Mobile Device Policy

Vishwakarma University

Internal

Title: Mobile Device Policy.	**Doc No.:**
Approval Date: 18-07-2020	**Review:** Annual
Effective Date: 19-07-2020	**Department:** System and Technology

Ver. No	Release Date	Owner	Approved By	Change details
1.0	19-07-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Purpose

The purpose of this policy is to define standards and procedures for end users who have legitimate business requirements to access corporate data from mobile devices connected to VU's network.

2. Scope

This policy applies to all the VU staff who utilize either VU – owned or personally – owned mobile device to access, store, backup, relocate or access any University or Interested Party – specific data.

This mobile device policy applies to, but is not limited to, all devices and accruing media that fit the following device classifications:

- Laptop, Notebook, Tablet computers
- Smartphones
- Home or personal devices used to access corporate resources

Any mobile device capable of storing corporate data and connecting to VU's network

3. Objective

The objective of this policy is to enable users to access VU data from a mobile device connected to VU's network in secure manner.

4. Policy Statement

- It is the responsibility of every staff of the VU who uses a mobile device to access VU resources to ensure that all security protocols used in the management of data on conventional storage infrastructure

- It is imperative that any mobile device that is used to conduct the VU business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:
- CISO reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to VU's network & infrastructure.
- CISO shall engage in disciplinary action if there is a probable cause to believe that such equipment is being used in such a way that puts the VU's systems, data, users, and interested parties at risk
- Prior to initial use on the VU network or related infrastructure, all mobile devices must be registered with system administrator
- A list of approved, supported mobile devices and related software applications and utilities shall be maintained by system administrator
- Devices that are not on this list shall not be connected to VU infrastructure.
- All users of mobile devices must employ reasonable physical security measures.
- End users are expected to secure all VU assigned or personally owned mobile devices used for VU's business activity
- Any non-VU mobile device used to synchronize with VU's computer systems/ mobile devices/ network on which VU information is stored shall have anti-virus and anti-malware software installed which is deemed necessary by the VU's IT policies
- Confidential data stored on mobile devices other than VU's systems shall be password protected
- Authorized mobile devices that are being used to store the VU's data must adhere to the security requirements of the VU's information security policies.

- System administrator shall follow media disposal policy to permanently erase VU-specific data from authorized mobile devices once their use is no longer required
- In the event of a lost or stolen mobile device it is incumbent on the user to report this to system administrator immediately. The device shall be remotely wiped off with all data and locked to prevent access.
- Any mobile device that is being used to manage VU data must only connect to wireless network that is at least WPA2-AES encrypted. Connection to open wireless network (no encryption) is prohibited.
- Users shall observe their VU provided data card usage. Persistent heavy usage shall be highlighted by system administrator to the CISO and users must provide justifications to their HOD/DEAN. Users are held responsible for charges incurred from excessive personal usage.
- All authorized users using VU issued/ personally owned mobile devices with VU/ personal SIM card shall report mobile device details to system administrator.
- For any department-specific applications needed, the Head of department should seek approval from CISO to allow user to access the same.
- Staff, contractors, and temporary staff shall make no modifications of any kind to VU-owned and installed hardware or software without notifying system administrator.
- CISO reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end-users to transfer data to and from mobile devices on the VU network.

- The end-user agrees to immediately report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of VU resources, databases, networks, etc. to system administrator

5. Enforcement

- Failure to comply with VU policy shall result in immediate suspension of all network access privileges so as to protect the VU's infrastructure.
- Any attempt to contravene or bypass said security implementation shall be deemed an intrusion attempt and shall be dealt in accordance with the VU's HR's disciplinary action policy.

6. Reference Document

- Bring Your Own Device Policy
- Access control Policy
- Media disposal policy
- Acceptable use of information assets policy
- HR IT Policy

7. Distribution List

The following users have access to this policy:

- All Staff and contractors of Vishwakarma University having access to VU information through mobile devices

8. Definitions/Acronyms

- VU: Here it refers to Vishwakarma University
- Staff: Here it refers to Teaching Staff/ Non-Teaching Staff/ Office Staff/ Peons