HR Remote Work Policy

1. Purpose

This Remote Work Policy outlines the guidelines, procedures, and expectations for employees who are approved to work remotely. The purpose of this policy is to ensure a consistent and effective approach to remote work, maintain high levels of productivity, protect company assets, and support a positive work-life balance for eligible employees. This policy applies to all employees who have been approved for a remote work arrangement. Remote work is a flexible work arrangement and is not an entitlement; it may be revoked or modified at any time at the company's discretion.

2. Eligibility

Remote work eligibility is based on a number of factors, including the employee's role, performance, and the operational needs of the team and company.

2.1 Criteria for Eligibility

To be considered for a remote work arrangement, an employee must meet the following criteria:

- **Job Suitability:** The employee's job responsibilities must be conducive to remote work, as determined by their manager and HR. Not all roles are suitable for remote work.
- **Performance:** The employee must be in good standing, meeting or exceeding performance expectations in their most recent performance review. Employees on a Performance Improvement Plan (PIP) or with recent disciplinary actions are typically ineligible.
- **Duration of Employment:** Generally, employees must have successfully completed their introductory period (typically Date) before being considered for a remote arrangement.
- **Work Environment:** The employee must maintain a dedicated, safe, and secure home workspace conducive to productive work, free from excessive distractions.

2.2 Application and Approval

Employees must submit a formal Remote Work Agreement Request form (File) to their manager for review and approval. The request will be reviewed by the manager and then

by HR (Person) for final approval. Approvals are granted for a specified period and require periodic renewal.

2.3 Policy Review

The company reserves the right to review and modify an employee's remote work status based on performance, team needs, or changes in business requirements. An approved remote work arrangement can be terminated at any time with appropriate notice.

3. Security

Maintaining the security and confidentiality of company information is paramount, regardless of the employee's location. Remote employees must adhere to all existing company security policies.

3.1 Data Protection

Remote employees are responsible for protecting company data and property from unauthorized access, damage, or theft.

- **Confidentiality:** All confidential, proprietary, or sensitive company information (electronic and physical) must be handled with the same level of care as if working in the office.
- **Physical Security:** Company equipment (laptops, phones, etc.) must be secured and not left unattended in public spaces. Physical documents containing company information must be stored securely and shredded when no longer needed.
- **Screen Lock:** Employees must lock their computer screen when stepping away from their desk.

3.2 Equipment

The company will provide necessary equipment (e.g., laptop, monitor) for remote work. Employees are responsible for the safe custody and maintenance of company-owned equipment.

- **Personal Devices:** The use of personal computers or mobile devices for company work is strictly prohibited unless explicitly approved under a separate Bring Your Own Device (BYOD) policy.
- **Reporting Incidents:** Any loss, theft, or damage to company equipment, or any suspected security breach, must be reported immediately to the IT Department (Person) and the employee's manager.

4. VPN (Virtual Private Network)

Access to the company's internal network and sensitive resources is strictly controlled and requires the use of a Virtual Private Network (VPN).

4.1 Mandatory Use

All remote employees must use the company-provided VPN to connect to the corporate network for any work-related activities that require accessing internal systems, shared drives, or confidential data.

4.2 VPN Protocol and Security

- **Installation:** The VPN software must be installed on company-issued devices only.
- **No Split Tunneling:** To ensure all traffic is routed securely through the corporate firewall for inspection, split tunneling is strictly forbidden.
- **Password Protection:** Employees must not share their VPN login credentials. Passwords must comply with the company's password policy and be changed regularly.
- **Troubleshooting:** Employees should contact the IT help desk (Person) for any issues related to VPN access or connectivity.

5. Expenses

The company will provide clear guidelines regarding reimbursement for expenses incurred while working remotely.

5.1 Company-Provided Equipment

The company will cover the cost of all required, company-approved equipment necessary for the role.

5.2 Internet and Utilities

The company will not reimburse employees for home internet service, utilities (electricity, heat, water), or rent, as these are generally considered ordinary household expenses.

5.3 Communication and Supplies

The company will reimburse remote employees for reasonable and necessary work-related expenses. Reimbursable expenses typically include the cost of a dedicated work phone line (if required and approved), office supplies such as printer ink, paper, and

pens, approved ergonomic accessories, and required travel to the main office or offsite meeting locations. Expenses that are generally not reimbursable include personal cell phone usage/plan costs, the purchase of home furniture (such as a desk or chair), and daily commute costs.
All requests for reimbursement must be submitted using the standard expense report form (File) and must be accompanied by original receipts, in accordance with the company's expense policy.

6. Monitoring

To ensure compliance with company policies, maintain security, and assess productivity, the company reserves the right to monitor remote employee activities and access company equipment.

6.1 Equipment Monitoring

Company-issued equipment is subject to monitoring, inspection, and review at any time, with or without notice, in accordance with applicable laws. Monitoring may include, but is not limited to:

- **System Activity:** Monitoring of network traffic, websites visited, and application usage.
- **Security Audits:** Regular security checks and audits of company-issued devices.
- **Data Access:** Logging of access to company files and systems.

6.2 Performance Monitoring

Managers will monitor remote employee performance through standard output measures, including project deliverables, meeting deadlines, quality of work, and communication responsiveness, consistent with expectations for in-office employees.

6.3 Workplace Visits

The company reserves the right to conduct an in-person safety and security inspection of the remote workspace, with reasonable notice, to ensure compliance with this policy, particularly concerning equipment security and safety standards.

Policy Effective Date: Dec 3, 2025

Last Reviewed: Jan 15, 2026