**DV162\_41\_PAS On BIOS Settings**

**Possible Answers Sheet**

Q1. What key is used to gain access to the BIOS configuration?

Ans: Oftenly its del key, or any function key or combination of some keys.

Q2. How can you access the BIOS using virtualization software?

Ans: We can access the BIOS by using Hyper-V and VMware’s Workstation Players virtualization softwares.

Q3. Is there access to BIOS in VirtualBox?

Ans: There is no access to BIOS using VirtualBox virtualization software.

Q4. How can one access the BIOS if they are using VirtualBox?

Ans: There is no access to BIOS if they are using VirtualBox.

Q5. Is there an option to press a key to start the BIOS in Windows 8, 10, or 11?

Ans: If system boot is set on fast startup mode then there is no option to press a key, but we can still get access to BIOS by holding down shift key when we start clicking restart.

Q6. What versions of Windows might cause a problem when trying to access the BIOS? Ans: Windows 8, Windows 10, and Windows 11

Q7. Why might some versions of Windows cause a problem when trying to access the BIOS?

Ans. That’s because in these versions of Windows, there’s a feature called fast startup that’s turned on by default.

Q8. What happens when you power down our system?

Ans: When we power down our system, it puts our system into a hibernated state where Windows is not completely shut down.

Q9. What are some ways to bypass the fast start-up process?

Ans: Some ways to bypass the fast start-up process are to hold down the Shift key when clicking restart in the Windows desktop, enable and disable this capability from settings, update and security, recovery, advanced startup, and then restart now, or use the system configuration setting for restarting our system under MSconfig.

Q10. Is there a way to bypass the fast start-up process without access to the desktop? Ans: Yes, you can bypass the fast start-up process without access to the desktop by interrupting the normal boot process three times.

Q11. What does Windows do when there is a third interruption?

Ans: Windows disables the fast start-up process and allows access to the normal boot process.

Q12. Why is it important to make a backup of the BIOS settings before making any changes?

Ans: It is important to make a backup of the BIOS settings before making any changes because making changes to the BIOS can cause boot failures or prevent the system from starting at all.

Q12. Is it possible to download a copy of the BIOS configuration?

Ans: Yes, some BIOS implementations allow you to download a copy of the configuration.

Q13. What should be considered when making changes to the BIOS?

Ans: It should be considered that it is easy to make a change that could cause the system to have a problem, so the changes should be fully understood before making them.

Q14. What should you do if you make a change in BIOS and there is a problem?

Ans: If you make a change and there is a problem, you can go back to our BIOS configuration, change the configuration back to the original settings, and restart our system.

Q15. How can you prevent our operating system from having accessed any of our system’s hardware?

Ans: You can disable that hardware in the BIOS, and it will be invisible to the operating system.

Q16. What can you configure on the BIOS?

Ans: You can configure where the BIOS should go to boot our system, and determine which boot devices are available to our system and in which order these boot devices should be checked.

Q17. How can you determine the order of boot devices?

Ans: You can determine the order of boot devices by accessing the primary boot sequence option in the BIOS.

Q18. What is an example of a boot option?

Ans: An example of a boot option is the startup option from a Lenovo UEFI BIOS. This is the startup option. And you can see there is an option for a primary boot sequence. And it will be used when the system is powered up normally. If we click on the primary boot sequence, it brings us to a number of options. And you can see exactly which order the storage drives use.

Q19. What is the order in which the boot up options are enabled and disabled?

Ans: The order is SATA 2, M.2, and then SATA 1.

Q20. What can be done with the BIOS configuration?

Ans: The BIOS configuration can be used to enable or disable certain hardware on the system, such as USB connections.

Q21. What is the potential danger of having USB interfaces?

Ans: The potential danger of having USB interfaces is that someone could gain access to our systems by transferring top-secret information that is stored in very large databases in a matter of seconds and simply walking out the door.

Q22. What did the U.S Department of Defense do in 2008?

Ans: In 2008, the U.S Department of Defense had to disable all of the USB interfaces on their systems and disallow the use of any type of flash media because someone connected a USB drive that was infected with the SillyFDC worm and plugged it into their Department of Defense computer.

Q23. What did the worm do after gaining access to the Department of Defense network?

Ans: The worm was able to move between systems within the Department of Defense network, resulting in a ban of USB-connected storage devices and the disabling of all USB interfaces on the Department of Defense computers.

Q24. How can USB interfaces be disabled in the BIOS?

Ans: USB interfaces can be disabled in the BIOS by finding the devices section of the BIOS and disabling USB access completely, or by modifying which USB interfaces to enable or disable.

Q25. How are the temperatures of computing systems kept cool?

Ans: Computing systems are kept cool by fans inside of the computers, which can be controlled through a number of different BIOS configurations.

Q26. What is a fan controller?

Ans: A fan controller is a device that looks at the temperature inside of our system and either increases or decreases how much airflow may be going through our computer.

Q27. How do you connect to the fan connections on the motherboard?

Ans: You need to connect directly to the fan connections on the motherboard. Those are usually well marked, and you can plug directly in with our existing fans.

Q28. What is a secure boot?

Ans: Secure boot is part of the UEFI specification and uses digital signatures to verify that the boot process has not been modified by a third party.

Q29. What does secure boot do?

Ans: Secure boot can keep malware from making any changes to our system, and if changes are identified, it can stop the boot process and limit the scope of that malware.

Q30. Is secure boot supported with most operating systems?

Ans: Yes, secure boot is supported with most operating systems, including Windows, Linux, and other operating systems.

Q31. What is needed to use secure boot?

Ans: An operating system needs to have a digital signature associated with it that is checked during the startup process, and the public key for the manufacturer of that operating system needs to already be available in the BIOS.

Q32. What does the BIOS contain to prevent unauthorized changes?

Ans: The BIOS contains fail safes to prevent anyone from making changes to the important information regarding secure boot.

Q33. How does secure boot verify that the system has not been modified?

Ans: Secure boot verifies the digital signature associated with the bootloader, with the public key that’s already embedded within the BIOS, and if that verifies, the system has not been modified and it can continue with the boot process.

Q34. How can I enable or disable secure boot?

Ans: You can enable or disable secure boot by modifying the setting in the BIOS.

Q35. What is a supervisor password?

Ans. A supervisor password is a password set in the BIOS that restricts anyone from changing any of the BIOS settings.

Q36. What happens if the supervisor password is forgotten?

Ans. If the supervisor password is forgotten, the BIOS must be reset in order to regain access to the system.

Q37. Where is password information stored?

Ans: Password information is stored in the BIOS configuration, which is on a flash memory connected to the motherboard.

Q38. What was the legacy reference to the BIOS?

Ans: The legacy reference to the BIOS was the Complementary Metal Oxide semiconductor (CMOS).

Q39. How is this done on an Asus motherboard?

Ans: On an Asus motherboard, this is done by using a jumper labeled CLRTC (Clear Real-Time Clock) to short two pins on the motherboard.

Q40. What do we do to reset the BIOS configuration?

Ans: We would push a jumper onto the two pins so that we’ve created a short between both of those pins and power on the system.

Q41. What type of battery is on most modern motherboards?

Ans: It is a 3-volt lithium-ion battery labeled CR 2032.

Q42. What happens if the battery goes bad?

Ans: If the battery goes bad, the date and time on our system will reset back to the original settings when you start our computer.

Q43. Does the motherboard also support additional hardware?

Ans: Yes, the motherboard might also support additional hardware in the form of a Trusted Platform Module or a TPM.

Q44. What can a TPM be used for?

Ans: A TPM can be used for cryptographic functions, creating cryptographic keys, and verifying keys on the system. It can also be used to digitally-sign data and send it to a third party for verification.

Q45. What is a TPM?

Ans: A Trusted Platform Module (TPM) is a secure environment on a computer motherboard that stores sensitive data and is used for authentication purposes.

Q46. Is it possible to hack into the TPM?

Ans: No, it is not possible to hack into the TPM as it is designed to prevent attacks such as brute force from gaining access to the data.

Q47. What is an HSM?

Ans: A Hardware Security Module (HSM) is a standalone device or purpose built appliance that is used to manage cryptographic keys and provide cryptographic functions.

Q48. What are some forms that HSMs can take?

Ans: HSMs can be an adapter card installed into a server, a smart card, or a USB drive.

Q49. What is a benefit of a purpose-built HSM appliance?

Ans: A purpose-built HSM appliance can have cryptographic accelerators built into the hardware, which can increase the overall throughput of applications.