Procedure document

For

Bring Your Own Device Policy

Version 1.0

Confidentiality and usage statement

This BYOD (Bring Your Own Device) policy procedure document contains confidential information related to ZAM solution's technology and security practices. Access to this document and any information contained within is restricted to authorized employees, contractors, and associates who have been granted access rights by the company's management. Unauthorized access, disclosure, copying, or distribution of the content in this document is strictly prohibited.

Procedure document

POLICIES

Device specification policies

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.

- First the devices must be brought to the IT department of the company.
- Then the device must be handed over to the Information security officer of ZAM solutions to check the device such as if the device specifications are compatible with the company's set of rules for BYOD devices
- The Information security officers must collect all the details of the devices such as the type of the device, RAM size, serial number.
- Only after registering the personal devices using this procedure, the users are allowed to use it for work purposes.

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 prescribed by the IT service department of the company.

- While registering the devices in the beginning the beginning the prevailing operating systems will be checked and if it is not up to date the operating systems will be updated by the Information security officer in the IT department.
- If any of the devices does not meet the hardware requirements or software requirements required by the company, then that device cannot be registered in the company, and it cannot be used for any work purposes.

c. A safe and strong password must be assigned to all the devices in accordance with the Information security password policy of the company.

- The password must be typically 8 to 12 characters long and it must be a combination of both uppercase letters and lower-case letters. It must also be a combination of numbers as well as special characters.
- The passwords must be changed frequently, and it must be between regular intervals. Each user must change their passwords every 60 to 90 days.
- It is advised for the users to use multi factor authentication for added security and the guidance for setting up Multi factor authentication will be provided by the IT department of the company upon the user request.
- The users are advised not to use any of their passwords again and again to enhance security.
- An account lockout policy will be configured by the IT department while registering the device and the threshold will be 5 invalid login attempts, if there were 5 invalid login attempts the device can be temporarily.
- In case of lock outs, the user must contact the IT department and has to bring the device to the company physically to unlock it.
- The user can reset their passwords by completing two steps such as first the user has to authorize his email address and then has to answer the three security questions correctly, which he/she might have answered at the beginning while setting up the passwords.

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.

- The users are not allowed to connect their BYOD devices directly to the internal network unless or otherwise the user has obtained authorized written permission from the senior Information security officer of the company or the user's device is being monitored by the IT department.
- Only the devices owned by the company are monitored by the IT department therefore the users cannot connect their BYOD device to the internal network directly unless for an exception.
- If the user must connect the BYOD device to the internal network directly, they have to obtain an authorized letter from the senior information security officer of ZAM solutions priorly.

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)

- While the user registers the device, the user will be advised regarding the patches which will be categorized into many types as critical, important, and optional, and the users must focus on critical and important patches for security. One of such critical patches is updating the Malware.
- Under the category of user help in the internal company website, there are materials which explains the users regarding the importance of security patches and how to update their devices, and this can be used if the employee doesn't have much idea regarding how to update a security patch.
- The automatic update feature must be turned on in all the BYOD devices and the time frames can be scheduled appropriately.

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.

- The users are strictly prohibited from linking their devices to a PC or another device which does not have up to date malware and this is considered as a rule violation and will be considered as a serious offense.

g. Applications such as MDM (Mobile Device Management) must be installed on all the personal devices to ensure secure access to corporate resources.

- The users are required to use Mobile Device Management (MDM) or Endpoint Management solutions to help manage patch updates for BYOD devices as those tools can help in the enforcement of patch update policies and track compliance.

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.

- While setting up VPN the IPsec VPN must be used and L2TP protocol must be used.
- Tools and processes to enforce policy compliance and monitor the status of BYOD devices using the VPN.
- The VPN policy must align with evolving security threats, technology, and best practices must be followed by keeping the VPN system up to date.

i. The devices must be configured with an auto lock feature which locks the device automatically after five minutes of idle time.

- This feature will be set up while registering the device for BYOD, then this will be enabled in the devices.

j. In case of a lost or stolen device, this must be reported to the Information Security team immediately.

- In case of a lost or stolen device, the user has to immediately report it to the Information Technology department of the company.
- In case of reporting any such incident, as advised earlier, a remote data wipe will be performed, and the user has to ensure that their personal data has a backup.
- The data erasure will be performed as identification of the lost device, conforming ownership, initiating remote access using the mobile device management or any other remote management tools, reviewing the applicable laws, collecting any evidence if possible and then executing data erasure.
- The device will be tracked using the built-in device tracking feature such as find my device.

User responsibility policies

a. The users are required to register any gadgets that are brought in for use in the IT department.

- The users must first bring their devices to the company and provide them to the IT department for inspection.
- Then the BYOD service user must fill in a form which collects details like the user's name, device model, device specification, position of the user and some more information to register their device/devices.
- The user must sign the agreement saying that he/she is willing to adhere to the BYOD policy of the company.

b. The users are advised to use biometric identification to protect their devices.

- The users can use their biometrics such as fingerprint or facial detection to access their BYOD devices as this enforces increased security and can reduce the risk of any other person gaining access to that system.

c. The users are not allowed to load any pirated software or illegal content onto their devices.

- The users must only load software from authorized sources to their devices and it must only be downloaded from the authorized platforms.
- Most of the software required for work will be provided by the company through drives or this software can be installed via handing over your device to the Information technology department.
- If the users are downloading that software by themselves, they must check the reliability of the platform.

d. The users must only deploy applications from platforms that have been authorized by the platform owner.

- The users must check the authorization of the platform before loading any data to their BYOD device and must only deploy the applications in the platforms if only it is 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.

- In case of any doubts regarding an application's source, the user can contact a professional from the IT department to clarify it.
- Moreover, the IT department contains documents with the applications which will be needed during the work related to the company and the permitted sources from where these applications can be downloaded. The users can also access these documents to obtain necessary details.

f. The users must update their devices with the regular security patches.

- While the device is registered under the BYOD policy, the users must be given a list which contains all the details of the critical and non-critical security patches associated with that device.
- The users must be advised to update the critical security patches once a week and the non-critical security patches can be updated once a month.
- Awareness must be provided by the Information security department regarding the importance of updating security patches.
- Endpoint security solutions must be implemented on all BYOD devices that connect to the company's external network, including antivirus, anti-malware, and host-based firewalls.

g. In case of a lost or stolen device, the company has the right to wipe off the corporate data remotely, therefore the users are advised to have regular backups of their personal data during such remote wipes.

    - The users must backup their data in the BYOD device every two weeks to avoid data loss during the remote wipe of data.

h. Users must avoid combining their professional and personal email accounts on their devices.

    - The users are advised to maintain two different user accounts in the BYOD device, one for personal usage and one for work purposes.
    - All the work-related documents must be stored in the work-related account and the work-related emails also must only be handled via the work-related account.
    - All the work-related mail received and forwarded will be monitored by the company.

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.

    - At the case of such event the user must fill the Incident Reporting form available on the company's portal as soon as possible and this is accessible by all the employees.
    - The user must not alter or delete any data on that device once such an incident has occurred as there are possibilities for the evidence to be destroyed.
    - Preservation of evidence is crucial for the investigation.
    - The IT or security team should investigate the incident thoroughly to determine the scope and impact of the breach and collect evidence as much as possible.
    - The junior information systems officer must document all actions taken during the incident response, including communication, containment measures, and findings from the investigation.
    - This document has to be submitted to the senior information security officer.

j. In case of a lost or stolen device, this must be reported to the Information Security team immediately.

    - In case of a lost or stolen device the user must report this issue to the Information Security department of the company immediately

- The Information security department must launch a police complaint regarding the device.
- The Information Security department must perform an immediate remote data wipe.
- In built feature such as find my device and find my phone will be used to locate the lost device

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.

- The information security department should create an Acceptable user policy (AUP) and the users has to adhere according to that acceptable user policy.
- The AUP will outline what is considered acceptable and unacceptable behavior on the network.
- The Mobile Device Management or Mobile application Management must be configured to restrict the installation of unauthorized apps from the untrusted sources by the IT department.
- While the user registers the device for BYOD the network access controls must be implemented by the IT department to restrict access to specific websites or types of content. This can be done using firewalls, content filtering, and intrusion detection/prevention systems.
- Role-based access control (RBAC) must be implemented by the IT department to limit user privileges and provide access to the users based on their job roles.
- Educational sessions must be conducted for the employees about the risks associated with downloading or sharing illegal content and engaging in unauthorized file sharing.
- Training sessions will be provided by the IT department for the users to recognize social engineering tactics and phishing attempts.

b. The practice of jailbreaking (iOS) or rooting (Android) personal devices is prohibited due to the security risks associated with these activities.

- The rooting of Android devices and jailbreaking of iOS devices is strictly prohibited on personal devices used within the company's network or premises as under the BYOD policy.

- All personal devices registered under BYOD connecting to the company network or accessing company resources must maintain their original, unaltered operating systems and configurations.
- If a user performs rooting or Jail breaking, this will be considered as a violation of rules in the company.
- Once a user performs any such activity, his permission of BYOD will be cancelled, and he will have to face a legal trial to decide if the employee is terminated or not.
- The violation of this policy may result in taking disciplinary actions such as verbal or written warnings, temporary suspension of privileges, termination of the employment contract and also legal action if applicable.

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.

- Unauthorized use of cameras, video, and recording functions on personal devices is strictly prohibited within company buildings.
- Employees who need to use cameras, video, or recording functions for legitimate business purposes or any valid reason must obtain prior permission from their department head and the senior information security officer.
- Even if permission is obtained recording is prohibited in areas designated as sensitive, secure, or restricted. This also includes research and development facilities, laboratories, restrooms, and any areas marked as "No Recording."
- Employees and visitors are expected to respect the privacy and consent of others. Recording without the explicit consent of all the individuals involved is a violation of this policy.
- The violation of this policy may result in taking disciplinary actions such as verbal or written warnings, temporary suspension of privileges, termination of the employment contract and also legal action if applicable.
- The company will actively be monitoring in accordance with this policy. Employees are encouraged to report policy violations to the IT department, or security personnel. Any reported violations will be investigated thoroughly, and appropriate actions will be taken.

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.

- Usage of devices for personal work during work hours should be avoided. Devices registered under BYOD are primarily for business-related tasks during work hours.
- If employees choose to use work devices for personal tasks during work hours, it should be limited to non-disruptive activities that do not interfere with their job responsibilities.
- All usage of BYOD devices, whether for work or personal purposes, must comply with all company policies, including those related to data security and acceptable use.
- When using work devices for personal activities, employees must ensure the security and confidentiality of company data and information.
- Violation of this policy may result in verbal or written warnings, Loss of BYOD privileges, Termination of participation in the BYOD program and also legal actions if applicable.

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.

- The company has the complete right to disable access to its applications and resources on an employee's BYOD device when there is a valid business need or security concern.
- Employees will be notified in advance if possible if their access will be disabled. However, in certain situations, immediate action may be required for security reasons.
- Employees whose access is disabled must request and receive authorization The junior Information Security manager or the IT department to have access re-enabled.
- Employees are responsible for regularly backing up their personal data and information on their BYOD devices to avoid data loss in the event of access disabling.
- All access disabling and re-enabling procedures must adhere to company policies and procedures, including those related to data security and the terms of acceptable usage.
- Violation of this policy may result in verbal or written warnings, loss of access to company resources in BYOD, termination of participation in the BYOD program and also legal actions if applicable.

Statement of understanding

Including a confidentiality and usage statement in your BYOD policy procedure document reinforces the importance of data security and responsible usage, and it serves as an agreement between the company and its employees and contractors regarding the policy's terms and conditions.

Date of approval: 30/10/2023
Approved by: Ms. Jane Krysten,
Senior Information security Auditor,
ZAM solutions,
Colombo, Sri Lanka
011 123498