Draft 6.5 Remote Access Policy:

Purpose: The purpose of this policy is to establish guidelines for remote access to the organization's information technology (IT) resources, including networks, systems, and data. Remote access refers to accessing these resources from outside the organization's physical premises, including through virtual private networks (VPNs) or other secure connections.

Scope: This policy applies to all employees, contractors, vendors, and third-party users who access the organization's IT resources remotely. It covers all devices used for remote access, including laptops, smartphones, tablets, and other personal devices.

Policy:

1. Access: Remote access to the organization's IT resources is granted based on business needs, job requirements, and approved by the respective department head or IT manager. All requests must be submitted through the IT helpdesk or any other designated process. Remote access must be enabled with the appropriate security controls such as multi-factor authentication.

2. Security Requirements: All remote access sessions must be secure and comply with the organization's information security policies and standards. Remote access sessions should be encrypted and require authentication using approved methods such as tokens, smart cards, or biometrics. Remote access should not be conducted through public or unsecured networks, such as public Wi-Fi unless an authourized VPN is used.

3. Passwords: Passwords used for remote access should comply with the organization's password policy. Passwords should be unique and not used for any other accounts. Passwords must be changed regularly and never shared with anyone.

4. Device Requirements: Remote access should only be conducted from approved devices that comply with the organization's IT standards and security policies. All devices should have updated antivirus and security software. Personal devices used for remote access should comply with the organization's Bring Your Own Device (BYOD) policy.

5. Data Protection: All data accessed remotely must be protected in accordance with the organization's data protection policies and standards. Data should not be stored on personal devices, including laptops or mobile devices, without encryption or authorization. Data should only be transferred using secure methods, such as VPNs or secure file transfer protocols.

6. Monitoring and Auditing: All remote access sessions should be monitored and logged to detect and respond to any suspicious or unauthorized activity. Logs should be reviewed regularly and retained according to the organization's data retention policy.

7. Termination of Access: Remote access should be terminated immediately upon termination of employment or contract. Remote access should also be terminated if a device is lost or stolen, or if there is any suspected or confirmed security breach.

Enforcement: Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Violations may also result in legal action, including civil or criminal penalties.

Review: This policy will be reviewed annually or more frequently if needed by the IT department to ensure it remains current and effective.