Bring Your Own Device (BYOD)

2020-05-07

Document Number:

QMZ-BYOD-01.DOCX

Prepared by: Qmuzik Technologies (Pty) Ltd

~~Submitted to:~~

CONTENTS

1. Overview

With the advent of the Smart Devices like the smartphone (which can broadly be defined as a portable computing device) that are being used to access emails and other company information due to their convenience, portability and connectivity, some guidance is needed to manage this new risk to the company. The risk is present due to these devices making use of company infrastructure, and as such new rules and regulations need to put in place to manage this risk.

2. Purpose

This policy establishes Qmuzik Technologies' guidelines for employee use of personally owned electronic devices for work-related purposes, and to protect the security and integrity of ~~Company XYZ's~~Qmuzik's data and technology infrastructure as well as other approved customer data we have for whatever reason. Limited exceptions to the policy may occur due to variations in devices and platforms.

3. Scope

This policy applies to all Qmuzik Technologies employees and affiliates.

4. Policy

4.1. Acceptable Use of your owned device

- The company defines acceptable business use as activities that directly or indirectly support the business of Qmuzik Technologies.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation~~, such as reading or game playing.~~
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.
- Devices' camera and/or video capabilities are not disabled while on-site.
- Devices may not be used at any time to store or transmit illicit materials, store or transmit proprietary information belonging to another company, harass others or engaging in outside business activities.
- There is currently no limitation on the Applications (further referred to as "Apps") that may be installed on devices, until such a time as it is deemed necessary to do so.
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- Qmuzik Technologies has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

4.2. Devices and Support

- Smartphones and tablets including iPhone, Android, Blackberry, Nokia and Windows phones are allowed with no limitations on the models or Operating Systems (OS).
- Connectivity issues may be supported by IT, however employees should contact the device manufacturer or vendor/network carrier for Operating System or hardware – related issues.

- Devices must have installed at least the basic manufacturer's security applications.

4.3. Reimbursement

- The company will not reimburse the employee for the purchase of the device if it is bought primarily for personal use.
- The company will not reimburse the employee for the use of the device unless previously arranged individually per employee contract if the device is used for conducting business.

4.4. Security

- 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 company network. See *QMZ-PASS-01 Qmuzik Password Policy* for further reference.
- The device itself must lock itself with a password, biometrics, facial recognition or a PIN code if it is idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

4.5. Risks, Liabilities, Disclaimers

- The company reserves the right to disconnect / disallow devices from its network
- Any data stored on the device is the responsibility of the device owner. The company will not be liable for personal data stored on the device. All data must be backed up by the device owner if they wish to do so.
- Lost or stolen devices must be reported to the company in order to deactivate access to company resources where it is possible.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company 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.
- ~~Company XYZ~~Qmuzik reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

5. Policy Compliance

5.1 Compliance Measurement

As Information security is o~~a~~f paramount importance at Qmuzik, ~~T~~the Qmuzik Technologies team will verify compliance to this policy through various methods, including but not limited to, periodic checks, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exception

Any exception to the policy must be approved by the Qmuzik Technologies Management team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

None

8. Revision and version control

Version Number	Date	Description of Change	Changed By
1.0	2020/05/07	Creation	Tinus Kleingeld
2.0	2020/05/15	Revision	Adriaan Voges

9. Policy acceptance

The undersigned hereby agrees that this policy is valid and can be enforced.

Name	Role	Signature
