Remote Work and Access Policy

📄 Section 1: Policy Purpose and Scope

1.1 Purpose

The purpose of this policy is to establish clear guidelines, standards, and procedures for employees who are approved to work remotely, ensuring consistency, security, and productivity while maintaining a positive work-life balance.

1.2 Scope and Applicability

This policy applies to **all full-time and part-time employees** of **[Company Name]** who have received formal, written authorization to perform work outside of a designated corporate office location. It covers all company equipment, data, and access methods used for remote work.

💻 Section 2: Eligibility and Agreement

2.1 Eligibility Criteria

Remote work arrangements are a privilege, not a right, and are subject to departmental needs and managerial approval. Eligibility is determined by the following factors:

- The nature of the job must allow for remote completion of core duties.
- The employee must demonstrate high levels of productivity, accountability, and communication skills.
- The employee must maintain a satisfactory performance rating for the past 12 months.

2.2 Remote Work Agreement

All approved remote work employees **must** sign a formal **Remote Work Agreement** outlining their specific schedule, designated workspace, communication expectations, and adherence to security protocols. This agreement must be reviewed annually.

🔒 Section 3: Technology and Data Security

3.1 Company Equipment

[Company Name] will provide all necessary equipment (laptop, monitors, peripherals) for the employee to perform their duties. **Employees must not** use personal devices for accessing company data unless explicitly approved via the "Bring Your Own Device (BYOD) Policy."

3.2 Secure Access (VPN)

All access to company internal networks, servers, and sensitive resources **must** be conducted through the Company-provided **Virtual Private Network (VPN)** connection. The VPN must be active at all times while conducting company business.

3.3 Data Confidentiality

Employees are strictly responsible for maintaining the confidentiality and security of company data.

- Sensitive physical documents **must not** be stored in the remote workspace.
- Employee laptops **must** be password-protected, encrypted, and kept physically secure at all times.

📞 Section 4: Communication and Performance

4.1 Availability and Response Time

Remote employees **must** be available and responsive during their agreed-upon core working hours.

- **Response Time:** Employees shall aim to respond to urgent communication (e.g., instant messages or calls) within **15 minutes** and emails within **2 hours** during core hours.
- **Status Updates:** Employees must keep their availability status updated on all company communication platforms (e.g., Slack, Teams).

4.2 Performance Monitoring

Performance of remote employees will be measured by **deliverables and objective results** as outlined in their job description and annual goals, rather than hours spent or physical presence.

📅 Section 5: Policy Violations and Review

5.1 Consequences of Non-Compliance

Failure to comply with any section of this policy, particularly those concerning data security (Section 3), **will result in immediate disciplinary action**, up to and including the permanent revocation of remote work privileges and termination of employment.

5.2 Policy Review

This policy is owned by the **HR Department** and will be reviewed and updated annually, or as necessitated by changes in technology or local regulations.