Bring Your Own Device Policy

Vishwakarma University

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

Table of Contents

1. Purpose

This policy is intended to protect and maintain the security and integrity of VU's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

2. Scope

All mobile devices, whether owned by VU or owned by Staff, that have access to VU's networks, data and systems, not including VU's IT-managed laptops. This includes smartphones, tablet and computers. Limited exceptions to the policy may occur where there is a business need

3. Objective

VU developed this BYOD policy to protect VU's information assets in order to safeguard VU's interested parties, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of all mobile devices when accessing the VU's network and is intended to protect the security and integrity of VU's data and technology infrastructure. VU reserves the right to restrict the use of mobile devices if users do not abide by the policies and procedures outlined below. VU's Staff must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the VU's network.

4. Policy

4.1. Acceptable Use

- The VU defines acceptable business use as activities that directly or indirectly support the business of VU.
- Staff are blocked from accessing certain websites during work hours/while connected to the VU's network at the discretion of the VU.

- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another VU
  - Harass others
  - Engage in outside business activities
  - Store or transmit proprietary information belonging to VU Etc.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, etc., which will be permitted)
- Staff will not use their mobile device to access the following VU owned resources: email, calendars, contacts, documents, etc. unless authorized.

4.2. Connectivity

- Devices must be on the approved list of devices, available from the System Administrator OR you may apply for a device to be added to the approved list by submitting it to the Vice Chancellor who will have full discretion to approve or reject the device.
- The VU reserves the right to refuse or remove permission for your device to connect with the VU's systems. The Management will refuse or revoke such permission and may take all steps reasonably necessary to do so, where in VU reasonable opinion a device is being or could be used in a way that puts, or could put, the VU, VU's Staff, VU's business connections, VU's systems, or VU's data at risk or that may otherwise breach this policy.
- In order to access VU's systems it may be necessary for the IT Administrator OR CISO to install software applications on Staff's device. If you remove any such software, your access to VU systems will be disabled.

4.3. Monitoring

- The contents on the VU's systems and VU data are VU's property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on VU behalf is VU's property, regardless of who owns the device.
- VU reserves the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on VU's behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device [as well as keystroke capturing and other network monitoring technologies], whether or not the device is in Staff's possession.
- In case of VU owned mobile devices, it is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore Staff should have no expectation of privacy in any data on the device. Staff are advised not to use VU's systems for any matter intended to be kept private or confidential.
- In case of VU owned mobile devices, monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, in order to: prevent misuse of the device and protect VU data; ensure compliance with VU rules, standards of conduct and policies in force from time to time (including this policy); monitor performance at work; and ensure that Staff members do not use VU's

facilities or systems for any unlawful purposes or activities that may damage VU's business or reputation.

- VU may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. VU may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.
- By signing the declaration at the end of this policy, Staff confirm the agreement (without further notice or permission) to such monitoring and to VU's right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). Staff's also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

4.4. Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Email related issues are handled by the System Administrator
- Devices must be presented to the System Administrator for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

4.5. Reimbursement

Only in case of non-VU owned mobile devices;

- The VU will not reimburse the Staff for any percentage of the cost of the device.
- The VU will not cover the cost of the entire phone/data plan.
- The VU will reimburse the Staff for the following charges: roaming, plan overages, etc.

4.6. Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required
- The users should comply with the VU's Password Policy norms on the portable devices as well
- Passwords will be rotated quarterly and the new password can't be one of the previous passwords.
- The device must lock itself with a password or PIN if it's idle for two minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Staff are automatically prevented from downloading, installing and using any app without the CISO/Vice Chancellor's approval.
- Staff' access to VU data is limited based on user profiles defined by CISO/ Vice Chancellor and automatically enforced.
- The Staff's device may be remotely wiped if

1) The device is lost,
2) The Staff terminates his or her employment,
3) IT detects a data or policy breach, a virus or similar threat to the security of the VU's data and technology infrastructure

4.7. Risks/Liabilities/Disclaimers

- While System Administrator will take every precaution to prevent the VU's data from being lost in the event it must remote wipe a device, it is the System Administrator's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The VU reserves the right to disconnect devices or disable services without notification
- Lost or stolen devices must be reported to the VU within 24 hours. Employers are responsible for notifying their mobile carrier immediately upon loss of a device
- The Staff is expected to use his or her devices in an ethical manner at all times and adhere to the VU's acceptable use policy as outlined above
- The Staff is personally liable for all costs associated with his or her device
- The Staff assumes full liability for risks including, but not limited to, the partial or complete loss of VU and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable
- Any personnel who visits the Examination Department is liable to ensure that he/she does not carry any mobile device inside the premises without approval (written) from Department Head.
- VU reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy

5. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Reference Documents

- Mobile Device Policy
- Acceptable Use of Information Assets Policy
- HR IT Policy

7. Distribution List

The following Staff have access to this policy:

All Staff, contractors, consultants, temporary and other third party contractors of VU.

8. Definitions/ Acronyms

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