idexcel

NDA for Remote Working

This special Non-Disclosure Agreement ("Agreement") is effective as of **01-oct-2024_**

BY AND BETWEEN:

1. **Idexcel Technologies Private Limited,** having its registered office at Suite – 301, H.No. 8-3-945/E, Yellareddy Guda, Ameerpet, Hyderabad 500073, India, hereinafter referred to as “Company”, (which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors and assigns); and

2. Name: **Mohit Mishra**

Address: __ **Mishra auto near mahavir school,swarajpuri road,gaya(BIR), 823001**
Hereinafter referred to as the “Employee” or “you” or “your” (as the context may require), (which expression shall, unless it be repugnant to the context or the meaning thereof be deemed to mean and include his heirs, legal representatives, executors, and administrators).

Remote Work Policy

The organization has established guidelines and procedures when employees are working remotely or work-from-home. The policy aims to ensure the confidentiality, integrity, and availability of organizational data, maintain productivity, and support a safe and flexible work environment.

1. Authorization and Equipment:

- Work from home is allowed for authorized employees based on business needs.
- Employees permitted to engage in remote computing must obtain appropriate approval and use laptops provided by the organization.

2. Device Use and Security:

- Devices must be used only for official work and not for personal activities.
- Mobile devices must be protected with a strong password or biometric authentication, and passwords should not be shared.
- All mobile devices must have up-to-date security software and operating system patches installed.
- Lost or stolen devices must be reported to HR & IS teams immediately.
- Sensitive and confidential information should not be stored on mobile devices unless authorized and necessary for business purposes.

3. Network Access:

- All remote connections to the organization's network must be established through a secure Virtual Private Network (VPN). Employees must connect only to Idexcel VPN-approved endpoints.
- Employees should avoid using public Wi-Fi networks when accessing sensitive information or conducting business-related activities.

4. Data Storage and Access:

- OneDrive is to be used for storing and sharing business-related files and documents. Personal or non-work-related files should not be stored on mobile devices or OneDrive unless explicitlyauthorized.
- Mohit Mishra

- Access controls, including permissions and sharing settings in OneDrive, should be regularly reviewed and updated.
-

5. Application and Configuration Management:

- Unauthorized installation of applications or modification of device settings is strictly prohibited.
- Employees must not install unauthorized applications or download files from untrusted sources.
- Ensure you do not advertently or inadvertently change the configuration setup and applications installed on the device by the IS team.

6. Device Usage and Safety:

- Mobile devices should not be used while driving to ensure safety.
- Employees should use mobile devices responsibly and professionally, adhering to company policies and guidelines.
- Ensure the safety and security of mobile devices (laptops, tablets, mobiles) used for remote working.
- Protect against unauthorized remote access to organizational internal systems or misuse of facilities.

7. Remote Work Practices:

- Ensure that family members and friends do not get unauthorized access to organizational information or resources.
- Employees should maintain regular communication with their managers, team members, and other relevant stakeholders using approved communication channels (e.g., Email, Teams).
- Employees are expected to be responsive during established work hours and promptly address work-related requests and inquiries.
- Collaboration tools and project management systems may be utilized to facilitate teamwork and ensure the timely completion of tasks.
- Employees working from home are responsible for creating a suitable workspace that promotes productivity and ensures a safe and comfortable environment.

8. Compliance and Performance:

- Remote employees must adhere to all organizational policies related to data security, privacy, and confidentiality.
- Employees should use secure and approved methods to access and transmit organizational data, such as VPNs or encrypted connections.
- Use of employees' personal devices is strictly prohibited.
- Performance expectations for remote employees should align with those of in-office employees and be clearly communicated.
- Established measurable goals and objectives for WFH employees are regularly reviewed for performance.
- Employees should take appropriate measures to secure and protect organizational assets.
- Employees must comply with all applicable laws, regulations, and organizational policies, including data protection, confidentiality, and ethical conduct.
- Mohit Grish KA

- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

Employee Mohit Mishra

Sign: ______

Name: **MOHIT MISHRA**

____

for **Idexcel Technologies Private Ltd.**

Sign: ______________________________

Department: **Human Resources**