QUADRANT RESOURCES Pvt.Ltd.
ACHIEVE MORE TOGETHER

Mobile Device Policy

Version 1.0

Revision History

Version #	Date (DD-MMM-YYYY)	Details of the Changes	Modified By	Reviewed & Approved By
1.0	03 Nov 2023	First Release	Manu Mitragotri	Sridhar Reddy
1.0	14 Jun 2024	Reviewed No Changes Made	Manu Mitragotri	Sridhar Reddy

Introduction

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows. However, as the capabilities increase so do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of an office building.

Mobile devices include items such as:

- Laptops
- Notebooks
- Tablet devices
- Smartphones
- Smart watches

The purpose of this policy is to set out the controls that must be in place when using mobile devices. It is intended to mitigate the following risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of classified information through observation by the public
- Introduction of viruses and malware to the network
- Loss of reputation

It is important that the controls set out in this policy are always observed in the use and transport of mobile devices.

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Quadrant Resources (Quadrant") systems.

The following policies and procedures are relevant to this document:

- *Access Control Policy*
- *Teleworking Policy*
- *User Access Management Process*
- *Cryptographic Policy*

Mobile device policy

Devices provided by Quadrant.

Unless specifically authorized, only mobile devices provided by Quadrant must be used to hold or process classified information on behalf of the organization.

If you are required to make use of mobile equipment, you will be provided with an appropriate device(s) which will be configured to comply with the organization's policies. Support will be provided by the IT Support Desk who may at times need access to your device for problem resolution and maintenance purposes.

You must ensure that the device is transported in a protective case when possible and is not exposed to situations in which it may become damaged. Do not leave the device unattended in public view, such as in the back of a car or in a meeting room or hotel lobby.

Do not remove any identifying marks on the device such as a company asset tag or serial number. Ensure that the device is locked away when being stored and that the key is not easily accessible.

Do not add peripheral hardware to the device without the approval of the IT Support Desk. The IT Support Desk must be consulted before the device is taken out of the country. This is to ensure that it will work and to consider any insurance implications.

You will not hold classified information on the device unless this has been authorized and appropriate controls (e.g. encryption) put in place. Do not keep access tokens, Personal Identification Numbers or other security items with the device.

Ensure that the device screen locks after a short period of not being used and requires an access code or password to unlock it. Passwords used must be strong and difficult to guess. No unsecured logons (i.e. those that do not require a password) may be set up on the device.

The organization-provided device is for your business use only; it must not be shared with family or friends or used for personal activities. You may be asked to return the device to the [IT Support Desk] at any time for inspection and audit. You must not install any unauthorised software or change the configuration or setup of the device without consulting the [IT Support Desk] first.

Where possible, the device will be secured so that all the data on it is encrypted and so is only accessible if the password is known. If the device is supplied with encryption, do not disable it.

Changes to files held on the device may not be backed up on a regular basis if it is not connected to the corporate network for a period. Try to schedule some time in to achieve this on a regular basis. Do not take your own unencrypted backups of classified information.

Where applicable, virus protection will be installed on the device by the organization. Ensure that the device is connected to the corporate network on a regular basis to allow the virus signatures to be updated. Do not disable virus protection on the device.

The device must not be connected to non-corporate networks such as wireless or the Internet unless a VPN (Virtual Private Network) is used. When in public places, ensure that you site the device such that unauthorised people cannot view (or take photographs or video of) the screen.

Use of personal mobile devices

The low cost and general availability of such devices has fuelled the desire amongst employees and other stakeholders to use their own devices for business use. This is commonly referred to as “Bring Your Own Device” (BYOD). In some cases, this can provide increased flexibility and remove the need for the employee to carry more than one device on a regular basis.

However, the concept of allowing an employee to make use of their own device(s) for business purposes may result in the need for such devices to be subject to additional controls over and above those typically in place for a consumer device.

Common issues and security challenges with BYOD may include:

- Use of the device by other family members
- Default storage of data in cloud backup facilities
- Increased exposure to potential loss in social situations e.g. on the beach, in a bar
- Potential access to websites that do not meet the organizations acceptable use policy
- Connection to insecure networks e.g. unsecured wireless hotspots

- Anti-virus protection and how often the device is patched
- Installation of potentially malicious apps onto the device (often without the user being aware that they are malicious)

These issues must be considered when assessing the suitability of any given device to hold specific data belonging to the organization.

It is a joint decision between the organization and the owner of the device concerning whether any particular device will be used for business purposes. Such use is not compulsory, and the employee has the right to decide whether the additional controls placed on the device by the organization are acceptable and therefore whether they choose to use the device for business purposes.

It is important that the controls set out in this policy are always observed in the use and transport of BYOD mobile devices. Individuals must not use their own devices to hold and process company information unless they have submitted a request to do so, and that request has been formally approved. It is Quadrant's policy to assess each BYOD request on an individual basis in order to establish:

- The identity of the person making the request
- The business reason for the request
- The data that will be held or processed on the device
- The specific device that will be used

Requests must be submitted to the IT Support Desk.

The general principle of this policy is that the degree of control exercised by the organization over the BYOD device will be appropriate to the sensitivity of the data held on it. The information classification scheme in use within Quadrant is described in the document Information Classification Procedure.

Guidance to be used in the decision regarding who should have access to what information on which device is summarised in Table 1 below.

In order to ensure its data is adequately protected it is important for Quadrant to be able to monitor and audit the level of compliance with this policy. The level of monitoring and audit will be appropriate to the classification of the information held on the device.

The methods and timing of monitoring and audit will be such that the device owner's privacy is not invaded and must be in line with applicable privacy legislation. In general, monitoring of usage outside of business hours will be avoided.

In the event of the device being lost or stolen, the owner must inform the IT Support Desk as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it. Quadrant reserves the right to remote wipe the device where possible as a security precaution. This may involve the deletion of non-business data belonging to the device owner.

Upon leaving the organization, the device owner must allow the device to be audited and all business-related data and applications removed.

INFO CATEGORY	EXAMPLE CONTENT	WHO MAY HAVE ACCESS VIA BYOD	TYPES OF BYOD DEVICES	REQUIRED CONTROLS	COMMENTS
Level 0 - Public	Product catalogues, pricing information, company location addresses and contact numbers	Anyone	Any	None	This information is generally available to the public and accessed via publicly accessible means, such as a website
Level 1 – Internal Use	Internal procedures, product details, internal company communications e.g. non-restricted or confidential email	Employees and other approved stakeholders	Laptops Tablets Smartphones	Device password protection Inactive lock Remote wipe Application password protection Periodic audits	This area is the most likely use of BYOD within the organization
Level 2 - Restricted	HR information, bank details, personal information covered by data protection legislation	Restricted groups of employees	Laptops only	Full disk encryption VPN Automated patching Anti-virus Firewall Regular audits	This information must only be accessed via devices with strict security controls. This may practically preclude the use of a BYOD device depending on the circumstances
Level 3 - Confidential	Company resourcing plans, commercial proposals, unpublished financial information	No-one	None	Not applicable	This information must only be accessed via organization-provided devices with strict security controls

Table 1: BYOD requirements