To: All Employees

From: [Management/IT Department]

Date: [Insert Date]

Subject: Remote Connectivity and Internet Standard Policy

Dear Team,

As we continue to support flexible work arrangements, this letter outlines the mandatory standards for remote connectivity and internet usage to ensure security, productivity, and data integrity.

1. Internet Connection Requirements

Employees are responsible for maintaining a stable and high-speed internet connection. A minimum download speed of [Insert Speed, e.g., 25 Mbps] and upload speed of [Insert Speed, e.g., 5 Mbps] is required for video conferencing and accessing company applications.

2. Secure Connection (VPN)

All remote access to the company internal network, servers, and sensitive data must be conducted via the approved Company Virtual Private Network (VPN). Use of public, unsecured Wi-Fi (e.g., coffee shops or airports) without a VPN is strictly prohibited.

3. Router and Hardware Security

Employees must ensure their home Wi-Fi networks are secured with a strong password (WPA2 or WPA3 encryption). Default administrator passwords on home routers should be changed immediately.

4. Authorized Equipment

Remote work should be performed only on company-issued devices. Connecting personal devices to the company network via remote tools is prohibited unless specifically authorized by the IT Department.

5. Compliance and Monitoring

Usage of the company network remains subject to the standard Acceptable Use Policy. The company reserves the right to monitor connectivity logs to ensure compliance with security protocols.

Failure to adhere to these standards may result in the revocation of remote work privileges or disciplinary action.

Please sign below to acknowledge that you have read and understood this policy.

_____
Employee Signature

_____
Date