Cybersecurity Improvement Program Q&A

1. **Why do I have to use my personal device for work?**
    - **Answer:** The BYOD policy allows employees to use their personal devices for work purposes, offering flexibility and convenience. It enables you to access work-related applications and information from anywhere, improving productivity and work-life balance.
2. **Will the company be able to see my personal data on my device?**
    - **Answer:** No, the company cannot see your personal data. Microsoft Intune only manages work-related apps and data. Your personal files, photos, and apps remain private and inaccessible to the company.
3. **What exactly will the company have access to on my device?**
    - **Answer:** The company will only have access to work-related data and applications managed through Microsoft Intune. This includes the company's email/calendars/ contacts, and work documents. Personal data and applications remain private.
    - Additionally, Microsoft Intune ensures your device meets security standards by checking for measures such as having antivirus software installed, ensuring patch updates are enabled, and verifying the operating system version and serial number.
4. **What happens if I leave the company?**
    - **Answer:** If you leave the company, the IT Division will remotely remove the company's data and work-related applications from your device using Microsoft Intune. Your personal data and apps will remain unaffected. You can also disconnect your device from the company portal by following the provided guidelines.
5. **Will my device's performance be affected by installing Intune?**
    - **Answer:** Microsoft Intune is designed to have minimal impact on your device's performance. It runs in the background and only manages work-related data and applications.
6. **What should I do if I encounter technical issues with my device?**
    - **Answer:** In case you encounter any technical issues, you can contact the IT Team at your campus for assistance by sending an email to IThelpdesk@vas.edu.vn. For more detailed questions about security, you can reach out to Mr. Mai Thanh Trung, our IT Information Security Manager.
7. **Can I access company resources on my device without an internet connection?**

- **Answer:** Access to some company resources requires an internet connection, while others may be available offline.

8. **How does the company ensure my device's security?**
    - **Answer:** After registration to the VAS BYOD Portal, devices will have the settings applied and will undergo evaluation based on the criteria in the table below:

Windows	MacOS	Android	iOS/iPadOS
After the user registers their device with the BYOD Portal, VAS will apply the following settings: • Turn on Device Firewall. • Require a built-in password to unlock device: - Minimum password length: 8 characters - Password complexity: Require numerical characters, lowercase letters, uppercase letters - Password expiration: 90 days. • Ensure Windows Security is always turned on and up to date. In the case of using a 3rd party anti-virus solution (such as McAfee, Kaspersky etc.), it must be up to date and always turned on.	**After the user registers their device with the BYOD Portal, VAS will apply the following settings:** • Turn on the Device Firewall. • Require a built-in password to unlock device: - Minimum password length: 8 characters - Password complexity: Require numerical characters, lowercase letters, uppercase letters - Password expiration: 90 days. • Turn on System Integrity Protection, real-time protection, and cloud-delivered protection. Allow apps to be downloaded from Mac App Store and identified developers.	**After registration, devices will undergo an evaluation that includes the following criteria:** • Encryption of data storage on devices is required. • A password is required to unlock mobile devices. • Basic integrity and device integrity are required. This means that devices with **unlocked bootloader, rooted, or non-Google certified** will be marked as non-compliant.	**After registration, devices will undergo an evaluation that includes the following criteria:** • Encryption of data storage on devices is required. • A password is required to unlock mobile devices. • Jailbroken devices will be marked as non-compliant

    - Please be aware that if your laptops do not currently have licenses for Windows OS or Microsoft 365 apps, registering them with Microsoft Intune will automatically assign a company license to each registered device.

9. **Can I opt out of the BYOD policy?**

- **Answer:** The BYOD policy is designed to offer flexibility and convenience. If you have concerns or prefer not to use your personal device for work, please discuss alternative arrangements with your manager or HR Division.

10. **How do I register my device with Microsoft Intune?**
    - **Answer:** To register your device, follow the instructions provided by the IT Division. Typically, this involves downloading the Intune Company Portal app, signing in with your work credentials, and following the on-screen prompts to complete the registration process.

11. **What types of devices are eligible for the BYOD policy?**
    - **Answer:** The BYOD policy typically includes smartphones, tablets, and laptops. Specific eligibility criteria will vary for each type of device.

12. **What if my device is not compatible with Microsoft Intune?**
    - **Answer:** If your device is not compatible with Microsoft Intune, you will not be able to register it with the company portal. Please contact the IT Division for assistance. They will help you determine the best course of action, which may include using an alternative device or finding other solutions.

13. **How does Microsoft Intune handle app updates on my device?**
    - **Answer:** Microsoft Intune ensures that work-related apps are regularly updated to the latest versions for security and functionality. It manages updates for these apps without affecting your personal applications.

14. **What should I do if my device is lost or stolen?**
    - **Answer:** If your device is lost or stolen, immediately inform the IT Division by contacting the IT team at your campus. They can remotely wipe company data from your device using Microsoft Intune to prevent unauthorized access to sensitive information.
    - For iOS/Android devices: Please note that we will only remotely wipe company data from your device.
    - For Mac/Windows devices: Please be advised that we have the capability to remotely wipe all data from your devices. However, please note that we will only initiate this action upon your official requests.

15. **What should I do if I change my device or get a new one?**
    - **Answer:** If you change your device or get a new one, you will need to register the new device with Microsoft Intune. Please contact your local IT team for assistance and guidance on transferring your work-related apps and data to your new device.

16. **Will registering my device with Microsoft Intune drain my battery or use a lot of data?**

- **Answer:** Microsoft Intune is designed to have minimal impact on your device's battery life and data usage. It runs efficiently in the background, ensuring that work-related tasks do not interfere significantly with your device's performance.

17. **How does Microsoft Intune handle updates and patches for my device?**
    - **Answer:** Microsoft Intune helps ensure that work-related apps are up to date with the latest security patches. It may prompt you to install updates to maintain compliance with company security standards.
18. **Is there a specific operating system version required for my device to be compatible with Microsoft Intune?**
    - **Answer:** Yes, your device must run a supported operating system version to be compatible with Microsoft Intune. Please refer to the company's BYOD policy or contact the IT department for the specific version requirements.
19. **Will using Microsoft Intune affect my personal app usage or limit any functionalities?**
    - **Answer:** Microsoft Intune will not affect your personal app usage. Only the Windows Hello features (such as fingerprint, PIN, and facial recognition) won't be available after joining VAS BYOD Portal.
20. **Will the company pay for my device if I use it for work?**
    - **Answer:** No. While the company appreciates the use of personal devices for work, the Cybersecurity Improvement Program for BYOD typically does not include reimbursement for the cost of the device.
21. **How will the BYOD security policy affect my existing VPN connection?**
    - Answer: It won't. The VPN app on your device will continue to function normally after you register it on the BYOD portal. However, please note that the VAS network does not allow VPN traffic, so you won't be able to use it while connected to the school network.
22. **What happens if my registered device needs repairs?**
    - **Answer**: Each user can register up to 5 devices (smartphone, tablet, laptop Mac/Windows) on the BYOD Portal. You can register another device to continue your work during the repairs.
23. **Are there any specific guidelines for securing my device at home or in public places?**
    - **Answer:** Yes, we advise always connecting to secure Wi-Fi networks, never leaving your device unattended in public places, and implementing physical security measures such as device locks or using secure cases.
24. **Can I use VAS VPN with my personal device under the BYOD policy?**
    - **Answer:** No,
25. **How do I handle data backup of work-related data on my personal device?**

- **Answer:** You can back up all VAS work-related data into your VAS OneDrive.

26. What are the consequences of non-compliance with the BYOD policy?

- **Answer:** Non-compliance may result in the inability to access Microsoft 365 services; however, the device can still access the internet with limited speed.

27. **Who should I contact for privacy concerns related to BYOD?**

- **Answer:** For any privacy concerns, please reach out to Mr trung.thanh.mai@vas.edu.vn – VAS IT Security Manager or raise the request to ITHelpdesk@vas.edu.vn

28. Is there any training available for securing personal devices used for work purposes?

- **Answer:** Yes, our IT Division offers annual training sessions and resources designed to help you secure your personal device. We will notify you of these sessions and strongly encourage all employees to participate.

29. How can we separate personal and corporate data on employee-owned devices to ensure both privacy and compliance with our organizational security policies?

- **Answer:** After registering your device with the VAS BYOD Portal, all corporate data will be automatically stored in a dedicated, secure space on your smartphone. This ensures a clear separation between personal and organizational information, enhancing both security and privacy. On your laptop, you can easily switch between your personal and company accounts in Microsoft applications.