with a dishonest and fraudulent intentions are prohibited and no one should indulge in any of these.

  a) Unauthorized computer system or computer network or computer resource

  b) Downloading, copying or extracting any unauthorized data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.

  c) Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

  d) Damaging or causing to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network.

e) Disrupting or causing disruption of any computer, computer system or computer network;

f) Charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

- **Compliance:**

  ARVIND would maintain an active program to ensure compliance with and maintain awareness about the Policy. All ARVIND personnel are required to adhere to this Policy and any associated or supporting policies. Failure to do so may be grounds for disciplinary action.

5.0 Enforcement

All information that was generated before the policy came into effect shall also be classified appropriately.

Actions that are required to be followed by the end user, with respect to information sensitivity, shall be communicated through the Acceptable Usage Policy. Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters, etc.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing ARVIND's information, shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreements entered by them with ARVIND.

Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

7.0 Approvals

For exceptions, other than specified in this document, users can approach, below list of approvers, with detailed justification or write an email too.

	Name	Designation
Prepared By	Advait Sharma	Sr. Manager Network and Security - IT
Reviewed By	Anil Patel	Dy. General Manager - IT
Approved By	Nitin Parmar	CIO - IT

8.0 Revision History

Version	Author	Date	Revisions
0.5	Kinshuk Joshi	01 Apr 2016	Initial Document
1.0	Kinshuk Joshi	01 Aug 2016	Revised
1.0	Nilesh Panchal	01 Nov 2018	Revised
2.0	Advait Sharma	19th Jul 2021	Revised
3.0	Advait Sharma	14th Jun 2024	Review and Revised