**Introduction**

This Mobile Device Policy outlines the procedures and requirements for using mobile devices, including smartphones, tablets, and laptops, to access company data and resources. This policy applies to all employees, contractors, and temporary workers who utilize mobile devices for business purposes.

**2. Device Ownership**

The company may provide mobile devices to employees for work purposes. These devices and all data stored on them are the property of [Company Name].

Employees may also use personally owned mobile devices (BYOD) to access company data and resources. However, such use must comply with the provisions outlined in this policy.

**3. Device Security**

* All mobile devices used for work, whether company-owned or BYOD, must be secured with a strong password, PIN, or biometric authentication.
* Users are responsible for keeping their device software and applications updated with the latest security patches.
* Company-issued devices may have additional security features enabled, such as remote wipe capabilities and mobile device management (MDM) software.
* Downloading and installing applications from unauthorized sources is strictly prohibited.

**4. Data Security**

* Company data accessed or stored on mobile devices must be encrypted.
* Users are prohibited from transferring or storing sensitive company data on personal cloud storage services without prior IT department approval.
* Employees should be cautious when using public Wi-Fi networks and avoid accessing sensitive company data on unsecured connections.
* Downloading and installing applications that could compromise company data security is strictly prohibited.

**5. Lost or Stolen Devices**

* In the event of a lost or stolen mobile device, the user must immediately report the incident to the IT Helpdesk.
* The IT department may remotely wipe the device to protect company data.
* Users are responsible for backing up any personal data stored on the device.

**6. Acceptable Use**

* Mobile devices used for work purposes must only be used for authorized business activities.
* Personal use of mobile devices is permitted, but it should not interfere with work duties.
* Using company-issued devices for illegal or unethical activities is strictly prohibited.

**7. Monitoring**

The company reserves the right to monitor the use of mobile devices accessing company data and resources. This may include monitoring network traffic, application usage, and data storage.

**8. Compliance**

* Failure to comply with this Mobile Device Policy may result in disciplinary action, up to and including termination of employment and/or access to company data and resources.

**9. Review**

This Mobile Device Policy will be reviewed and updated periodically to reflect any changes in technology, security best practices, or regulatory requirements.

**10. Questions and Support**

* If you have any questions regarding this Mobile Device Policy, please contact the IT Helpdesk at [Phone Number] or [Email Address].

**Employee Acknowledgement**

By using a mobile device to access company data and resources, you acknowledge that you have read and understood this Mobile Device Policy and agree to comply with its provisions.

**Employee Name (Print):** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Employee Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_