1. Remote Work / Telework Policy

Version: 2025-01
Effective Date: [Insert Effective Date]
Company: NMT

---

2. Purpose

The purpose of this Remote Work / Telework Policy is to provide guidelines for employees who work remotely or telecommute. This policy ensures that remote work aligns with the company's operational goals while maintaining productivity, security, and employee well-being.

---

3. Eligibility and Approval

3.1 Eligible Roles

• **Full-Time Employees:** Employees in roles that do not require a physical presence (e.g., IT, marketing, customer service) may be eligible for remote work.
• **Part-Time Employees:** Eligibility may depend on role and manager discretion.
• **Contractors:** Eligibility is determined case-by-case and requires prior approval.

3.2 Exceptions

• **Roles Requiring On-Site Presence:** Positions involving facilities management, maintenance, or roles requiring direct customer interaction are not eligible.
• **New Employees:** Employees in probation may not be eligible until completion of the probationary period.

3.3 Approval Process

1. Submit a Remote Work Request Form to the direct manager.
2. The manager will assess the request based on business needs and employee performance.
3. Final approval will be communicated within five business days.

---

4. Work Location and Hours

4.1 Work Location

• Employees must work from a secure location that supports productivity and confidentiality.
• Public locations such as cafés or parks should be avoided due to risk of exposing sensitive information.

4.2 Work Hours

• **Core Hours:** Employees must be available from 10 AM to 3 PM in their local time zone.
• **Flexibility:** Outside core hours, employees may adjust their schedules if communicated with the team.
• **Overtime:** Requires prior managerial approval.
• **Breaks:** Employees should take regular breaks, including at least one 30-minute break for every 4 hours worked.

4.3 Availability Rules

• Employees must remain reachable via company communication tools during core hours.
• Out-of-office notifications must be used for extended absences.

---

5. Equipment and Allowances

5.1 Company Equipment

• The company provides necessary equipment such as laptops and peripherals.
• Employees are responsible for proper care and maintenance of equipment.

5.2 Allowances

• **Internet Stipend:** Monthly stipend based on local market rates.
• **Energy Stipend:** May be provided with managerial approval.

5.3 Ownership and Return

• All company-provided equipment remains company property.
• Equipment must be returned upon termination or upon request.

---

6. Security and Confidentiality

6.1 Data Security

• Use of a Virtual Private Network (VPN) is mandatory.
• Multi-Factor Authentication (MFA) must be used when accessing sensitive information.

6.2 Data Handling

• Employees must follow IT Security Policy guidelines.
• Confidential information must not be stored on personal devices.

6.3 BYOD Rules

• Personal devices used for work must comply with security protocols.
• Devices must be registered with the IT department.

6.4 Restricted Locations

• Employees should avoid working in locations where unauthorized individuals may view or access company information.

---

7. Performance and Communication

7.1 Performance Metrics

• Employees will be evaluated using KPIs and OKRs set by their managers.

7.2 Communication Rituals

• **Daily Check-ins:** Short daily team meetings.
• **Weekly Updates:** A weekly summary of accomplishments and plans.

7.3 Meeting Etiquette

• Be punctual and prepared for meetings.
• Use video conferencing where possible.

7.4 Response-Time SLAs

• Respond to emails and messages within 24 hours on workdays.

---

8. Health & Safety

8.1 Ergonomics

• Employees are encouraged to create ergonomic workspaces.
• Resources on best practices are available via the intranet.

8.2 Incident Reporting

• Any work-related injury must be reported immediately to the manager.

8.3 H&S Self-Checklists

• Employees should complete quarterly safety self-checklists.

---

9. Expenses and Reimbursements

9.1 Allowed Costs

• Reimbursable expenses include internet costs, office supplies, and ergonomic equipment.

9.2 Per-Day Caps

• Maximum reimbursement of $50 per day for work-related expenses.

9.3 Required Proofs

• Receipts must be submitted with the Expense Reimbursement Form within 30 days of the expense.

---

10. Compliance and Monitoring

10.1 Acceptable Use

• Employees must comply with the Acceptable Use Policy while working remotely.

10.2 Monitoring

• The company may monitor remote work practices to ensure compliance.

10.3 Misuse Consequences

• Violations may result in disciplinary action, up to and including termination.

---

11. Exceptions and Escalation Paths

11.1 Exceptions

• Any exceptions to this policy must be approved by HR and the employee's manager.

11.2 Escalation Paths

• Decisions regarding eligibility may be appealed to HR.

---

12. Appendix

12.1 Glossary

- **VPN:** Virtual Private Network
- **MFA:** Multi-Factor Authentication
- **KPI:** Key Performance Indicator
- **OKR:** Objectives and Key Results

12.2 Related Policies

- IT Security Policy
- Code of Conduct

12.3 FAQ

Q1: Can I work from a different country?
A1: Yes, but prior approval from your manager and HR is required.

Q2: What if I need to work outside core hours?
A2: You may adjust your schedule but must inform your team.

Q3: How do I report a health and safety issue?
A3: Report it to your manager and complete an incident report form.

Q4: What happens if I lose company equipment?
A4: Report it immediately; replacement may be employee responsibility depending on circumstances.

Q5: How often is performance evaluated?
A5: Quarterly, based on KPIs and OKRs.

Q6: Who can I ask about this policy?
A6: Contact your HR representative.

Q7: Can I use my personal device for work?
A7: Yes, but BYOD rules must be followed.

End of Policy Document