Data Protection Policy

1) Purpose of the Policy: At Squatrix Solution, we often handle sensitive data from various stakeholders, including clients, employees, partners, and vendors. This data may include personal, confidential, or proprietary information. As part of our business processes, we must ensure that this information is protected and handled in accordance with legal and ethical standards. This policy outlines our approach to safeguarding data to prevent misuse and ensure compliance with data protection laws.

2) Guiding Principles: This policy is governed by the following principles, which should guide all employees in their handling of data:

a) **Respect and Confidentiality**: All data collected, processed, and stored must be treated with the utmost respect. This means understanding the sensitivity of personal and business information and ensuring that confidentiality is maintained at all times.

b) **Compliance with Law**: Squatrix Solution complies with all applicable data protection regulations and standards, ensuring the lawful and transparent use of information.

c) **Integrity in Action**: Every action concerning data protection will align with the company's values of integrity and honesty. We ensure that data is used solely for the purpose for which it was collected and is never misused.

3) Scope of the Policy This policy applies to all Squatrix Solution employees, contractors, vendors, and stakeholders who have access to personal and business-related data.

a) Personal and Confidential Data

- Personal data refers to information related to an identifiable person, such as name, contact details, financial information, and job-related details.
- Confidential data includes business-sensitive information such as proprietary technologies, pricing structures, and business strategies.

b) External Stakeholders

- Government bodies, law enforcement, and legal entities may request information. This policy outlines the process for managing such requests, ensuring we comply with statutory obligations while protecting individual privacy.

c) Application of the Policy

- This policy applies to all Squatrix Solution employees who handle data. It provides clear guidance on how to manage, edit, store, retrieve, disclose, and destroy information safely.

Data Protection Policy

d) Sensitive Information

- Squatrix Solution does not collect sensitive personal information (e.g., religious beliefs, political opinions, or personal preferences) unless it is legally required for business purposes.

4) Data Management Procedures

a) Handling Data

- All data must be handled fairly and lawfully, in compliance with local data protection regulations.
- Employees must ensure accuracy, timeliness, and sensitivity when processing data. For example, when assessing a candidate for recruitment, all qualifications and other details must be accurately matched.

b) Data Maintenance

- **Confidentiality, Integrity, and Availability**: Data access is restricted to authorized personnel only, ensuring accuracy and relevance to the company's business processes.
- **Relevance**: Squatrix Solution will ensure personal data is kept up to date and that outdated information is archived or deleted as required by law.
- **Security**: Data access is limited to authorized employees based on their role, with appropriate IT safeguards in place (firewalls, passwords, encryption).

c) Prevention of Misuse

- Visitors' access to workspaces is controlled and monitored.
- Hard copies of sensitive data are stored securely and are archived or destroyed when no longer needed.
- All reusable storage media must be properly erased once the data is transferred to the secure company network.

d) Third-party Involvement

- Contracts with third-party vendors include strict clauses to ensure that they handle data securely and in accordance with legal requirements.

e) Training and Awareness

- Regular training sessions will be conducted for all employees on the proper handling, storage, and processing of data.
- Specific training will be provided to key roles that interact with client or employee data.

Data Protection Policy

f) Responding to External Queries

- All queries from external parties must be vetted and handled by authorized personnel. For example, legal requests (e.g., from the police or courts) will be handled according to statutory guidelines, while unauthorized queries, such as those from marketing agencies, will be refused.

5) Non-Adherence and Reporting Failure to comply with this policy must be reported to a line manager, Head of HR, or Legal. Squatrix Solution will investigate non-compliance, take corrective actions, and inform the necessary personnel of the resolution and any changes made to improve data protection systems.

6) Feedback and Grievance Employees can submit any feedback, suggestions, or grievances related to the Data Protection Policy to the **Director** via email.