NUST BRING YOUR OWN DEVICE(BYOD) POLICY

DRAFT 1 .2022

NUST ICTS TEAM

Table of Contents

1 Overview 2

2 Scope 2

3 Definition of terms 2

4 Policy Statement 2

5 Acceptable Use 3

6 Permitted Devices and Software 4

7 Security 4

8 Risks/Liabilities/Disclaimers 5

Approved by ……

1 Overview

Bring your own device (BYOD) refers to the practice of using a personal computing device (computer, tablet, phone etc.) for work or business related activities.

2 Scope

This policy applies to employees, faculty, students, guests and any other user that utilizes the network or computing resources provided by the University for business related activities with a personally owned device

3 Definition of terms

i. Authorized Users: Refer to the definition in the Acceptable Use Policy and Procedures Section
ii. Pirated Software: is software that is not included in the list of NUST approved software.
iii. BYOD : Bring Your Own Device
iv. Enterprise resource planning (ERP) refers to a type of software that organizations use to manage day-to-day business activities such as accounting, procurement, project management, risk management and compliance, and supply chain operations.
v. A learning management system (LMS) is a software application or web-based technology used to plan, implement and assess a specific learning process.

4 Policy Statement

The University grants its employees and students the privilege of bringing and using smartphones, laptops and tablets of their choosing at work for their convenience. The University reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the University's data and

technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

University employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the University network.

5 Acceptable Use

5.1. The University defines acceptable business use as activities that directly or indirectly supports the business of the University.

5.2. The University defines acceptable personal use on University time as reasonable and limited personal communication or recreation, such as reading or game playing.

5.3. Devices' camera and/or video and other capabilities are not disabled while on-site.

5.4. Devices may not be used at any time to:

- 5.4.1. Store or transmit illicit materials
- 5.4.2. Store or transmit proprietary information belonging to another University
- 5.4.3. Harass others
- 5.4.4. Engage in outside business activities

5.5. The use of applications such as:

- 5.5.1. weather,
- 5.5.2. productivity apps,
- 5.5.3. Facebook, etc. are permitted.

5.6. Pirated applications are not allowed.

5.7. Employees and students may use their computing devices to access the following University-owned resources:

- 5.7.1. email,
- 5.7.2. calendars,
- 5.7.3. contacts,
- 5.7.4. documents,
- 5.7.5. ERP
- 5.7.6. LMS
- 5.7.7. WiFi etc.

6 Permitted Devices and Software

6.1. Smartphones and laptops including iPhones, Android phones

6.2. Devices that have commonly used systems like Windows, MacOS, Linux, Android and IOS are allowed.

6.3. Connectivity issues are supported by ICTS personnel; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

6.4. In some instances devices must be presented to ICTS for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

7 Security

7.1. In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the University's network.

7.2. The University's strong password policy is: Passwords must be at least eight characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords that are linked to the University's ICT services should be rotated every 90 days and the new password can't be one of 15 previous passwords.

7.3. The device must lock itself with a password or PIN if it's idle.

7.4. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.(Security Compromised Devices).

7.5. Employees and students are forbidden from downloading, or installing compromised applications which threaten the University's network.

7.6. The University will permit common devices to connect to the network.

7.7. Employees' and students' access to University data is limited based on user profiles defined by the ICTS department and will be automatically enforced.

7.8. The University data that will be in the employee's device may be remotely wiped out if 1) the device is lost, 2) the user terminates his or her employment, 3) ICTS department detects a data or policy breach, a virus or similar threat to the security

of the University's data and technology infrastructure.

8 Risks/Liabilities/Disclaimers

8.1. While the ICTS department will take every precaution to prevent the users' personal data from being lost in the event it must remotely wipe clean a device, it is the users' responsibility to take additional precautions, such as backing up email, contacts, etc.

8.2. The University reserves the right to disconnect devices or disable services without notification.

8.3. Lost or stolen devices must be reported to the University within 24 hours. Employees and students are responsible for notifying their mobile carrier immediately upon loss of a device.

8.4. The user is expected to use his or her devices in an ethical manner at all times and adhere to the University's acceptable use policy as outlined in Section 7 of the NUST ICT Acceptable Use Policy.

8.5. The user is personally liable for all costs associated with his or her device.

8.6. The user assumes full liability for risks including, but not limited to, the partial or complete loss of University 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.

8.7. The University has no obligation to reimburse individuals whose devices develop a problem presumably through connecting to the network.

8.8. The University reserves the right to take appropriate disciplinary action for noncompliance with this policy.