Scenario:

Your organization plans to implement a BYOD (Bring Your Own Device) policy.

Security Risks Assessment and Mitigation Strategies

|  |  |  |  |
| --- | --- | --- | --- |
| # | Security Risk | Description | Mitigation Strategy |
| 1 | Data Leakage | Employees may transfer sensitive data to personal or insecure platforms. | - Conduct orientation sessions on the Data Privacy Act and raise awareness about data protection practices.  - Provide training on employees' accountabilities and responsibilities related to handling sensitive information. |
| 2 | Lost or Stolen Devices | Unauthorized access due to misplaced or stolen personal devices. | - Enforce device encryption and strong authentication.  - Enable remote wipe via MDM.  - Require immediate incident reporting. |
| 3 | Malware and Untrusted Apps | Malicious apps may compromise devices and network integrity. | - Enforce the use of authorized and vetted applications only on all devices connected to the network.  - Implement Mobile Device Management (MDM) or endpoint protection solutions to monitor and control app installations.  - Conduct regular cybersecurity awareness training for personnel to recognize and avoid malicious apps.  - Regularly update software and security patches to reduce vulnerabilities. |
| 4 | Lack of Visibility and Control | IT cannot fully manage or monitor personal devices. | - Deploy endpoint management tools.  - Conduct regular inspections.  - Create clear usage and monitoring policies with employee consent. |
| 5 | Network Access Risks | Devices may connect to unsecured networks or pose threats to internal systems. | - Require VPN for remote access.  - Apply Network Access Control (NAC).  - Use VLAN segmentation and strict firewall policies. |