Non-Disclosure Agreement

1. Policy Objective: A Software Non-Disclosure Agreement (NDA), also referred to as a Confidentiality Agreement, is a digital legal acknowledgment by the Employee. As per company policy, an employee electronic acceptance is required for all employment categories including full-time, part-time, contract, freelancer, remote/work at home, internship trainee, or any other engagement with the company.

The NDA outlines the terms and conditions under which confidential information related to software will not be shared by employees with anyone within or outside the company. The obligations of the employee are to protect software information, including code documentation, Software Architecture Design, Source Code, and more…

2. Policy Scope: The NDA policy applies to all current and former company employees.

3. Confidential Information: For the purposes of this NDA Policy, "Confidential Information" shall mean any non-public information, data, software code & architect documentation, company's online resources & source code, or any materials related to the software and any related intellectual property owned or controlled by the company.

4. Obligations: The employee agrees to hold the Confidential Information of the company & its customers in strict confidence and to take all reasonable precautions to prevent unauthorized disclosure or use of the Confidential Information. The Employee shall not reproduce, disclose, or distribute the Confidential Information to any 3rd party without the prior written consent of the company.

5. Duration: The obligations of confidentiality shall strictly survive for the total period of employment in the company until the next year from the date of resignation, including acceptance of the resignation letter (Company/employer side) and 30 days' notice period (employee side).

The employee must not disclose the Confidential Information during or after their employment with the company. Employees are not permitted a 'one day notice period' for resigning from their job due to confidential data, IT Security clearance, and the handover activities of ongoing IT projects.

6. Return or Destruction of Information: Upon the Company's written request or the termination of discussions between the parties, the Employee shall promptly return or, at the Company's option, destroy all copies of the Confidential Information in his/her possession.

7. No License or Ownership: Nothing in this NDA Policy shall be construed as granting any license or ownership rights to the Employee in the Confidential Information, whether expressly, by implication, estoppel, or otherwise.

8. Governing Law: This NDA Policy shall be governed by and construed in accordance with the laws of 'The Prevention of Electronic Crimes ACT, 2016' (or recent ACT), with all applicable clauses of CHAPTER II OFFENCES AND PUNISHMENTS including;

- Unauthorized access to information system or data
- Unauthorized copying or transmission of data
- Interference with information system or data
- Unauthorized access to critical infrastructure information system or data
- Unauthorized copying or transmission of critical infrastructure data
- Interference with critical infrastructure information system or data
- Glorification of an offence
- Cyber terrorism
- Hate speech
- Recruitment, funding and planning of terrorism
- Electronic Forgery
- Electronic Fraud
- Making, obtaining, or supplying device for use in offence
- Unauthorized use of identity information
- Unauthorized issuance of SIM cards etc.
- Tampering, etc. of communication equipment
- Unauthorized interception
- Offences against dignity of a natural person
- Offences against modesty of a natural person and minor
- Child pornography
- Online grooming, solicitation and cyber enticement
- Commercial sexual exploitation of children
- Use of information system for kidnapping, abduction or trafficking or minor
- Malicious code
- Cyber stalking
- Cyberbullying
- Spamming
- Spoofing
- Legal recognition of offences committed in relation to information system
- Pakistan Penal Code, 1860 (Act XLV of 1860) to apply

Note: additional clauses of the most up-to-date 'The Prevention of Electronic Crime ACT' may apply as Governing Law of this Policy. Copy of recent 'The Prevention of Electronic Crime ACT' available in the website section resources/Significant Policies as ready reference for all job applicants and concerns.

9. Compliance: The company abides by 'The Prevention of Electronic Crimes ACT 2016'. Failure to comply with this NDA Policy may lead to legal proceedings against the employee or other parties involved. Any individual convicted of a crime under the relevant clauses of 'chapter ii offences and punishments' of the ACT may receive a minimum prison sentence of up to seven years, a fine of up to ten million Pakistani rupees, or both.

The event can be reported to FIA Cyber Crime Wing under the law 'The Prevention of Electronic Crimes ACT 2016', which may result in legal actions against the employee.

Moreover, the employee will be responsible for compensating the company for any damages caused by their unprofessional conduct and covering the legal expenses.

10. Policy Revision & Approval: The Board of Directors of the Company in its meeting held on January 11, 2022, considered and approved this Policy (Original Issue). Any revision to this policy shall be subject to a review and approval by the Board as and when is required.

Please visit *https://vietech.pro/resources/significantpolicies* to address any concerns and review the latest policy updates.

Version	Date	Nature of Changes	Approved By
1	11.01.2022	Original issue.	BOD Meta GRC (Private) Limited
2	28.02.2023	No change in the policy. The policy revised due to change in name of the company from Meta GRC (Pvt.) Limited to Vie Tech (Pvt.) Limited [SECP Certificate#B048304, APL#7460, Dated 24.02.2023]	BOD Vie Tech (Private) Limited formerly known as Meta GRC (Pvt.) Ltd.