Mobile Phone Policy

At [Organization Name], we recognize the importance of mobile phones as tools for communication and productivity in the modern workplace. This policy outlines the guidelines and responsibilities for the appropriate use of mobile phones by employees, contractors, and authorised users.

Scope

This policy applies to all employees, contractors, and authorised users who have been provided with company-owned or company-issued mobile phones for business purposes. It encompasses the use of mobile phones for work-related communication, as well as personal use within reasonable limits.

Responsibilities

Employees:

- Employees are responsible for using company-issued mobile phones in a professional and responsible manner, adhering to company policies and guidelines regarding acceptable use.
- They must ensure that company-issued mobile phones are used primarily for work-related communication and tasks, and that personal use does not interfere with work responsibilities or productivity.
- Employees should exercise caution when using mobile phones to access sensitive or confidential information and take appropriate security measures to protect against unauthorised access or data breaches.

Supervisors/Managers:

- Supervisors or managers are responsible for overseeing the use of mobile phones within their teams and ensuring that company policies and guidelines are followed.
- They must communicate expectations regarding mobile phone usage to their team members and provide guidance and support as needed to ensure compliance with company policies.
- Supervisors or managers should monitor mobile phone usage within their teams and address any concerns or issues promptly to maintain productivity and efficiency.

IT Department:

- The IT department is responsible for managing and maintaining company-issued mobile phones, including provisioning, configuration, and troubleshooting.
- They must ensure that mobile phones are equipped with necessary security measures, such as password protection and encryption, to protect against unauthorised access and data breaches.
- The IT department should provide training and support to employees regarding mobile phone usage and security best practices.

Acceptable Use Guidelines

Work-Related Communication: Company-issued mobile phones should be used primarily for work-related communication, including phone calls, text messages, and emails.

Personal Use: Personal use of company-issued mobile phones is permitted within reasonable limits but should not interfere with work responsibilities or productivity. Employees should refrain from excessive personal use during work hours.

Data Security: Employees must take measures to protect company data and information when using mobile phones, including avoiding downloading unauthorised apps or accessing unsecured networks.

Device Security: Employees should secure company-issued mobile phones with passwords or biometric authentication and report any lost or stolen devices to the IT department immediately.

Compliance: Employees must comply with all relevant laws, regulations, and company policies regarding mobile phone usage, including privacy laws and data protection regulations.

Device Management

Provisioning: Company-issued mobile phones will be provided to employees as necessary for their roles and responsibilities. Employees may be required to sign an agreement acknowledging their responsibilities regarding mobile phone usage.

Configuration: Mobile phones will be configured by the IT department with necessary software, applications, and security settings to ensure compliance with company policies and standards.

Monitoring: The IT department may monitor mobile phone usage for security and compliance purposes, including tracking data usage, app installations, and network connections.

Lost or Stolen Devices

Employees must report any lost or stolen company-issued mobile phones to the IT department immediately. The IT department will take appropriate measures to remotely wipe or disable the device to prevent unauthorised access to company data.

Review and Updates

This policy will be reviewed periodically to ensure its effectiveness and compliance with Australian legislative requirements and industry standards. Updates may be made as necessary to reflect changes in technology, company policies, or legal requirements.

Authorised by

[Sign]

[Name]
[Position]
[Company]