Information Security Document

Bring Your Own Device Policy

Version 1.0

Version 1.0

Confidentiality and usage Statement

This Bring Your Own Device policy document is completely owned by ZAM solutions. This document only contains policies related to the BYOD concept and it is completely created only for the reference of the internal and the external stakeholders associated with ZAM solutions.

The information and the content in this document are confidential and it is only proprietary to ZAM solutions. Any means of unauthorized distribution, sharing or reproduction of this document is strictly prohibited as it is outside the scope of ZAM solutions.

Any request to share this document outside the domain of ZAM solutions will require a written approval form the board of management of the ZAM solutions.

1. Introduction to BYOD

   This document defines the BYOD policy to be followed by the internal as well as the external stakeholders of ZAM solutions. ZAM solutions has a requirement to protect its information assets to safeguard its staff, information assets, data and all the intellectual assets.

   The BYOD policies defined in this document provides a framework which support ZAM solutions in terms of security and technology.

2. Purpose

   The usage of BYOD services poses a high risk and can cause threats to the information systems and security if not properly managed.

   The purpose of this document will be to control the usage of BYOD based on the best practices that is essential to protect ZAM solution's sensitive information in accordance with the ZAM solution guidelines.

3. Scope

   The scope of this document applies to all users, which includes staff, consultants and contactors related to ZAM solutions.

4. BYOD Devices

   The following set of devices are approved for the employees of BYOD use and connecting to the ZAM Solutions network.

   - Android smart phones and tablets
   - IOS phones and iPad
   - Mac book
   - Personal laptops

Before the access to any of the company's network the devices must be presented to the IT department of ZAM solutions for proper provisioning, configuration of standard apps such as browsers, office productivity software and security tools such as anti-virus.

5. Privacy

   ZAM solutions will respect the privacy and the integrity of your personal devices and will only allow authorized technicians to access it to implement security controls, or to respond to any legitimate discovery requests coming from administrative civil or criminal proceedings.

6. Policies

6.1 Device specification

a. All the devices must be registered and verified to ensure that they meet the standards and the device specification policies of the organization and to make sure that those devices are compatible with the ZAM solution's network and security infrastructure.
b. Only the operating systems permitted by the company must be used by all devices and all the devices must meet the minimum hardware requirements prescribe by the IT service department of the company.
c. A safe and strong password must be assigned to all the devices in accordance with the Information security password policy of the company.
d. Only devices which are monitored by the IT department will be allowed to connect to the internal network and any other device will not be allowed to connect to the internal network.
e. It is mandatory to keep all the devices up to date with the patches given by the manufacturers and this must be regularly examined and updated (at least once a month)
f. The devices shall not be linked to a PC that does not have up to date malware enabled and is in violation of policy prescribed by ZAM solutions.
g. Applications such as MDM (Mobile Device Management) must be installed on all the personal devices to ensure secure access to corporate resources.
h. After the registration of the devices, VPN will be set up in those devices by the IT department to securely access the corporate network.
i. The devices must be configured with an auto lock feature which locks the device automatically after five minutes of idle time.

6.2 User responsibility

a. The users are required to register any gadgets that are brought in for use in the IT department.
b. The users are advised to use biometric identification to protect their devices.
c. The users are not allowed to load any pirated software or illegal content onto their devices.
d. The users must only deploy applications from platforms that have been authorized by the platform owner.
e. If the employees are confused whether an application came from a permitted source, the Information security team of the company must be contacted.
f. The users must update their devices with the regular security patches.
g. In case of a lost or stolen device, the company has the right to wipe of the corporate data remotely, therefore the users are advised to have regular backups of their personal data during such remote wipes.

h. Users must avoid combining their professional and personal email accounts on their devices.
i. If the user suspects that any unauthorized access to organization data has occurred, it must be immediately reported to the Information security team via Incident management procedure.
j. In case of a lost or stolen device, this must be reported to the Information Security team immediately.

6.3 Restrictions and authorized usage

a. The users are not allowed to download, share or access illegal content, engage in unauthorized file sharing or participate in any activities that compromise network security.
b. The practice of jailbreaking (iOS) or rooting (Android) personal devices is prohibited due to the security risks associated with these activities.
c. The employees with camera, video or recording capabilities on their personal devices are not permitted to utilize those functions anywhere in the company buildings unless the authorization has been granted in advance.
d. Personal use of work devices during work hours must be avoided as this may result in reducing the productivity of the employees and distract others as well.
e. Unless authorized by the management, the employees are not allowed to use their personal devices for work purposed during their unpaid leave days, ZAM solutions reserves the complete right to disable the company’s application and access on the employee's personal device when required.

6.4 Guidelines to store sensitive information.

a. First and foremost, the precaution to be taken is that the employees must not share their login information with anyone.
b. Any company data transfer must be sent over TLS(HTTPS), to protect the user credentials as well as the data during the transfer.
c. It is advisable to send the data as a single lump than dividing it into small chunks as it saves money and time in terms of latency and operational charges.

7. Roles and responsibilities
    - The information security team of ZAM solutions is responsible for reviewing and implementing these policies.
    - All the employees as well as the management are required to follow these policies strictly.
    - Implementation of each policy will be discussed in detail in the procedure document.

8. Policy review
    This policy document must be reviewed and updated annually according to the ICT laws.

9. Policy Approval
    This policy has been approved by the Senior Information security Auditor of ZAM solutions.

Date of approval: 30/10/2023
Approved by: Ms. Jane Krysten
Senior Information security Auditor
ZAM solutions
Colombo Sri Lanka
011 1234987