

## **Remote Work Policy**

### **1. Objective**

The purpose of this policy is to set guidelines for employees while working from home.

### **2. Scope**

This policy applies to employees who are permitted to work in a home office. The consideration for remote work requires a written recommendation from the direct supervisor and shall be finalized by the Head of Department and HR.

### **3. Policy Guidelines**

- **Compliance with Policies and Procedures:** Employees remain obligated to comply with all company rules, practices and instructions as outlined in the HR Policy manual.
- **Workspace Expectations**
  - Remote work shall only be performed from the employee's primary residence and employees are required to:
    - ✓ Designate a workspace that is quiet and distraction free.
    - ✓ Workspace that is dedicated for placement and installation of equipment to be used while teleworking.
    - ✓ Maintain this workspace in a safe condition, free from hazards and other dangers to the employee and equipment.
    - ✓ The company shall not be responsible for costs associated with the setup of the employee's home office, such as remodeling, furniture or lighting, nor for repairs or modifications to the home office space.
  - Employee is expected to submit three photos of the home workspace to management prior to implementation wherever feasible.
  - **Schedule:** A general schedule must be communicated to the employee and agreed to by the direct supervisor. Deviations from that schedule if any, should be immediately communicated to the supervisor.
  - **Attendance:** The employee must adhere to attendance and break schedules as agreed upon with their manager and in compliance with the company policy.
  - **Performance objectives:** The Supervisor is encouraged to submit a formal work plan for the employee working remotely. The plan will identify and outline areas of responsibilities, daily tasks and measurable long term objectives and short terms goals. For agent staff, the performance reports must be published on a daily basis.
  - **Availability and Communication:** Employees undertaking remote work must be logged into the company's communication platform each day to ensure that they are accessible and can easily participate with their team members. Employees must be available by phone, email, Microsoft Teams or any other login id (if client specified) during scheduled shift hours including web cam viewing (if mandated only) and also be present for staff meetings, if required. Any exceptions shall require prior permission from the direct supervisor.
  - **Role of Supervisor:** The Supervisor shall ensure that the employee is working in accordance with the Remote Work Policy, review and sign-off on records of hours worked (timesheets) as and when required, monitor and review the Remote Work Policy

agreement on a regular basis and schedule communication meetings including methods of disseminating information to employees who are working from home.

- Company materials taken home, if any, should be kept in the designated work area at home and not be made accessible to others.
- The company reserves the right to make on-site visits to the remote work location (only if need be) for purposes of determining that the site complies with the rules set forth herein and to maintain, or retrieve company-owned equipment, software, data or supplies.
- Employee may use only the computer accounts and workspace authorized by the company. Use of another person's account, identity, security devices/tokens, or presentment of false or misleading information or credentials, or unauthorized use of information systems/services is prohibited.
- Employees are responsible for all use of information systems conducted under their user ID(s) and are expected to take all precautions including password security and file protection measures to prevent use of their accounts and files by unauthorized persons/entities. Sharing of passwords or other access tokens with others is prohibited.
- To protect access to information systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the company has the right with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. The company may also monitor, record, inspect, copy, remove or otherwise alter any data, file, or system resources in its sole discretion. The company further has the right to periodically inspect systems and take any other actions necessary to protect its information systems including monitoring employee keystrokes. The company also has access rights to all files and electronic mail on its terminal systems. Anyone using these systems expressly consents to such oversight.
- Equipment supplied by the employee, if deemed appropriate by the organization, will be maintained by the employee. However the company accepts no responsibility for damage or repairs to employee-owned equipment.
- The company reserves the right to reject from the network or block electronic communications and content deemed not to be in compliance with this or other policies governing use of company's information systems.

- **Equipment to be Provided by Employee**

- Computer System (if not provided for by the company)
- Internet Bandwidth
- Web Camera (not a mandatory requirement unless specified)
- USB or 3.5mm Headset with Microphone

- **Employer Provided Equipment and Maintenance / Usage Expectations**

- Employees will be provided equipment that is essential to their job duties and the list of such equipment shall be notified.

- **Equipment provided by the company is company property and employees must keep it safe and avoid any misuse by adhering to the below guidelines:**

- Keep equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Follow all data encryption, protection standards and settings.
- Refrain from downloading suspicious, unauthorized or illegal software.
- Make sure to always lock the system when taking a break.

- Comply with the terms of computer software license and copyright agreements, computer virus and protection requirements and procedures.
- **Right to seize/inspect company-owned Computing Devices:** The company reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other company-owned computing device, to seize such device and/or copy, any and all information from the data storage mechanisms of such device as may be required in the sole discretion of the company in connection with investigations of possible wrongdoing or legal action. In addition to the foregoing, privately owned devices connected to the company network are also subject to inspection by authorized company personnel.
- **Home Safety:** It is expected that the employee's workspace at home must meet the following standards:
  - Temperature, ventilation, lighting, and noise levels are adequate for maintaining a home office.
  - Electrical equipment is free of recognized hazards that would cause physical harm (frayed, exposed, or loose wires; loose fixtures, bare conductors, etc.).
  - Electrical system allows for grounding of electrical equipment (three-prong receptacles).
  - The home workspace (including doorways) is free of obstructions to permit visibility and movement.
  - Phones lines, electrical cords, and surge protectors are secured under a desk or alongside a baseboard.
  - The home workspace should be free of combustibles, floors are in good repair, and carpets are well secured.
- 4. Employees who leave the company are obligated to return any confidential files and equipment back to the company. The equipment shall be in the same condition as at the time of issuance. The I.T. team shall inspect the equipment and recovery, if any for repairmen, shall be charged to the employee at the time of clearance and full and final settlement.
- 5. **Consequences of Policy Violation**

Any unauthorized, inappropriate, illegal or other use of company's information systems or failure to comply with this policy shall subject the violator to disciplinary action by the company, including, but not limited to, termination of employment and criminal prosecution.
- 6. The company reserves the right to revise all or any portion of this policy at any time and from time to time in its sole discretion, subject to applicable laws, rules and regulations.
- 7. Any deviation in the policy shall need approval of the Global CPO.

---

I have read and been informed about the content, requirements, and expectations of the Remote Work Policy. I have received a copy of the policy and agree to abide the policy guidelines as a condition of my employment.

Employee Name	<u>HUMA KHAN</u>
Employee Signature	<u>HUMA KHAN</u>
Date	<u>20/05/2022</u>