BEZPEČNOSTNÍ NASTAVENÍ BIOS/UEFI

informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené

|  |  |  |
| --- | --- | --- |
| V *místo a datum* | schvaluji |  |
|  | *titul jméno a příjmení* |
|  | *odpovědná osoba / bezpečnostní ředitel* |

Nastavení BIOS / UEFI

Nastavení BIOS / UEFI

* 1. Nastavit silné heslo pro vstup do BIOSu / UEFI volbou „BIOS / UEFI password“ (délka hesla minimálně 12 znaků).
	2. V sekci Security / Secure Boot Configuration nastavit volbu Secure Boot (Secure Boot Enable) na Enabled. Tato volba je podmíněna používáním UEFI, formátem disků GPT a použitím 64-bitové verze operačního systému.

Tato volba také nastaví volbu UEFI / Legacy Boot (Boot Mode) na hodnotu UEFI Only (UEFI) a volbu CSM Support na hodnotu No.

|  |
| --- |
| *uvést, zda byla volba Secure Boot aktivována včetně příslušného snímku obrazovky* |

* 1. V sekvenci Boot Priority Order umístit na první pozici HDD/SDD, který obsahuje systémový oddíl nebo Windows Boot Manager.

|  |
| --- |
| *popsat konkrétní sekvenci, která je použita včetně snímku obrazovky zobrazující použitou bootovací sekvenci* |

* 1. Některé typy UEFI umožňují při startu počítače aktivovat definovanou klávesou (F12) jednorázové Boot Menu (Temporary Startup Device, Boot Option Menu), které umožní provést bootování z externího USB zařízení nezávisle na bootovací sekvenci. Bootování z externího USB zařízení musí být zabezpečeno těmito způsoby v závislosti na schopnosti konkrétního typu UEFI:
		1. V sekci Boot nastavit volbu Boot Device List F12 Option na hodnotu Disabled, která deaktivuje spuštění jednorázového Boot Menu nebo
		2. V sekci Boot nastavit volbu USB Boot (Enable USB Boot Support) na hodnotu Disabled, která znemožní bootovat z externího USB zařízení.
		3. V případě, že IS obsahuje čtečku paměťových karet (Secure Digital SD) je nutné deaktivovat možnost bootování z paměťových karet nastavením volby Secure Digital SD Card Boot na Disabled.

|  |
| --- |
| *uvést způsob zabezpečení proti bootování z externích USB disků a paměťových karet, jestliže to UEFI umožňuje včetně příslušných snímků obrazovky* |

* 1. Nastavení zakázání nepotřebných komunikačních portů (USB, ThunderBolt, FireWire, BlueTooth, eSata, čtečka paměťových karet Secure Digital SD a další).

|  |
| --- |
| *popsat konkrétní nastavení výše uvedených komunikačních portů a vložit snímek zobrazující konkrétní nastavení výše uvedených komunikačních portů* |

* 1. Deaktivace modulu bezdrátové sítě Wireless LAN a Bluetooth.

|  |
| --- |
| *popsat deaktivaci modulu bezdrátové sítě Wireless LAN a Bluetooth a vložit snímek zobrazující deaktivaci uvedených modulů. Jestliže počítač (notebook) neobsahuje uvedené moduly, uvede se, že uvedené moduly nejsou součástí informačního systému* |

Nastavení zákazu přístupu k bezdrátovým sítím Wireless LAN

* 1. Zakázání funkčnosti WLAN modulu v BIOS: Nastavení k výstupním portům LAN, USB, FireWire, Modem jsou zpravidla v sekci ADVANCED. V současné době nejsou tato nastavení u některých notebooků v BIOS dostupná a tato zařízení / porty nejsou na úrovni BIOS řiditelná.
	2. Mechanické vypnutí WLAN modulu: Provádí se přepnutím přepínače nebo funkční klávesou a je indikováno nápisem WLAN Enabled /Disabled po dobu několika sekund a dále rozsvícením / zhasnutím indikátoru – diody WLAN.

|  |
| --- |
| *uvést jakým způsobem je zákaz přístupu k bezdrátovým sítím WLAN realizován spolu s příslušným snímkem obrazovky. V případě, že počítač (notebook) neobsahuje modul WLAN, uvede se konstatování, že modul WLAN není součástí informačního systému* |

Nastavení zákazu přístupu k zařízení typu Bluetooth

* 1. Zakázání funkčnosti Bluetooth modulu v BIOS: Nastavení zařízení typu Bluetooth jsou zpravidla v sekci ADVANCED. V současné době nejsou tato nastavení u některých notebooků v BIOS dostupná a tato zařízení nejsou na úrovni BIOS řiditelná.
	2. Mechanické vypnutí Bluetooth modulu: Provádí se přepnutím přepínače nebo funkční klávesou a je indikováno nápisem Bluetooth Enabled /Disabled po dobu několika sekund a dále rozsvícením / zhasnutím indikátoru – diody Bleutooth.

|  |
| --- |
| *uvést jakým způsobem je zákaz přístupu k bezdrátové síti BlueTooth realizován spolu s příslušným snímkem obrazovky. V případě, že počítač (notebook) neobsahuje modul BlueTooth, uvede se konstatování, že modul BlueTooth není součástí informačního systému* |