VA TECH WABAG LIMITED

Policy on Cyber Security & Data Privacy

Prepared by	IT Department
Recommended by	CIO
Approved by	Board of Directors
Date of Approval	March 17, 2023

Revision History

Version	Date of Revision	Author	Description of Changes
1.0	-	IT Department	Initial Version

Contents

1. Introduction & Purpose of the Policy

This policy refers to the Company's commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. The Company must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting customers, incurring penalties for non-compliance and suffering damage to its reputation. At the same time, the Company must ensure users can access data as required for them to work effectively. With this policy, the Company ensures that it gathers, stores and handles data fairly, transparently and with respect towards individual rights.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

2. Coverage & Scope of the Policy

This policy refers to all parties or stakeholders (employees, job candidates, customers, suppliers, vendors etc) who provide any amount of information to the Company. Employees of the Company must follow this policy. Contractors, consultants, partners and any other external entity who are dealing with the Company, have to adhere this Policy. Generally, this policy refers to anyone that the Company collaborates with or acts on its behalf and may need occasional access to data.

3. Data Privacy

As part of the Company's operations, it is needed to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, permanent account number (PAN), Aadhaar, financial data etc. The Company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible. Once the data is available to the Company, the following rules shall apply on it:

- The data should be accurate and kept up to date;
- The data should be collected fairly and only for lawful purposes;
- The data should be processed within the legal boundaries of the Company;
- The data should be protected against any unauthorized and illegal access by external or internal parties.

The data so obtained should not be:

- Communicated Informally;
- Transferred to organizations, states or countries that do not have adequate data protection policies;
- Distributed to any party other than the ones agreed upon by the data's owner except legal authorities.

The privacy and protection of data has to be ensured by the following practices in the Company:

1. Restrict and monitor access to sensitive data;
2. Develop data collection procedures;
3. Regular trainings on the data privacy and security measures to be given to all employees and directors;
4. To ensure establishing a clear procedure for reporting privacy breaches and data misuse;
5. Include contract clauses or communicate statements on how to handle data;
6. Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.).

The above practices are not an exhaustive list and judgement of an individual based upon the situations would also apply for the protection of proprietary data.

4. Cyber Security

The following procedures are to be followed by all employees for the protection of data and IT systems of the Company from unauthorized accesses and malwares:

1. Each employee shall have a unique user id for access to the data and accountability;
2. All employees are expected to read this policy thoroughly;
3. Access shall be granted based upon the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks;
4. Access to the IT resources and services are to be provided through provision of unique user accounts and complex passwords (managed by IT Department) based on HR records;
5. Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains;
6. All employees and contractors shall be given network access in accordance with business access control procedures;
7. Network routing controls shall be implemented to support the access control policy;
8. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access;
9. All users (including the employees who access to sensitive data from home through internet / VPN while working from home) must keep their workplace clear of any sensitive or confidential information and ensure confidentiality & integrity of the sensitive & confidential data;
10. All users must keep their passwords confidential and not share them;
11. All Company's staffs and contractors shall access sensitive data and systems only if there is a business need to do so with the approval from higher management and / or by way of executing a Non-Disclosure Agreement or Confidentiality Agreement;

12. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only;
13. The responsibility to implement access restrictions lies with the IT Security department.

5. Reporting Requirements

The reporting of incidents related to cyber security and data privacy are to be reported as per the following:

1. Periodic reports detailing all incidents shall be produced by the IT Security team of the IT department and sent to the Chief Information Officer (CIO) of the Company;
2. High-priority incidents discovered by the IT Security team shall be immediately escalated and informed to CIO;
3. Executive / Employee responsible for IT Security in IT department shall also prepare a monthly report showing the number of IT security incidents and the percentage that were resolved and submit the same to CIO;
4. Cluster IT department shall report incidents of significance like security breach, loss of confidential information etc., to the CIO.

6. Disciplinary Actions

The Company expects all the employees to follow the policy at all times and those who don't and cause security breaches are subject to face following disciplinary action:

1. *First-time, unintentional, small-scale security breach:* The employee will be issued a verbal warning and further trainings on cyber security and data privacy will be conducted for him/her;
2. Intentional, repeated or large scale breaches (which cause severe financial or other damage): Each incident will be examined on a case to case basis to decide upon the disciplinary proceeding to be done;
3. The employees may note that their user credentials are very sensitive for them from organisation point of view and they shall maintain confidentiality on this and if any breach / malpractice / misuse happens due to usage of such credentials by any other employees with or without knowledge of the actual user, then the actual user shall only be held responsible.

This policy shall be reviewed by CIO as per the requirement or whenever policy changes are announced by MeITY (Ministry of Electronics and Information Technology, Government of India) and / or Statutory authorities.

7. Amendment

Any amendment or modification in any applicable laws relating to the *"Cyber Security & Data* Privacy", shall automatically be applicable to the Company.