Remote Access Policy

Policy Title: Remote Access Policy
Policy Number: 33-2.1
Version: 1.0
Effective Date: 01/01/2025
Approving Authority: J&K Booking Agency

1. Purpose

The purpose of this policy is to define the requirements for securely accessing J&K Booking Agency's network, data, and systems remotely. The policy ensures that remote access is granted to authorized employees, contractors, and other third parties in a secure manner, reducing the risk of data breaches, unauthorized access, and malware infections.

2. Scope

This policy applies to all employees, contractors, consultants, and third-party vendors who require remote access to J&K Booking Agency's systems, applications, and data. It covers all devices (e.g., desktops, laptops, mobile devices) that are used to access the network remotely.

3. Policy Statements

3.1. Authorized Access

- Remote access is granted only to employees, contractors, and third parties who require access for business-related purposes.
- All remote access must be approved by the employee's department head and the IT department.

3.2. Authentication and Authorization

- Remote access must be secured through multi-factor authentication (MFA), which includes at least two forms of identification: something you know (password) and something you have (token, phone app, etc.).
- Access will only be granted to specific systems and resources necessary for the employee's role.
- Strong password policies must be adhered to for all accounts used for remote access. Passwords should meet complexity standards.

3.3. VPN Access

- Employees must use the company-approved Virtual Private Network (VPN) to access J&K Booking Agency's network remotely. The VPN must be configured to use strong encryption to protect data during transmission.
- VPN access is logged, and access logs will be reviewed regularly to ensure compliance with the policy.

3.4. Device Security

- All devices used to access the company's network remotely must have up-to-date antivirus software installed, with automatic updates enabled.
- Remote devices must have encryption enabled to protect sensitive data in case of device theft or loss.
- Remote access via personal devices is permitted only if the device complies with the company's security requirements. Personal devices that do not meet the standards may be denied access.

3.5. Data Protection

- Employees must ensure that all sensitive or confidential data accessed remotely is stored in company-approved systems and is not saved locally on remote devices unless explicitly permitted.
- Employees must not share or transmit sensitive information via unencrypted or insecure methods (e.g., unencrypted email, untrusted cloud storage).

3.6. Network Security

- All remote access must be conducted via a secure network (e.g., home networks, public Wi-Fi networks must be avoided unless a secure VPN is used).
- The IT department must monitor the network for unauthorized access or unusual activity, including during remote access sessions.

3.7. Termination of Access

- Remote access privileges will be revoked immediately upon termination of employment or when no longer required for business purposes.
- Employees must return any company-issued equipment and revoke remote access credentials upon termination or when access is no longer needed.

3.8. Compliance

- All users must comply with J&K Booking Agency's data protection policies, including the handling, storage, and transmission of sensitive or confidential information.
- Failure to comply with the terms of this policy may result in disciplinary action, including termination, and legal consequences where applicable.

4. Roles and Responsibilities

- **Employees** are responsible for ensuring that they follow the guidelines outlined in this policy and maintain the security of their remote access devices.
- **IT Department** is responsible for granting, monitoring, and reviewing remote access permissions, providing training, and enforcing security measures.
- **Department Heads** are responsible for approving remote access requests for employees within their departments.

5. Enforcement

This policy will be enforced through the following mechanisms:

- Regular audits of remote access logs.
- Security scans of remote access devices to ensure compliance with encryption and antivirus requirements.
- User training and awareness campaigns regarding remote access security.

6. Exceptions

Any exceptions to this policy must be approved in writing by the employee's direct supervisor, CISO and CEO and must be documented with justification and a risk assessment.

7. Policy Review

This policy will be reviewed annually or when there are significant changes to company infrastructure, technology, or legal requirements.