Remote Work Policy

1. Purpose

The purpose of this Remote Work Policy is to provide employees with flexible work arrangements while ensuring compliance with organizational security, confidentiality, and data protection requirements. This policy works in conjunction with the Information Security Policy.

---

2. Scope

This policy applies to all employees approved to work remotely, either partially or fully. All remote work arrangements are subject to compliance with the organization's Information Security Policy and related IT guidelines.

---

3. Remote Work Eligibility

- Employees may work remotely **up to 3 days per week**.
- Remote work eligibility is determined by the reporting manager based on job role, performance, and business needs.
- Remote work is a privilege and may be revoked at any time for operational or security reasons.

---

4. Approval Process

4.1 Manager Approval

- All remote work requires **prior approval from the employee's manager**.
- Employees must submit remote work requests in advance through the approved system.
- Approval may be denied or modified based on team coverage, performance, or security concerns.

4.2 Policy Acknowledgment

Employees must acknowledge and agree to comply with:

- Remote Work Policy
- Information Security Policy
- Any additional IT or data protection guidelines

---

5. Work Schedule and Availability

5.1 Core Working Hours

- Employees must be available during **core working hours** as defined by the organization.
- Employees must remain reachable via approved communication tools.
- Failure to maintain availability may result in revocation of remote work privileges.

---

6. Security and Compliance Requirements

6.1 Approved Devices

- Employees must use **company-approved devices only**, as defined in the Information Security Policy.
- Use of personal devices is prohibited unless explicitly approved by IT.

6.2 Access Control

- Employees must not share login credentials under any circumstances.
- Passwords must be managed in accordance with company security standards, including periodic changes.

6.3 Network Security

- Employees must use secure internet connections.
- Use of public or unsecured Wi-Fi for company work is discouraged unless protected by a company-approved VPN.
- Devices must be locked when unattended.

---

7. Data Protection and Confidentiality

- Confidential and sensitive data must be handled in compliance with company security policies.
- Company data must not be stored on personal devices or external storage without authorization.

- Employees must ensure that unauthorized individuals cannot view or access company information.

---

8. Incident Reporting

Remote employees must immediately report:

- Lost or stolen devices
- Suspected data breaches
- Phishing attempts or unauthorized access

Incidents must be reported according to the procedures defined in the Information Security Policy.

---

9. Performance and Monitoring

- Remote employees are subject to the same performance standards as on-site employees.
- The organization reserves the right to monitor system usage to ensure productivity and security compliance, in accordance with applicable laws.

---

10. Policy Violations

Violation of this policy or related security policies may result in:

- Revocation of remote work privileges
- Disciplinary action
- Further action as defined in company policies

---

11. Review and Amendments

This policy may be updated periodically to align with business needs and security requirements. Employees will be notified of any changes.

---

12. Conclusion

This Remote Work Policy enables flexibility while maintaining accountability and security. Employees are expected to follow all guidelines responsibly to protect company information and ensure operational effectiveness.