Bezpečnostní dokumentace

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

(verze 1.1)

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

Obsah

[BEZPEČNOSTNÍ POLITIKA 8](#_Toc187310816)

[Úvod 8](#_Toc187310817)

[Úvodní ustanovení 8](#_Toc187310818)

[Vymezení pojmů 8](#_Toc187310819)

[Bezpečnostní cíle 9](#_Toc187310820)

[Předpoklady 9](#_Toc187310821)

[Oblast personální bezpečnosti 9](#_Toc187310822)

[Obecné požadavky 9](#_Toc187310823)

[Role v informačním systému 10](#_Toc187310824)

[Bezpečnostní správa 10](#_Toc187310825)

[Provozní správa 10](#_Toc187310826)

[Oblast informační bezpečnosti 10](#_Toc187310827)

[Nastavení parametrů BIOS/UEFI 10](#_Toc187310828)

[Minimální požadavky počítačové bezpečnosti 11](#_Toc187310829)

[Tvorba přístupových hesel 11](#_Toc187310830)

[Archivace auditních záznamů 12](#_Toc187310831)

[Bezpečnost V/V portů 12](#_Toc187310832)

[Bezpečné mazání informací 12](#_Toc187310833)

[Antivirová ochrana a aktualizace virových řetězců 12](#_Toc187310834)

[Instalace a používání HW a SW 13](#_Toc187310835)

[Oblast fyzické bezpečnosti 13](#_Toc187310836)

[Obecné požadavky 13](#_Toc187310837)

[Podmínky pro provozování pracoviště 13](#_Toc187310838)

[Přeprava a ukládání nosičů utajovaných informací 13](#_Toc187310839)

[Režimová opatření 14](#_Toc187310840)

[Způsob evidence HW komponent 14](#_Toc187310841)

[Ochranné prvky 14](#_Toc187310842)

[Kompromitující vyzařování 15](#_Toc187310843)

[Oblast administrativní bezpečnosti 15](#_Toc187310844)

[Obecné požadavky 15](#_Toc187310845)

[Evidence a označování nosičů informací 15](#_Toc187310846)

[Likvidace nosičů utajovaných informací 16](#_Toc187310847)

[Provozně bezpečnostní dokumentace 17](#_Toc187310848)

[Požadavky bezpečného provozu 17](#_Toc187310849)

[Údržba a opravy 17](#_Toc187310850)

[Krizové situace a bezpečnostní incidenty 17](#_Toc187310851)

[Dostupnost 18](#_Toc187310852)

[Test bezpečnosti 18](#_Toc187310853)

[Kontrolní činnost 19](#_Toc187310854)

[VÝSLEDKY ANALÝZY RIZIK 20](#_Toc187310855)

[Úvodní ustanovení 20](#_Toc187310856)

[Personální bezpečnost a organizačních opatření 20](#_Toc187310857)

[Fyzická bezpečnost 21](#_Toc187310858)

[Informační bezpečnost část obecné požadavky 21](#_Toc187310859)

[Informační bezpečnost část operační systém 21](#_Toc187310860)

[Informační bezpečnost část komunikační 24](#_Toc187310861)

[Informační bezpečnost část aplikační 24](#_Toc187310862)

[Informační bezpečnost část kompromitující vyzařování 25](#_Toc187310863)

[POPIS BEZPEČNOSTI 26](#_Toc187310864)

[Úvod 26](#_Toc187310865)

[Úvodní ustanovení 26](#_Toc187310866)

[Druh a rozsah zpracovávaných utajovaných informací 26](#_Toc187310867)

[Určení a rozsah informačního systému 26](#_Toc187310868)

[Podmínky provozování 27](#_Toc187310869)

[Personální bezpečnost 27](#_Toc187310870)

[Obecné požadavky 27](#_Toc187310871)

[Informační bezpečnost 28](#_Toc187310872)

[Nastavení parametrů BIOS/UEFI 28](#_Toc187310873)

[Bezpečnostní nastavení operačního systému 28](#_Toc187310874)

[Přístupová hesla 29](#_Toc187310875)

[Auditní záznamy 29](#_Toc187310876)

[Bezpečnost V/V portů 29](#_Toc187310877)

[Bezpečné mazání 29](#_Toc187310878)

[Antivirová ochrana a aktualizace virových řetězců 30](#_Toc187310879)

[Instalace a používání HW a SW 30](#_Toc187310880)

[Požadavky na dostupnost 30](#_Toc187310881)

[Fyzická bezpečnost 30](#_Toc187310882)

[Obecné požadavky 30](#_Toc187310883)

[Podmínky pro provozování pracoviště 30](#_Toc187310884)

[Přeprava a ukládání nosičů utajovaných informací 31](#_Toc187310885)

[Režimová opatření 31](#_Toc187310886)

[Způsob evidence HW komponent 31](#_Toc187310887)

[Ochranné prvky 31](#_Toc187310888)

[Kompromitující vyzařování 32](#_Toc187310889)

[Administrativní bezpečnost 32](#_Toc187310890)

[Obecné požadavky 32](#_Toc187310891)

[Evidence a označování nosičů informací 33](#_Toc187310892)

[Likvidace nosičů utajovaných informací 34](#_Toc187310893)

[Provozně bezpečnostní dokumentace 34](#_Toc187310894)

[Požadavky bezpečného provozu 35](#_Toc187310895)

[Údržba a opravy 35](#_Toc187310896)

[Krizové situace a bezpečnostní incidenty 35](#_Toc187310897)

[Změny při provozování pracoviště 36](#_Toc187310898)

[Testy bezpečnosti 36](#_Toc187310899)

[Kontrolní činnost 37](#_Toc187310900)

[Příloha: Vzory administrativních pomůcek 38](#_Toc187310901)

[Seznam vzorů 38](#_Toc187310902)

[Vzor č. 1: pověření k činnosti 39](#_Toc187310903)

[Vzor č. 2: ukončení pověření k činnosti 40](#_Toc187310904)

[Vzor č. 3: školení uživatelů 41](#_Toc187310905)

[Vzor č. 4: evidence uživatelů 42](#_Toc187310906)

[Vzor č. 5: evidence nosičů informací 44](#_Toc187310907)

[Vzor č. 6: evidence příjmu a výdeje nosičů informací 46](#_Toc187310908)

[Vzor č. 7: provozní deník pracoviště 48](#_Toc187310909)

[Vzor č. 8: specifikační list pracoviště 50](#_Toc187310910)

[Vzor č. 9: test bezpečnosti 52](#_Toc187310911)

[BEZPEČNOSTNÍ NASTAVENÍ OPERAČNÍHO SYSTÉMU MS WINDOWS 54](#_Toc187310912)

[Úvod 54](#_Toc187310913)

[Vysvětlivky k použitým označením 54](#_Toc187310914)

[Část první 55](#_Toc187310915)

[Všeobecná nastavení OS MS Windows 55](#_Toc187310916)

[Automatizované nastavení zabezpečení 55](#_Toc187310917)

[Příprava pevného disku 55](#_Toc187310918)

[Instalace operačního systému 55](#_Toc187310919)

[Nastavení antivirového programu 55](#_Toc187310920)

[Použití technologie ReadyBoost 55](#_Toc187310921)

[Nastavení zákazu přístupu k bezdrátovým sítím Wireless LAN 55](#_Toc187310922)

[Nastavení zákazu přístupu k zařízení typu Bluetooth 56](#_Toc187310923)

[Nastavení systémových služeb 56](#_Toc187310924)

[Nastavení přístupových práv k souborům a adresářům 57](#_Toc187310925)

[Nastavení uživatelských účtů a skupin uživatelů 57](#_Toc187310926)

[Tiskárny 57](#_Toc187310927)

[Odinstalování nepotřebných aplikací (doporučení k zpřehlednění systému) 57](#_Toc187310928)

[Část druhá 58](#_Toc187310929)

[Zásady účtů 58](#_Toc187310930)

[Zásady hesla 58](#_Toc187310931)

[Zásady uzamčení účtů 59](#_Toc187310932)

[Část třetí 59](#_Toc187310933)

[Místní zásady 59](#_Toc187310934)

[Zásady auditu 59](#_Toc187310935)

[Přiřazení uživatelských práv 61](#_Toc187310936)

[Možnosti zabezpečení 62](#_Toc187310937)

[Část čtvrtá 68](#_Toc187310938)

[Služba protokolu událostí 68](#_Toc187310939)

[Místní počítač – zásady / Konfigurace počítače / Šablony pro správu / 68](#_Toc187310940)

[Součásti systému Windows / Služba protokolu událostí 68](#_Toc187310941)

[Část pátá 70](#_Toc187310942)

[Šablony pro správu – konfigurace počítače 70](#_Toc187310943)

[Součásti systému Windows / Možnost přihlášení k systému Windows 70](#_Toc187310944)

[Windows Components / Windows Logon Options 70](#_Toc187310945)

[Součásti systému Windows / OneDrive 71](#_Toc187310946)

[Windows Components / OneDrive 71](#_Toc187310947)

[Součásti systému Windows / Uživatelské rozhraní pověření 71](#_Toc187310948)

[Windows Components / Credential User Interface 71](#_Toc187310949)

[Součásti systému Windows / Zásady automatického přehrávání 71](#_Toc187310950)

[Windows Components / Autoplay Policies 71](#_Toc187310951)

[Systém / Přihlášení 72](#_Toc187310952)

[System / Logon 72](#_Toc187310953)

[Systém / Zásady skupiny 72](#_Toc187310954)

[System / Group Policy 72](#_Toc187310955)

[Systém / Instalace zařízení / Omezení pro instalaci zařízení 73](#_Toc187310956)

[System / Device Installation / Device Installation Restrictions 73](#_Toc187310957)

[Systém / Přístup k vyměnitelnému úložišti 74](#_Toc187310958)

[System / Removable Storage Access 74](#_Toc187310959)

[Ruční nastavení restrikcí pro USB zařízení typu Mass Storage 76](#_Toc187310960)

[Automatické nastavení restrikcí pro USB zařízení typu Mass Storage 77](#_Toc187310961)

[Systém / Obnovení 77](#_Toc187310962)

[System / Recovery 77](#_Toc187310963)

[Systém / Obnovení systému 77](#_Toc187310964)

[System / System Restore 77](#_Toc187310965)

[Ovládací panely / Přizpůsobení 78](#_Toc187310966)

[Control Panel / Personalization 78](#_Toc187310967)

[Část šestá 78](#_Toc187310968)

[Šablony pro správu – konfigurace uživatele 78](#_Toc187310969)

[Ovládací panely / Přizpůsobení 78](#_Toc187310970)

[Control Panel / Personalization 78](#_Toc187310971)

[Součásti systému Windows / Průzkumník Windows / 79](#_Toc187310972)

[Windows Components / File Explorer 79](#_Toc187310973)

[Část sedmá 79](#_Toc187310974)

[Aktivace OS Windows 10 bez připojení k Internetu 79](#_Toc187310975)

[Postup aktivace 79](#_Toc187310976)

[Část osmá 80](#_Toc187310977)

[Aktualizace OS Windows 10 bez připojení k Internetu 80](#_Toc187310978)

[Příprava aktualizačního média 80](#_Toc187310979)

[Vlastní aktualizace OS Windows 10 pomocí DVD 81](#_Toc187310980)

[Vlastní aktualizace OS Windows 10 pomocí USB flash disku 81](#_Toc187310981)

[SMĚRNICE BEZPEČNOSTNÍHO SPRÁVCE 82](#_Toc187310982)

[Úvodní ustanovení 82](#_Toc187310983)

[Povinnosti bezpečnostního správce 82](#_Toc187310984)

[SMĚRNICE PROVOZNÍHO SPRÁVCE 84](#_Toc187310985)

[Úvodní ustanovení 84](#_Toc187310986)

[Povinnosti provozního správce 84](#_Toc187310987)

[SMĚRNICE UŽIVATELE 85](#_Toc187310988)

[Úvodní ustanovení 85](#_Toc187310989)

[Povinnosti uživatele 85](#_Toc187310990)

[Zakázané činnosti uživatele 86](#_Toc187310991)

[Přístupové heslo 86](#_Toc187310992)

[Krizové situace a bezpečnostní incidenty 86](#_Toc187310993)

[Ukládání a manipulace s vyjímatelnými nosiči utajovaných informací nebo s přenosným PC 87](#_Toc187310994)

BEZPEČNOSTNÍ POLITIKA

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

Úvod

1.

Úvodní ustanovení

* + 1. Bezpečnostní politika informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen „Bezpečnostní politika“) je základní kapitolou bezpečnostní dokumentace informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen “Informační systém“).
		2. Bezpečnostní politika je tvořena souborem norem, pravidel a postupů vymezující způsob zajištění důvěrnosti, integrity a dostupnosti utajovaných informací, dostupnosti služeb informačního systému a odpovědnosti pracovníků v jednotlivých rolích.
		3. Bezpečnostní politika deklaruje zajištění plnění úkolů vyplývajících zejména ze zákona[[1]](#footnote-1)) a vyhlášky[[2]](#footnote-2)) při zpracování utajovaných informací v informačním systému.
1.

Vymezení pojmů

* + 1. Pro účely tohoto dokumentu se rozumí:

pracovištěm informačního systému jeden samostatný stacionární případně přenosný počítač, jeho programové vybavení, k tomu patřící periferní zařízení nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací, který je umístěn v ohraničeném prostoru a není propojen s jiným informačním případně komunikačním systémem (dále jen „pracoviště“),

informačním systémem jedno nebo několik samostatných vzájemně nepropojených pracovišť,

rolí souhrn určených činností a potřebných autorizací pro pracovníka působícího v informačním systému. Rozeznáváme tři základní role: uživatel informačního systému (dále jen „uživatel“), bezpečnostní správce informačního systému (dále jen „bezpečnostní správce“) a provozní správce informačního systému (dále jen „provozní správce“),

provozovatelem orgán státu[[3]](#footnote-3)), právnická osoba nebo podnikající fyzická osoba, která je držitelem certifikátu informačního systému.

1.

Bezpečnostní cíle

* + 1. Informační systém bude vytvářet podmínky pro bezpečné zpracovávání utajovaných informací při zajištění jejich důvěrnosti, integrity a dostupnosti.
		2. Pro zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací a služeb informačního systému budou použity bezpečností mechanizmy nevyžadující neúměrně komplikovanou obsluhu, která by neúměrně zatěžovala uživatele dodatečnými činnostmi nad rámec nutných úkonů při obsluze informačního systému.
		3. Bezpečnostní mechanismy budou zajišťovat odpovědnost uživatelů a dalších osob za jejich činnost v informačním systému.
		4. Ochrana utajovaných informací bude zajišťována v souladu s platnými právními předpisy a interními akty řízení upravujícími ochranu utajovaných informací.
1.

Předpoklady

* + 1. Informační systém bude možné provozovat pouze za předpokladu, že byl řádně certifikován Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) a schválen do provozu odpovědnou osobou nebo jí pověřenou osobou.
		2. Pro zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací a služeb informačního systému budou použita protiopatření navržená v kapitole „Výsledky analýzy rizik informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen „Výsledky analýzy rizik“).

Oblast personální bezpečnosti

1.

Obecné požadavky

* + 1. Uživatelem rozumíme fyzickou osobu, která v rozsahu svého pověření vykonává definované činnosti v informačním systému. Podle rozsahu oprávnění rozeznáváme uživatele koncové a privilegované.
		2. Pracovníkem správy informačního systému (dále jen „pracovník správy“) rozumíme bezpečnostního nebo provozního správce, kde:

bezpečnostní správce je privilegovaný uživatel informačního systému v roli vytvořené pro řízení, kontrolu a provádění stanovených činností k zajištění bezpečnosti informačního systému,

provozní správce je privilegovaný uživatel informačního systému v roli vytvořené pro zajištění provozu a požadované funkčnosti informačního systému.

* + 1. Pověření pracovníka do role privilegovaného uživatele informačního systému (pracovníka správy) slouží zároveň jako pověření do role koncového uživatele, pokud není v bezpečnostní dokumentaci informačního systému stanoveno jinak.
		2. Všichni uživatelé informačního systému budou:

oprávněni k přístupu k utajované informaci minimálně pro stupeň utajení Vyhrazené, pokud není stanoveno jinak,

písemně pověřeni do příslušné role v informačním systému,

evidováni ve stanovených pomůckách,

proškoleni v souladu s vyhláškou[[4]](#footnote-4)) a bezpečnostní dokumentací informačního systému.

1.

Role v informačním systému

* + 1. Pro činnost informačního systému budou definovány a personálně obsazeny následující role:

bezpečnostní správce,

provozní správce,

uživatel.

* + 1. Roli bezpečnostního a provozního správce lze sloučit.
		2. Pro každou definovanou roli v informačním systému bude vypracována „Bezpečnostní směrnice“, kde budou přesně definované povinnosti dané role.
1.

Bezpečnostní správa

* + 1. Bezpečnostní správou informačního systému rozumíme výkon role bezpečnostního správce.
		2. Bezpečnostní správce bude zejména zajišťovat a provádět:

bezpečnostní správu,

pravidelná roční školení uživatelů.

1.

Provozní správa

* + 1. Provozní správou informačního systému rozumíme výkon role provozního správce.
		2. Provozní správce bude zejména zajišťovat a provádět provozní správu.

Oblast informační bezpečnosti

Nastavení parametrů BIOS/UEFI

* + 1. Nastavení parametrů BIOS/UEFI bude provedeno podle doporučení NÚKIB
		2. Přístup k BIOS/UEFI bude umožněn pouze po zadání hesla, jehož délka je minimálně 12 znaků.
		3. Bootování bude povoleno pouze z HDD/SSD, který obsahuje systémový oddíl nebo Windows Boot Manager.
		4. V případě UEFI bude deaktivována možnost spuštění jednorázového Boot Menu (volba Boot Device List).
		5. Možnost bootování z ostatních zařízení (LAN, USB, Secure Digital SD apod.) bude zakázána.
		6. Nepotřebné komunikační a bezdrátové rozhraní (eSata, ThunderBolt, FireWire, Wireless, Bluetooth apod.) budou zakázány.
1.

Minimální požadavky počítačové bezpečnosti

* + 1. Nastavením a prostředky použitého operačního systému bude v informačním systému zajištěna:

jednoznačná identifikace a autentizace,

volitelné řízení přístupu,

vytváření auditních záznamů,

ošetření paměťových objektů před jejich dalším použitím.

* + 1. Použití operačních systémů, které nejsou schopny zajistit výše zmíněná nastavení je v informačním systému zakázáno.
		2. Pro informační systém budou stanoveny i další požadavky počítačové bezpečnosti, kterými jsou zejména:

tvorba přístupových hesel,

archivace auditních záznamů,

bezpečnost V/V portů,

bezpečné mazání informací,

antivirová ochrana a aktualizace virových řetězců,

instalace a používání HW a SW.

1.

Tvorba přístupových hesel

* + 1. Přístupové heslo k účtu informačního systému musí být chráněno jako utajovaná informace stupně utajení Vyhrazené.
		2. Politika hesel použitá v informačním systému bude vycházet z kapitoly „Výsledky analýzy rizik“ a bude definována v kapitole „Popis bezpečnosti informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen „Popis bezpečnosti“).
		3. Přístupové heslo k účtu uživatele nebo pracovníka správy nebude:

obsahovat přihlašovací jméno (login) ani ve změněné formě,

odvozeno ze jmen příbuzných nebo známých,

odvozeno z žádné informace, která má vztah k uživateli (číslo vozu, telefonní číslo, osobní číslo, značka auta, jméno ulice atd.),

použito v jiném informačním systému,

sdíleno s jiným uživatelem systému.

* + 1. Přístupové heslo k BIOSu, pevným účtům nebo ke službám operačního systému informačního systému bude chráněno jako utajovaná informace stupně utajení Vyhrazené a po dobu platnosti budou uložena v zabezpečené obálce.
1.

Archivace auditních záznamů

* + 1. Vytváření auditních záznamů bude zajišťováno funkcionalitou a nastavením použitého operačního systému případně i aplikačního software.
		2. Bezpečnostní správce bude provádět kontrolu a archivaci auditních záznamů podle pravidel popsaných v kapitole „Popis bezpečnosti“ a vycházejících z kapitoly „Výsledky analýzy rizik“.
		3. Auditní záznamy budou archivovány po dobu minimálně pěti let.
		4. Auditní záznamy nebudou klasifikovány jako utajované informace, pokud nebude stanoveno jinak, ale zacházet se s nimi bude jako s citlivými informacemi.
1.

Bezpečnost V/V portů

* + 1. Používání vstupně výstupních portů na pracovištích bude řízeno pomocí speciálních postupů nebo aplikací schválených NÚKIB (SW nebo HW technické prostředky).
		2. Řízení vstupně výstupních portů bude zajišťovat, že v informačním systému mohou být používána pouze schválená vstupně výstupní zařízení.
		3. Způsob řízení vstupně výstupních portů bude popsán v kapitole „Popis bezpečnosti“.
1.

Bezpečné mazání informací

* + 1. Ošetření opakovaného použití paměťových objektů bude zajištěno prostředky a nastavením použitého operačního systému.
		2. Požadavky na bezpečné mazání nosičů informací budou popsány v kapitole „Popis bezpečnosti“.
		3. Bezpečné mazání bude zajišťovat a provádět bezpečnostní správce.
		4. Snižování nebo rušení stupně utajení nosičů informací bude zakázáno.
1.

Antivirová ochrana a aktualizace virových řetězců

* + 1. V informačním systému bude použit SW antivirové ochrany, jehož aktualizaci bude provádět příslušný pracovník správy.
		2. Četnost provádění aktualizace virových řetězců bude definována v kapitole „Popis bezpečnosti“.
1.

Instalace a používání HW a SW

* + 1. Veškerý HW a SW použitý v informačním systému bude podléhat schválení NÚKIB.
		2. Pro každé pracoviště povede bezpečnostní správce evidenci použitého HW a SW.

Oblast fyzické bezpečnosti

1.

Obecné požadavky

* + 1. Fyzická bezpečnost pracovišť bude zajišťována zejména aplikovanými opatřeními v souladu s právními předpisy a interními akty řízení upravujícími ochranu utajovaných informací.
1.

Podmínky pro provozování pracoviště

* + 1. Obrazovka monitoru nebo konzole, klávesnice a tiskárny budou umístěny tak, aby bylo neoprávněné osobě zamezeno odezírání zpracovávané utajované informace.
		2. Při zpracovávání utajované informace typu audio záznamu, bude zajištěno, že nedojde k porušení povinnosti při ochraně utajované informace cestou akustického přeslechu.
		3. Pracoviště, jehož součástí bude alespoň jeden nevyjímatelný nosič informací, který nepotřebuje pro uchování informace trvalé připojení k elektrické energii, bude umístěno minimálně v příslušné zabezpečené oblasti kategorie Vyhrazené, třídy II.
		4. Pracoviště, jehož součástí budou pouze vyjímatelné nosiče informací, které nepotřebují pro uchování informace trvalé připojení k elektrické energii, bude umístěno minimálně v příslušném objektu kategorie Vyhrazené.
		5. Pracoviště s přenosným počítačem může být provozováno minimálně v objektu kategorie Vyhrazené, ale přenosný počítač musí být ukládán v příslušném úschovném objektu v zabezpečené oblasti minimálně kategorie Vyhrazené, třídy II.
1.

Přeprava a ukládání nosičů utajovaných informací

* + 1. Nosiče utajovaných informací budou přepravovány v aktovce, kufříku, kufru, přenosné bezpečnostní schránce nebo v kurýrním vaku, který je způsobilý k přepravě utajovaných dokumentů (dále jen „přenosná schránka“).
		2. Přenosná schránka bude zajišťována proti neoprávněné manipulaci s jejím obsahem např. uzamčením mechanickým zámkem, pečetěním apod. Přenosná schránka bude opatřena na vhodném místě názvem a adresou provozovatele informačního systému provozuje a nápisem: „V případě nálezu neotvírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!“.
		3. Přenosné počítače a vyjímatelné nosiče utajovaných informací se budou ukládat v zabezpečené oblasti minimálně kategorie Vyhrazené v příslušném úschovném objektu typu 1 nebo 1A.
1.

Režimová opatření

* + 1. Pro každé pracoviště budou stanovena režimová opatření v souladu s platným projektem fyzické bezpečnosti.
		2. Režimová opatření pracoviště budou upravovat zejména: umístění pracoviště, režim vstupu osob, manipulaci s klíči, manipulaci s HW komponentami pracoviště a výdej a příjem přenosných počítačů a vyjímatelných nosičů informací (především HDD/SSD).
		3. Dodržování stanovených režimových opatření bude kontrolovat bezpečnostní správce.
1.

Způsob evidence HW komponent

* + 1. Každá HW komponenta bude evidována bezpečnostním správcem.
		2. Evidované HW komponenty pracoviště budou zejména: základní jednotka (počítač, notebook), monitor, myš, klávesnice, HDD/SSD, tiskárna a scanner.
		3. Základní jednotka (počítač, notebook) bude na viditelném místě označena štítkem obsahujícím údaje o maximálním stupni utajení zpracovávaných utajovaných informací a názvem provozovatele informačního systému.
		4. Příklad štítku pro označení základní jednotky:

IS pro zpracování utajovaných informací:

VYHRAZENÉ

*Otisk razítka nebo název provozovatele*

1.

Ochranné prvky

* + 1. HW komponenty pracoviště obsahující alespoň jeden nevyjímatelný nosič informací, který nepotřebuje pro uchování informace trvalé připojení k elektrické energii, budou opatřeny ochrannými prvky.
		2. Ochranný prvek musí být číslovaný a obsahovat reziduální vrstvu, která zajistí znehodnocení ochranného prvku při pokusu o jeho sejmutí (odstranění z HW komponenty).
		3. Ochranné prvky budou na HW komponentě umístěny tak, aby při pokusu o vniknutí do HW komponenty došlo k jejich poškození a zároveň tak, aby byla možná jejich snadná vizuální kontrola uživatelem.
		4. Neporušenost ochranných prvků bude kontrolovat bezpečnostní správce minimálně jednou měsíčně nebo v případě nevyužívání informačního systému po delší časové období, vždy před započetím zpracování utajovaných informací.
		5. Uživatelé budou kontrolovat neporušenost ochranných prvků vždy před zahájením své práce.
		6. Porušení ochranného prvku bude považováno za bezpečnostní incident.
1.

Kompromitující vyzařování

* + 1. V informačním systému budou použita pouze HW zařízení, která musí splňovat požadavky na elektrickou bezpečnost a elektromagnetickou kompatibilitu (EMC) podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů ve znění pozdějších předpisů (dále jen „zákon č. 22/1997 Sb.“).

Oblast administrativní bezpečnosti

1.

Obecné požadavky

* + 1. Všechny utajované informace exportované z informačního systému budou označeny odpovídajícím stupněm utajení a bude s nimi nakládáno v souladu s právními předpisy a interními akty řízení upravujícími ochranu utajovaných informací.
1.

Evidence a označování nosičů informací

* + 1. Všechny nosiče informací používané v informačním systému budou evidované. Evidenci povede určený zaměstnanec provozovatele informačního systému nebo bezpečnostní správce.
		2. Nosiče informací, které budou sloužit jako pomůcka uživatele k ukládání utajovaných informací (záloha uživatelských dat apod., dále jen „provozní nosiče utajovaných informací“) a všechny HDD/SSD používané v informačním systému budou označeny a evidovány podle vyhlášky č. 479/2024 Sb., o informační bezpečnosti (štítek na kterém bude uvedeno zejména: název organizace, evidenční číslo a stupeň utajení). Příklad štítku utajovaného nosiče:

Provozovatel: ………………………..

…………………………………………

stupeň utajení: **V Y H R A Z E N É**

Ev.č.: …………………………………...

* + 1. V evidenci provozních nosičů zejména pak HDD/SSD disků budou uvedeny jejich výrobní čísla, tak aby byla zajištěna jejich jednoznačná identifikace.
		2. Nosiče informací, které budou určeny pro export utajovaných informací mimo organizaci, budou označeny a evidovány podle vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů (štítek na kterém bude uvedeno zejména: název organizace, číslo jednací nebo příloha k č. j. a stupeň utajení).
		3. Nosiče informací, které budou sloužit jako pomůcka uživatele pro neutajované informace (vkládání aktualizací virových řetězců, záloha auditních záznamů apod., dále jen „provozní nosiče“) budou opatřeny štítkem, na kterém bude uvedeno zejména: název organizace a evidenční číslo. Příklad štítku neutajovaného nosiče:

Provozovatel: ………………………..

…………………………………………

Ev.č.: ……………………….…….…...

* + 1. Evidenční číslo provozního nosiče obsahuje položky uvedené v § 42 odst. 4 písm. c) vyhlášky č. 479/2024 Sb., o informační bezpečnosti (zkratka stupně utajení, je-li nosič informací utajovaný, nebo zkratka informace o tom, že nosič informací je neutajovaný, pořadové číslo, rok zavedení do evidence a identifikaci provozovatele informačního systému).

Likvidace nosičů utajovaných informací

* + 1. S provozními nosiči utajovaných informací se bude nakládat jako s utajovanou informací až do doby jejich fyzického zničení.
		2. Likvidace provozních nosičů bude prováděna v souladu s platnou legislativou (vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a o certifikaci technických prostředků, ve znění pozdějších předpisů).
		3. Likvidace provozních nosičů utajovaných informací bude provádět příslušný zaměstnanec pověřený vedením jejich evidencí na certifikovaném zařízení fyzického ničení nosičů informací za přítomnosti dalšího zaměstnance (obvykle uživatele nosiče).
		4. O likvidaci provozního nosiče utajovaných informací bude proveden záznam v „Evidenci nosičů“. Záznam o zničení provozního nosiče bude podepsaný zaměstnanci, kteří likvidaci provedli.
		5. Pokud provozovatel informačního systému není schopen provést likvidaci provozního nosiče utajovaných informací, v souladu s požadavky platné legislativy, požádá NÚKIB o spolupráci (předá nosiče na NÚKIB, který zajistí jejich likvidaci).
1.

Provozně bezpečnostní dokumentace

* + 1. Všechny písemnosti týkající se bezpečnosti a provozu informačního systému se budou uchovávat minimálně po dobu 5 let od doby ukončení jejich používání.
		2. Bezpečnostní požadavky a opatření použitá v informačním systému budou popsány v kapitolách:

Výsledky analýzy rizik,

Popis bezpečnosti,

Testy bezpečnosti,

Bezpečnostní směrnice (pro každou definovanou roli),

další provozně bezpečnostní dokumentaci stanovené v kapitole
 „Popis bezpečnosti“.

Požadavky bezpečného provozu

1.

Údržba a opravy

* + 1. Údržba a opravy (dále jen „servis“) se bude provádět tak, aby nedošlo k porušení povinnosti při ochraně utajované informace.
		2. Servis zajišťuje provozní správce, pokud možno vlastními silami a v objektu minimálně kategorie Vyhrazené. V případě nutnosti je servisní úkon prováděn externím subjektem pod dohledem pracovníka správy.
		3. Pokud nelze provést servisní úkon vlastními silami a v objektu minimálně kategorie Vyhrazené, musí být ze zařízení odstraněny ochranné prvky a vyjmuty všechny nosiče informací, které pro zachování uložených informací nepotřebují trvalé napájení.
		4. Při servisu lze použít pouze takové náhradní komponenty, které splňují požadavky zákona č. 22/1997 Sb., a musí být pro tyto komponenty vydáno „Prohlášení o shodě“, „ES Prohlášení o shodě“ nebo označeny symbolem CE (CE Mark).
		5. O úkonech provedených v rámci servisu, musí pracovník správy provést záznam do příslušné provozní dokumentace.
1.

Krizové situace a bezpečnostní incidenty

* + 1. Za **krizovou situaci** v informačním systému bude považována porucha zařízení, požár nebo jiná živelní pohroma, teroristický útok nebo jeho hrozba.
		2. **Bezpečnostní incident** je událost, která má nebo může mít za následek ohrožení bezpečnosti informačního systému nebo porušení povinnosti při ochraně utajované informace.
		3. Za bezpečnostní incident bude považováno zejména:

porušení některého z bezpečnostních mechanismů,

porušení ochranných prvků,

ztráta nosiče utajovaných informací,

ztráta HW komponenty opatřené ochranným prvkem,

neoprávněné nakládání s nosičem utajovaných informací,

vyzrazení přístupového hesla,

porušení platných bezpečnostních směrnic,

další události, které mohou mít vliv na bezpečnost zpracovávaných utajovaných informací.

* + 1. Chování a povinnosti uživatelů a postup řešení krizových situací a bezpečnostních incidentů bude popsán v kapitole „Popis bezpečnosti“.
		2. O krizové situace nebo bezpečnostním incidentu musí bát informován bezpečnostní ředitel, který zajistí spolu s bezpečnostním správcem jeho prošetření.
		3. O krizové situaci nebo bezpečnostním incidentu, u kterého je výsledkem šetření potvrzeno porušení povinnosti při ochraně utajované informace, bude bezodkladně informován Národní bezpečnostní úřad.
		4. O průběhu šetření bezpečnostního incidentu a o výsledcích šetření bude zpracován písemný záznam, který se bude ukládat na dobu 5 let.
		5. O výskytu krizové situace nebo bezpečnostního incidentu provede uživatel a příslušný pracovník správy záznam do příslušné provozní dokumentace.
1.

Dostupnost

* + 1. Požadavky na dostupnost včetně plánu na obnovení činnosti informačního systému budou stanoveny a rozpracovány v bezpečnostní dokumentaci informačního systému.
1.

Test bezpečnosti

* + 1. U každého pracoviště bude před zahájením provozu provozovatelem prokazatelně proveden test bezpečnosti.
		2. Test bezpečnosti bude zaměřen na zjištění stavu bezpečnosti pracoviště podle bezpečností dokumentace z oblastí:

personální bezpečnosti a organizačních opatření,

administrativní bezpečnosti,

informační bezpečnosti,

fyzické bezpečnosti.

* + 1. Součástí testu bezpečnosti bude i fotodokumentace sloužící k zadokumentování aktuálního stavu.
1.

Kontrolní činnost

* + 1. Bezpečnostní správce bude oprávněn kdykoliv v průběhu životního cyklu informačního systému provádět kontroly dodržování bezpečnostních opatření.

VÝSLEDKY ANALÝZY RIZIK

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

Úvodní ustanovení

* + 1. V této kapitole jsou použity pojmy definované v interním dokumentu Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) „Analýza rizik informačního systému samostatných počítačů určených pro nakládání s utajovanými informacemi“ (dále jen „Analýza rizik“).
		2. Na základě výsledků provedené analýzy rizik se u informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen „informační systém“) vyžaduje aplikace následujících protiopatření.

Personální bezpečnost a organizačních opatření

| 1. Požadovaná protiopatření v oblasti personální bezpečnosti a organizačních opatřeních
 |
| --- |
| ID | Popis protiopatření |
| P1.1 | Všichni uživatelé musí splňovat podmínky pro přístup k utajované informaci stupně utajení minimálně stejného jako je stupeň utajení, pro který je určen informační systém (§ 6, 11 zákona č.412/2005 Sb.). |
| P1.2 | Všichni uživatelé jsou pro práci v informačním systému evidováni bezpečnostním správcem a autorizováni odpovědnou osobou nebo jí pověřenou osobou. |
| P1.3 | Všichni uživatelé jsou pravidelně, minimálně jedenkrát ročně) školeni z oblasti dodržování opatření stanovených v bezpečnostní dokumentaci informačního systému (§ 19 odstavce 4 a 5 vyhlášky č. 479/2024 Sb.). |
| P1.4 | Bezpečnostní správce musí mít v bezpečnostní dokumentaci stanovenu povinnost provádět pravidelnou kontrolu bezpečnostních opatření. |
| P1.5 | Servisní činnost v informačním systému se musí provádět tak, aby nebyla ohrožena jeho bezpečnost (§ 29 vyhlášky č. 479/2024 Sb.). |
| P1.6 | V bezpečnostní dokumentaci informačního systému musí být uveden seznam a řízení krizových situací (§ 30 vyhlášky č. 479/2024 Sb.). |
| P1.7 | V informačním systému může být používán pouze HW a SW odpovídající bezpečnostní dokumentaci, schválené NÚKIB a podmínkám certifikátu a certifikační zprávy (§ 28 odstavce 2 vyhlášky č. 479/2024 Sb.). |
| P1.8 | Pro každý informační systém musí být zavedena a obsazena role bezpečnostního správce pro zajištění bezpečnosti informačního systému (§ 18 vyhlášky č. 479/2024 Sb.). |
| P1.9 | Pro informační systém existuje úřadem schválená bezpečnostní dokumentace podle § 45 odstavce 2 a § 4 vyhlášky č. 479/2024 Sb. |

Fyzická bezpečnost

| 1. Požadovaná protiopatření v oblasti fyzické bezpečnosti
 |
| --- |
| ID | Popis protiopatření |
| P2.1 | Minimální míra zabezpečení zabezpečené oblasti pro umístění části informačního systému, ve které se ukládají utajované informace, se určuje v souladu s tabulkami bodových hodnot zabezpečení fyzické bezpečnosti uvedených v příloze č. 1 vyhlášky č. 479/2024 Sb. (příloha č. 1 kapitola 13 vyhlášky č. 528/2005 Sb., § 32 vyhlášky č. 447/2024 Sb., a § 24 odstavec 6 zákona č. 412/2005 Sb.). |
| P2.2 | Opatřování vybraných HW aktiv informačního systému ochrannými prvky tak, aby je bylo možné otevřít pouze při současném zničení těchto prvků (§ 22 odstavce 4 a 5 a § 13 odst. 3 písm. a) vyhlášky č. 479/2024 Sb.). |
| P2.3 | Aktiva informačního systému musí být umístěna v zabezpečené oblasti nebo objektu (§ 21 odst. 2 vyhlášky č. 479/2024 Sb., a § 24 odstavec 5 zákona č. 412/2005 Sb.). |
| P2.4 | Umístění aktiv informačního systému musí být provedeno tak, aby zamezovalo nepovolané osobě odezírat utajované informace nebo informace sloužící k identifikaci a autentizaci uživatele (§ 21 odst. 4 vyhlášky č. 479/2024 Sb.). |

Informační bezpečnost část obecné požadavky

| 1. Požadovaná protiopatření v oblasti informační bezpečnosti část obecné požadavky
 |
| --- |
| ID | Popis protiopatření |
| P3.1 | V informačním systému (pevný disk) se mohou používat pouze souborové svazky typu NTFS (pro operační systém Windows) |
| P3.2 | Start operačního systému je povolen v BIOS/UEFI pouze z pevného disku |
| P3.3 | Přístup do BIOS/UEFI je chráněn silným heslem o minimální délce 12 znaků |
| P3.4 | Je nastaveno vhodné řízení kontinuity (zálohování a postupy po haváriích atd.) |
| P3.5 | V informačním systému je nainstalován a trvale spuštěn systém virové detekce |
| P3.6 | Antivirová ochrana používá aktuální virové definice (minimálně vždy před započetím zpracování utajovaných informací) |

Informační bezpečnost část operační systém

| 1. Požadovaná protiopatření v oblasti informační bezpečnosti část operační systém
 |
| --- |
| ID | Popis protiopatření |
| P4.1 | Zavedení řízení správy účtů: |
| Chování výzvy ke zvýšení oprávnění pro správce v Režimu schválení správce | Vyzvat k zadání souhlasu |
| Chování výzvy ke zvýšení oprávnění pro standardní uživatele | Automaticky zamítnout požadavky na zvýšení |
| Při zobrazení výzvy ke zvýšení oprávnění přepnout na zabezpečenou plochu | Povoleno |
| Režim schválení správce pro integrovaný účet správce | Povoleno |
| Spustit všechny správce v Režimu schválení správce | Povoleno |
| Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelů | Povoleno |
| Zjistit instalace aplikací a zobrazit výzvu ke zvýšení oprávnění | Povoleno |
| Zvýšit oprávnění pouze u aplikací UIAccess, které jsou nainstalovány v zabezpečených umístěních | Povoleno |
| Zvýšit oprávnění pouze u podepsaných a ověřených spustitelných souborů | Zakázáno |
| Vyzvat uživatele ke změně hesla před jeho vypršením | 14 dnů |
| Zobrazit informace o uživateli, pokud je relace uzamčena | Zobrazované jméno uživatele, název domény a uživatelská jména |
| Zobrazit informace o předchozích přihlášeních během přihlášení uživatele | Povoleno |
| Povolit automatické přihlášení správce | Zakázáno |
| Automaticky přihlásit posledního interaktivního uživatele po restartování vyvolaném systémem | Zakázáno |
| Zabránit použití bezpečnostních otázek pro místní účty | Povoleno |
| Zapnout přihlášení praktickým PIN kódem | Zakázáno |
| Vypnout přihlášení pomocí obrázkového hesla | Povoleno |
| P4.2 | Zakázání anonymního přístupu: |
| Omezit použití prázdného hesla místního účtu pouze pro přihlášení ke konzole | Povoleno |
| Přejmenovat účet Guest | ano |
| Přejmenovat účet správce | ano |
| Stav účtu hosta | Zakázáno |
| Stav účtu správce | Zakázán nebo použito silné heslo a uloženo v obálce pro případné použití |
| Povolit automatické přihlášení správce | Zakázáno |
| P4.3 | Zavedení vhodné politiky hesel: |
| Heslo musí splňovat požadavky na složitost | Povoleno |
| Maximální stáří hesla | 730 dnů / 90 dnů |
| Minimální délka hesla | 12 znaků / 9 znaků |
| Minimální stáří hesla | 1 den |
| Ukládat hesla pomocí reverzibilního šifrování | Zakázáno |
| Vynutit použití historie hesel | 24 hesel |
| Doba uzamčení účtu | 0 minut |
| Prahová hodnota pro uzamčení účtu | 7 chybných pokusů / 3 chybné pokusy |
| Vynulovat čítač uzamčení účtu po | 60 minut |
| P4.4 | Zavedení řízení neobsluhovaných zařízení: |
| Povolit spořič obrazovky | Povoleno |
| Zabránit změnám spořiče obrazovky | Povoleno |
| Chránit spořič obrazovky heslem | Povoleno |
| Časový limit spořiče obrazovky | Povoleno 900 (15 min) |
| Vynutit konkrétní spořič obrazovky | Povoleno (mystery.scr) |
| P4.5 | Nastavení vhodných parametrů auditování: |
| Auditovat používání oprávnění | bez auditování |
| Auditovat přístup k adresářové službě | bez auditování |
| Auditovat přístup k objektům | bez auditování |
| Auditovat sledování procesů | bez auditování |
| Auditovat správu účtů | úspěšné pokusy, neúspěšné pokusy |
| Auditovat systémové události | úspěšné pokusy, neúspěšné pokusy |
| Auditovat události přihlášení | úspěšné pokusy, neúspěšné pokusy |
| Auditovat události přihlášení k účtu | úspěšné pokusy, neúspěšné pokusy |
| Auditovat změny zásad | úspěšné pokusy, neúspěšné pokusy |
| Generovat audity zabezpečení | Local Service, Network Service |
| Spravovat auditování a protokol zabezpečení | Administrator |
| Není-li možno protokolovat audity zabezpečení, vypnout okamžitě systém | Zakázáno |
| Minimální velikost protokolu - aplikační | 50 048 KB jako minimum |
| Minimální velikost protokolu - systém | 50 048 KB jako minimum |
| Minimální velikost protokolu - bezpečnost | 100 096 KB jako minimum |
| Automaticky zálohovat protokol při naplnění (všechny protokoly) | Povoleno |
| P4.6 | Vhodné nastavené řízení přístupu a použití vynucených cest: |
| Nadpis zprávy pro uživatele pokoušející se přihlásit | „Varování“ |
| Nevyžadovat stisknutí kláves Ctrl+Alt+Del | Zakázáno |
| Nezobrazovat naposledy použité uživatelské jméno | Povoleno |
| Text zprávy pro uživatele pokoušející se přihlásit | „Přihlašujete se do informačního systému nakládajícího s utajovanými informacemi podle zákona č. 412 / 2005 Sb. Nejste-li autorizováni pro práci v tomto systému, ihned se odhlaste, jinak se vystavujete možným sankcím podle tohoto zákona.“ |
| Povolit vypnutí systému bez nutnosti přihlášení | Zakázáno |
| Zabránit uživatelům instalovat ovladače tiskáren | Povoleno |
| Skrýt vstupní body pro Rychlé přepínání uživatele | Povoleno |
| Vždy použít klasické přihlašování | Povoleno |
| Vypnout automatické přehrávání | Povoleno (všechny diskové jednotky) |
| Nepřesouvat odstraněné soubory do koše | Povoleno |

Informační bezpečnost část komunikační

| 1. Povinná protiopatření v oblasti informační bezpečnosti část komunikační
 |
| --- |
| ID | Popis P5.x |
| P5.1 | Zakázání nepovolených komunikačních kanálů: |
| Zakázat všechny síťové adaptéry počítače včetně Wireless LAN. |
| Zakázat přístup k zařízení typu Bluetooth. |
| Nastavit přístupy k vyměnitelným úložištím CD, DVD, disketové jednotky, vyměnitelné disky, páskové jednotky, zařízení WPD (spouštění, čtení a zápis) |
| Pro řízení vstupně výstupních portů určených pro připojení vyměnitelných úložišť využívat vhodné SW nebo HW prostředky. |
| P5.2 | Nosiče informací používané v informačním systému musí být značeny a evidovány v souladu s § 13 odst. 2 a § 42 odstavcem 4 a 5 vyhlášky č. 479/2024 Sb. |
| P5.3 | Manipulace s nosiči prováděna v souladu s právními předpisy: |
| Aktiva informačního systému musí opatřeny ochrannými prvky, tak aby je bylo možné otevřít, pouze při současném zničení těchto prvků (§ 22 odstavce 4 a 5 a § 13 odst. 3 písm. a) vyhlášky č. 479/2024 Sb.) |
| Ničení nosiče utajovaných informací informačního systému musí být provedeno tak, aby se znemožnilo utajovanou informaci z něho opětovně získat (§15 odstavec 3 vyhlášky č. 479/2024 Sb.) |

* + 1. Část protiopatření P5.1 (nastavení přístupu čtení, zápis a spuštění k vyměnitelným úložištím) musí být podrobně specifikována v kapitole „Bezpečnostní nastavení operačního systému MS Windows informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené“ (dále jen „Bezpečnostní nastavení operačního systému MS Windows“).

Informační bezpečnost část aplikační

| 1. Povinná protiopatření v oblasti informační bezpečnosti část aplikační
 |
| --- |
| ID | Popis P6.x |
| P6.1 | Dostatečné testování SW před jeho nasazením: |
| každý SW je před nasazením do IS testován v provozním prostředí IS |
| testování se provádí s ohledem na požadovanou funkcionalitu SW |
| testování je zadokumentováno v provozní dokumentaci (např. provozní deník) |
| P6.2 | Správné nastavení SW: |
| nastavit parametry SW v souladu s instalační příručkou a požadavky bezpečnosti |
| nastavit parametry SW v souladu s provedenými testy |
| P6.3 | Používat pouze dostatečně odladěný SW: |
| používat především zavedený, vyzkoušený a testovaný SW |
| v případě SW vlastní výroby musí k SW existovat příručka pro instalaci, uživatelská příručka a musí být zadokumentovány provedené testy funkcionality SW |

Informační bezpečnost část kompromitující vyzařování

| 1. Povinná protiopatření v oblasti informační bezpečnosti část aplikační
 |
| --- |
| ID | Popis P7.x |
| P7.1 | Umístění aktiv informačního systému musí být provedeno tak, aby zamezovalo nepovolané osobě odezírat utajované informace nebo informace sloužící k identifikaci a autentizaci uživatele (§ 21 odst. 4 vyhlášky č. 479/2024 Sb.). |
| P7.2 | Používat pouze HW s prohlášením o shodě podle zákona č. 22/1997 Sb. |

POPIS BEZPEČNOSTI

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

Úvod

Úvodní ustanovení

* + 1. Popis bezpečnosti popisuje postupy při ochraně utajovaných informací v informačním systému.
		2. Popis bezpečnosti vychází z kapitol: Bezpečnostní politika a Výsledky analýzy rizik a stanoví minimální bezpečnostní opatření k zajištění bezpečnosti informačního systému. Bezpečnostní opatření jsou tvořena souborem norem, pravidel a postupů vymezující způsob zajištění důvěrnosti, integrity a dostupnosti utajovaných informací, dostupnosti služeb informačního systému a odpovědnosti pracovníků v jednotlivých rolích.
		3. Ochrana utajovaných informací v informačním systému je prováděna v souladu se zákonem[[5]](#footnote-5)) a vyhláškou[[6]](#footnote-6)).

Druh a rozsah zpracovávaných utajovaných informací

* + 1. Informační systém je určen pro zpracování utajovaných informací stupně utajení Vyhrazené. Tuto informaci vyznačí bezpečnostní správce na „Specifikační list pracoviště“.
		2. Jakékoliv změny v rozsahu a typu zpracovávaných utajovaných informací se musí neprodleně a prokazatelně nahlásit na NÚKIB.

Určení a rozsah informačního systému

* + 1. Informační systém je tvořen množinou jednoho nebo několika samostatných vzájemně nepropojených pracovišť, kde pracovištěm rozumíme jeden samostatný stacionární případně přenosný počítač, jeho programové vybavení, k tomu patřící periferní zařízení nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací, který je umístěn v ohraničeném prostoru a není propojen s jiným informačním případně komunikačním systémem.
		2. Celkový počet provozovaných pracovišť a počet uživatelů vychází z potřeb a požadavků provozovatele informačního systému.
		3. Informační systém je provozován v bezpečnostním provozním módu s nejvyšší úrovní[[7]](#footnote-7)). Tuto informaci vyznačí bezpečnostní správce na „Specifikační list pracoviště“.
		4. Základní jednotka (počítač, notebook) je na viditelném místě označena štítkem s uvedením stupně utajení, tak aby byla zřejmá její příslušnost k informačnímu systému.
		5. Ke každému pracovišti vede bezpečnostní správce „Specifikační list pracoviště“, který obsahuje:

maximální stupeň utajení zpracovávaných informací,

bezpečnostní provozní mód,

seznam použitého HW a SW,

umístění,

specifikace zabezpečené oblasti nebo objektu.

Podmínky provozování

* + 1. Informační systém je možné provozovat pouze za předpokladu, že jej certifikoval NÚKIB a odpovědná osoba nebo jí pověřená osoba jej schválila do provozu.
		2. V informačním systému lze provozovat pouze to pracoviště:

které, je umístěno v souladu s požadavky fyzické bezpečnosti,

jehož HW komponenty jsou označeny a nastaveny v souladu s výsledky analýzy rizik,

pro které bezpečnostní správce vede „Specifikační list pracoviště“,

pro které bezpečnostní správce vede „Evidenci uživatelů“,

které, NÚKIB schválil do provozu.

Personální bezpečnost

Obecné požadavky

* + 1. Pro Informační systém jsou definované tři základní role: uživatel, bezpečnostní správce a provozní správce.
		2. Rolí rozumíme souhrn určených činností a potřebných autorizací pro pracovníka působícího v informačním systému.
		3. Pro každou roli je vypracována směrnice, která definuje práva a povinnosti pracovníka vykonávající danou roli.
		4. Bezpečnostní a provozní správci a uživatelé splňují pro výkon své role následující podmínky:

jsou oprávněni k přístupu k utajované informaci minimálně pro stupeň utajení Vyhrazené,

jsou písemně pověřeni do příslušné role v informačním systému,

jsou evidováni ve stanovených pomůckách,

jsou proškoleni v souladu s vyhláškou[[8]](#footnote-8)).

* + 1. Pověření pracovníka do stanovené role provádí písemně odpovědná osoba nebo jí pověřená osoba. Pověření pracovníka do role bezpečnostního nebo provozního správce slouží zároveň jako pověření do role uživatele.
		2. Bezpečnostní správce vede evidenci uživatelů včetně jejich proškolení a pověření.
		3. Role provozního správce a bezpečnostního správce mohou být sloučeny.

Informační bezpečnost

Nastavení parametrů BIOS/UEFI

* + 1. Nastavení parametrů BIOS/UEFI je provedeno podle doporučení NÚKIB
		2. Přístup k BIOS/UEFI je umožněn pouze po zadání hesla, jehož délka je minimálně 12 znaků.
		3. Bootování je povoleno pouze z HDD/SSD, který obsahuje systémový oddíl nebo Windows Boot Manager.
		4. V případě UEFI je deaktivována možnost spuštění jednorázového Boot Menu (volba Boot Device List).
		5. Možnost bootování z ostatních zařízení (LAN, USB, Secure Digital SD apod.) je zakázána.
		6. Nepotřebné komunikační a bezdrátové rozhraní (eSata, ThunderBolt, FireWire, Wireless, Bluetooth apod.) jsou zakázány.
		7. Podrobné nastavení BIOS/UEFI je uvedeno v dokumentu „Bezpečnostní nastavení BIOS/UEFI informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené“.

Bezpečnostní nastavení operačního systému

* + 1. Pracoviště informačního systému jsou provozována se schváleným operačním systémem rodiny MS Windows.
		2. Operační systém je nastaven v souladu s kapitolou „Výsledky analýzy rizik“ a podle doporučení NÚKIB. Nastavení operačního systému je popsáno v kapitole „Bezpečnostní nastavení operačního systému MS Windows“.
		3. Použitý operační systém zajišťuje svými prostředky a nastavením:

jednoznačnou identifikaci a autentizaci uživatele,

volitelné řízení přístupu,

vytváření auditních záznamů,

ošetření paměťových objektů před jejich dalším použitím.

Přístupová hesla

* + 1. Přístupové heslo k účtu informačního systému je chráněno jako utajovaná informace stupně utajení Vyhrazené.
		2. Přístupová hesla k BIOS/UEFI, pevným účtům nebo ke službám operačního systému informačního systému jsou chráněna jako utajovaná informace stupně utajení Vyhrazené a jsou po dobu platnosti uložena v zabezpečené obálce v příslušném úschovném objektu.

Auditní záznamy

* + 1. Vytváření auditních záznamů je zajišťováno funkcionalitou a nastavením použitého operačního systému případně i aplikačního software.
		2. Bezpečnostní správce provádí kontrolu a archivaci auditních záznamů:

pravidelně 1x měsíčně nebo,

v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací.

* + 1. Auditní záznamy jsou archivovány po dobu minimálně pěti let.
		2. Auditní záznamy nejsou klasifikovány jako utajované informace, ale zachází se s nimi jako s citlivými informacemi.

Bezpečnost V/V portů

* + 1. Používání vstupně výstupních portů na pracovištích je řízeno. Řízení vstupně výstupních portů zajišťuje, že na pracovišti mohou být používána pouze schválená vstupně výstupní zařízení.
		2. Způsob řízení vstupně výstupních portů je popsán v kapitole „Bezpečnostní nastavení operačního systému MS Windows“.

Bezpečné mazání

* + 1. Bezpečným mazáním rozumíme smazání uložených informací, jehož cílem není snížit nebo zrušit stupeň utajení nosiče informací, ale pouze umožnění použití tohoto nosiče jiným uživatelem při zachování principu „need-to-know“.
		2. Bezpečné mazání nosičů informací není vyžadováno:

na vyjímatelných nosičích informací po celou dobu využívání vyjímatelného nosiče informací uživatelem nebo skupinou uživatelů (princip „need-to-know“),

na HDD/SSD po celou dobu používání HDD/SSD v informačním systému.

* + 1. Bezpečné mazání nosičů informací je vyžadováno (pokud to umožňuje stav nosiče):

na vyjímatelných nosičích informací při změně uživatele nebo skupiny uživatelů vyjímatelného nosiče informací,

na vyjímatelných nosičích informací při jejich vyřazení z používání nebo ničení,

na HDD/SSD při vyřazení HDD/SSD z informačního systému nebo jeho ničení.

* + 1. Bezpečné mazání zajišťuje nebo provádí bezpečnostní správce.
		2. Snižování nebo rušení stupně utajení nosičů informací je zakázáno. Jedinou výjimkou je stav, kdy lze prokazatelně dokázat, že po celou dobu používání nosiče na něj nebyla uložena žádná utajovaná informace.

Antivirová ochrana a aktualizace virových řetězců

* + 1. Na pracovišti je použit SW antivirové ochrany, který bezpečnostní správce uvede na „Specifikační list pracoviště“, a jehož aktualizaci provádí provozní případně bezpečnostní správce.
		2. Aktualizace virových řetězců je prováděna:

pravidelně 1x měsíčně nebo,

v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací.

Instalace a používání HW a SW

* + 1. Veškerý HW a SW použitý v informačním systému podléhá schválení NÚKIB.
		2. Pro každé pracoviště vede bezpečnostní správce „Specifikační list pracoviště“ na kterém je evidován použitý HW a SW.

Požadavky na dostupnost

* + 1. Dostupnost každého pracoviště stanoví odpovědná osoba nebo jí pověřená osoba tak, že určí maximální počet hodin, po kterou může být pracoviště nedostupné.
		2. V souladu se stanovenou dostupností volí bezpečnostní správce formu a frekvenci zálohování SW součástí pracoviště.

Fyzická bezpečnost

Obecné požadavky

* + 1. Fyzická bezpečnost pracovišť je zajišťována aplikovanými opatřeními v souladu s právními předpisy a interními akty řízení upravujícími ochranu utajovaných informací.

Podmínky pro provozování pracoviště

* + 1. HW komponenty každého pracoviště jsou umístěny tak, aby bylo neoprávněné osobě zamezeno odezírání zpracovávané utajované informace.
		2. Při zpracovávání utajované informace typu audio záznamu, je zajištěno, že nedojde k porušení povinnosti při ochraně utajované informace cestou akustického přeslechu.

Přeprava a ukládání nosičů utajovaných informací

* + 1. Nosiče utajovaných informací jsou přepravovány v aktovce, kufříku, kufru, přenosné bezpečnostní schránce nebo v kurýrním vaku, který je způsobilý k přepravě utajovaných dokumentů (dále jen „přenosná schránka“).
		2. Přenosná schránka je zajišťována proti neoprávněné manipulaci s jejím obsahem např. uzamčením mechanickým zámkem, pečetěním apod. Přenosná schránka je opatřena na vhodném místě názvem a adresou provozovatele informačního systému provozuje a nápisem: „V případě nálezu neotvírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!“.
		3. Přenosné počítače a vyjímatelné nosiče utajovaných informací se ukládají v zabezpečené oblasti minimálně kategorie Vyhrazené v příslušném úschovném objektu typu 1 nebo 1A.

Režimová opatření

* + 1. Na každém pracovišti se dodržují režimová opatření stanovená v příslušném projektu fyzické bezpečnosti.
		2. Dodržování stanovených režimových opatření kontroluje bezpečnostní správce.

Způsob evidence HW komponent

* + 1. Každá HW komponenta je evidována bezpečnostním správcem.
		2. Základní jednotka (počítač, notebook) je na viditelném místě označena štítkem obsahujícím údaje o stupni maximálním utajení zpracovávaných utajovaných informací a názvem provozovatele informačního systému.
		3. Příklad štítku pro označení základní jednotky:

IS pro zpracování utajovaných informací:

VYHRAZENÉ

*Otisk razítka nebo název provozovatele*

Ochranné prvky

* + 1. HW komponenty pracoviště obsahující alespoň jeden nevyjímatelný nosič informací, který nepotřebuje pro uchování informace trvalé připojení k elektrické energii, jsou opatřeny jedním nebo několika ochranným prvky.
		2. Ochranné prvky jsou na HW komponentě umístěny tak, aby při pokusu o vniknutí do HW komponenty došlo k jejich poškození a zároveň tak, aby byla možná jejich snadná vizuální kontrola uživatelem.
		3. Neporušenost ochranných prvků kontroluje bezpečnostní správce minimálně jednou měsíčně nebo v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací.
		4. Uživatelé kontrolují neporušenost ochranných prvků vždy před zahájením své práce.
		5. Porušení ochranného prvku je považováno za bezpečnostní incident.
		6. Ochranný prvek musí být číslovaný a obsahovat reziduální vrstvu, která při pokusu o sejmutí zůstává na původním povrchu.
		7. Použití ochranného prvku (jeho číslo) uvede bezpečnostní správce v Provozním deníku. Příklad ochranného prvku:



Kompromitující vyzařování

* + 1. V informačním systému jsou použita pouze HW zařízení, která splňují požadavky na elektrickou bezpečnost a elektromagnetickou kompatibilitu (EMC) podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů (dále jen „zákon č. 22/1997 Sb.“).
		2. Obrazovka monitoru nebo konzole, klávesnice a tiskárny jsou umístěny tak, aby bylo neoprávněné osobě zamezeno odezírání zpracovávané utajované informace.
		3. Při zpracovávání utajované informace typu audio záznamu, je zajištěno, že nedojde k porušení povinnosti při ochraně utajované informace cestou akustického přeslechu.

Administrativní bezpečnost

Obecné požadavky

* + 1. Všechny utajované informace exportované z informačního systému jsou označeny odpovídajícím stupněm utajení a je s nimi nakládáno v souladu s právními předpisy a interními akty řízení upravujícími ochranu utajovaných informací.

Evidence a označování nosičů informací

* + 1. Všechny nosiče informací používané v informačním systému jsou evidované. Evidenci vede určený zaměstnanec (obvykle bezpečnostní správce).
		2. Všechny HDD/SSD používané v informačním systému jsou vedeny podle výrobních čísel v evidenci bezpečnostního správce.
		3. Nosiče informací, které jsou používány jako pomůcka uživatele k ukládání utajovaných informací (záloha uživatelských dat apod., dále jen „provozní nosiče utajovaných informací“) jsou označeny a evidovány podle vyhlášky č. 479/2024 Sb., o informační bezpečnosti (štítek na kterém je uveden zejména: název organizace, evidenční číslo a stupeň utajení). Příklad štítku utajovaného nosiče:

Provozovatel: ………………………..

…………………………………………

stupeň utajení: **V Y H R A Z E N É**

Ev.č.: …………………………………...

* + 1. Nosiče informací, které jsou určeny pro export utajovaných informací mimo organizaci, jsou označeny a evidovány podle vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů (štítek na kterém je uveden zejména: název organizace, číslo jednací nebo příloha k č. j. a stupeň utajení).
		2. Nosiče informací, které jsou používány jako pomůcka uživatele pro neutajované informace (vkládání aktualizací virových řetězců, záloha auditních záznamů apod., dále jen „provozní nosiče“) jsou opatřeny štítkem, na kterém je uveden zejména: název organizace a evidenční číslo. Příklad štítku neutajovaného nosiče:

Provozovatel: ………………………..

…………………………………………

Ev.č.: ……………………….…….…...

* + 1. Evidenční číslo provozního nosiče se vytváří v souladu s § 42 odst. 4 písm. c) vyhlášky č. 479/2024 Sb., o informační bezpečnosti, a obsahuje zkratku stupně utajení, je-li nosič informací utajovaný, nebo zkratka informace o tom, že nosič informací je neutajovaný, pořadové číslo, rok zavedení do evidence a identifikaci provozovatele systému.
		2. Jednotlivé položky evidenčního čísla nosiče informací se oddělují lomítkem nebo spojovníkem.
		3. V případě evidence pevného disku, který je pevně zabudován v pracovní stanici nebo notebooku je pracovní stanice nebo notebook opatřen štítkem, který informuje o zabudovaném nosiči informací. Příklad štítku:

Zařízení obsahuje zabudovaný nosič informací:

ev.č.: ………………………...

stupeň utajení: **VYHRAZENÉ**

Likvidace nosičů utajovaných informací

* + 1. S provozními nosiči utajovaných informací se nakládá jako s utajovanou informací až do doby jejich fyzického zničení.
		2. Likvidace provozních nosičů utajovaných informací je prováděna příslušným zaměstnancem pověřeným vedením jejich evidencí na certifikovaném zařízení fyzického ničení nosičů informací za přítomnosti dalšího zaměstnance (obvykle uživatele nosiče).
		3. O likvidaci provozního nosiče utajovaných informací je proveden záznam v „Evidenci nosičů“. Záznam o zničení provozního nosiče je podepsaný zaměstnanci, kteří likvidaci provedli.
		4. Pokud provozovatel informačního systému není schopen provést likvidaci provozního nosiče utajovaných informací, požádá NÚKIB o spolupráci.

Provozně bezpečnostní dokumentace

* + 1. Všechny písemnosti týkající se bezpečnosti a provozu informačního systému se uchovávají minimálně po dobu 5 let od doby ukončení jejich používání.
		2. Pro informační systém je vypracována následující dokumentace:

Směrnice bezpečnostního správce,

Směrnice provozního správce,

Směrnice uživatele,

Testy bezpečnosti,

Řízení vstupně výstupních portů,

Bezpečnostní nastavení operačního systému,

Specifikační list pracoviště (pro každé pracoviště),

Evidence uživatelů (pro každé pracoviště),

Evidence nosičů informací (pro celý informační systém),

Provozní deník pracoviště (pro každé pracoviště),

Kniha manipulace s nosiči utajovaných informací nebo s přenosným počítačem.

Požadavky bezpečného provozu

Údržba a opravy

* + 1. Servis se provádí tak, aby nedošlo k porušení povinnosti při ochraně utajované informace.
		2. Servis zajišťuje provozní správce (držitel patřičné odborné kvalifikace podle vyhlášky č. 50/1978 Sb., o odborné způsobilosti v elektrotechnice) pokud možno vlastními silami a v objektu minimálně kategorie Vyhrazené. V případě nutnosti je servisní úkon prováděn externím subjektem pod dohledem pracovníka správy.
		3. Pokud nelze provést servisní úkon vlastními silami a v objektu minimálně kategorie Vyhrazené, jsou ze zařízení odstraněny ochranné prvky a vyjmuty všechny nosiče informací, které pro zachování uložených informací nepotřebují trvalé napájení.
		4. Při servisu lze použít pouze takové náhradní komponenty, které splňují požadavky zákona č. 22/1997 Sb., a pro tyto komponenty bylo vydáno „Prohlášení o shodě“, „ES Prohlášení o shodě“ nebo jsou označeny symbolem CE (CE Mark).
		5. O úkonech provedených v rámci servisu provádí pracovník správy záznam v provozním deníku pracoviště.

Krizové situace a bezpečnostní incidenty

* + 1. Za **krizovou situaci** v informačním systému je považována porucha zařízení, požár nebo jiná živelní pohroma, teroristický útok nebo jeho hrozba.
		2. V případě vzniku krizové situace na pracovišti je nutné zajistit, aby nedošlo k porušení povinnosti při ochraně utajované informace. Pokud to okolnosti dovolí, ukončí uživatel práci, vyjme vyjímatelné nosiče, odebere z tiskárny všechny listy vytištěných dokumentů, odebere z pracoviště „Provozní deník pracoviště“, zamkne a dále se řídí příslušnými směrnicemi objektu.
		3. **Bezpečnostní incident** je událost, která má nebo může mít za následek ohrožení bezpečnosti informačního systému nebo porušení povinnosti při ochraně utajované informace.
		4. Za bezpečnostní incident je považováno zejména:

porušení některého z bezpečnostních mechanismů,

porušení ochranných prvků,

ztráta nebo neoprávněné nakládání s nosičem utajovaných informací,

ztráta HW komponenty,

porucha HW nebo SW,

výskyt viru nebo jiného škodlivého SW,

vyzrazení přístupového hesla,

porušení platných bezpečnostních směrnic,

další události, které mohou mít vliv na bezpečnost zpracovávaných utajovaných informací.

* + 1. Uživatel je povinen bezodkladně informovat bezpečnostního správce o zjištění nebo podezření na krizovou situaci nebo bezpečnostní incident.
		2. V případě poruchy HW nebo SW nebo v případě výskytu viru je uživatel povinen přerušit práci až do vyřešení bezpečnostního incidentu.
		3. Bezpečnostní správce ověří, zda došlo nebo mohlo dojít, v souvislosti s krizovou situací nebo bezpečnostním incidentem k porušení povinnosti při ochraně utajované informace a neprodleně informuje odpovědnou osobu nebo jí pověřenou osobu a řídí se jejími pokyny.
		4. O bezpečnostním incidentu, který měl za následek porušení povinnosti při ochraně utajované informace, je bezodkladně informován Národní bezpečnostní úřad.
		5. O průběhu šetření bezpečnostního incidentu a o výsledcích šetření se zpracovává písemný záznam, který se ukládá na dobu 5 let.
		6. O výskytu krizové situace nebo bezpečnostního incidentu provádí uživatel a příslušným pracovník správy záznam.
		7. Bezpečnostní správce navrhuje na základě výsledků šetřených bezpečnostních incidentů odpovídající bezpečnostní opatření a případné změny bezpečnostní dokumentace.

Změny při provozování pracoviště

* + 1. Změnou při provozování pracoviště je rozuměna jakákoli změna, která je v rozporu se skutečností uvedenou ve „Specifikačním listu pracoviště“, provozní nebo provozně bezpečnostní dokumentací nebo příslušné evidenci (vyjma evidence uživatelů).
		2. Veškeré změny pracoviště jsou neprodleně oznamovány NÚKIB a podléhají jeho schválení.

Testy bezpečnosti

* + 1. U každého pracoviště je před zahájením jeho provozu:

prokazatelně proveden bezpečnostním správcem test bezpečnosti,

pracovníkem NÚKIB provedeno schválení pracoviště na základě doručeného testu bezpečnosti nebo provedené kontrolní obhlídky.

* + 1. Test bezpečnosti je zaměřen na zjištění stavu bezpečnosti pracoviště podle bezpečností dokumentace z oblastí:

personální bezpečnosti a organizačních opatření,

administrativní bezpečnosti,

informační bezpečnosti,

fyzické bezpečnosti,

ochrany proti úniku kompromitujícího vyzařování.

* + 1. Součástí testu bezpečnosti může být i fotodokumentace sloužící k zadokumentování aktuálního stavu.

Kontrolní činnost

* + 1. Bezpečnostní správce je oprávněn kdykoliv v průběhu životního cyklu informačního systému provádět kontroly dodržování bezpečnostních opatření.

Příloha: Vzory administrativních pomůcek

Seznam vzorů

* + 1. Vzor pověření k činnosti
		2. Vzor ukončení pověření k činnosti
		3. Školení uživatelů
		4. Evidence uživatelů
		5. Evidence nosičů informací
		6. Kniha manipulace s nosiči utajovaných informací nebo s přenosným počítačem
		7. Provozní deník pracoviště
		8. Specifikační list pracoviště

Vzor č. 1: pověření k činnosti

Pověření zaměstnance k výkonu role

Pověřuji k výkonu role v informačním systému určeného k nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené níže uvedené zaměstnance. Zaměstnanci byli zároveň proškoleni a seznámeni s příslušnou bezpečnostní směrnicí, která upravuje práva a povinnosti zaměstnance při výkonu role v informačním systému.

|  |  |  |  |
| --- | --- | --- | --- |
| Jméno a příjmení | č. OP | č. osvědčení nebo oznámení | role |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Dne: | *datum* |  | *titul jméno a příjmení* |
|  |  | *odpovědná osoba / bezpečnostní ředitel* |

Vzor č. 2: ukončení pověření k činnosti

Ukončení pověření zaměstnance k výkonu role

Ukončuji pověření k výkonu role v informačním systému určeného k nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené pro níže uvedené zaměstnance.

|  |  |  |
| --- | --- | --- |
| Jméno a příjmení | č. OP | role |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Dne: | *datum* |  | *titul jméno a příjmení* |
|  |  | *odpovědná osoba / bezpečnostní ředitel* |

Vzor č. 3: školení uživatelů

|  |  |
| --- | --- |
| Datum: | Školení provedl: |
|  |
| ŠKOLENÍ UŽIVATELŮ |
| Jméno a příjmení účastníka školení | Podpis |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Vzor č. 4: evidence uživatelů

evidence uživatelů

pro

pracoviště IS: *název pracoviště*

|  |  |  |  |
| --- | --- | --- | --- |
| Počet listů: | *5* |  |  |
| Vydáno dne: | *datum* |  | *titul jméno a příjmení* |
|  |  | *odpovědná osoba / bezpečnostní ředitel* |

| **p.č.** | **Titul, jméno, příjmení** | **role v IS** | **č. pověření nebo osvědčení** | **platnost pověření nebo osvědčení** | **pověřen od****(datum)** | **pověření ukončeno****(datum)** |
| --- | --- | --- | --- | --- | --- | --- |
| **od** | **do** |
| 1 | *Jan Novák* | *uživatel* | *NBÚ-150698* | *1.1.2021* | *31.12.2028* | *10.5.2022* |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |  |

Vzor č. 5: evidence nosičů informací

evidence nosičů informací

|  |  |  |  |
| --- | --- | --- | --- |
| Počet listů: | *5* |  |  |
| Vydáno dne: | *datum* |  | *titul jméno a příjmení* |
|  |  | *odpovědná osoba / bezpečnostní ředitel* |

| p.č. | Nosič (typ, velikost, sériové číslo) | Stupeň utajení | Evidenční označení | Datum zavedení | Datum vyřazení | Poznámka |
| --- | --- | --- | --- | --- | --- | --- |
| 01 | *USB flash disk (ADATA, 32 GB, 0256C52D0)* | *V* | *V/1/2021-TVA* | *5.8.2021* |  |  |
| 02 |  |  |  |  |  |  |
| 03 |  |  |  |  |  |  |
| 04 |  |  |  |  |  |  |
| 05 |  |  |  |  |  |  |
| 06 |  |  |  |  |  |  |
| 07 |  |  |  |  |  |  |
| 08 |  |  |  |  |  |  |
| 09 |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |

Vzor č. 6: evidence příjmu a výdeje nosičů informací

Kniha manipulace s nosiči utajovaných informací
nebo s přenosným počítačem

|  |  |  |  |
| --- | --- | --- | --- |
| Počet listů: | *10* |  |  |
| Vydáno dne: | *datum* |  | *titul jméno a příjmení* |
|  |  | *odpovědná osoba / bezpečnostní ředitel* |

| **p. č.** | **Typ nosiče informací / přenosného PC** | **evid.****označení** | **stupeň utajení** | **vydáno** | **vráceno** | **jiné záznamy** |
| --- | --- | --- | --- | --- | --- | --- |
| **datum** | **jméno, příjmení** | **podpis** | **datum** | **jméno, příjmení** | **podpis** |
| 01 | *USB flash disk* | *V/1/2021-TVA* | *V* | *2.5.2021* | *Jan Novák* | Novák | *2.5.2021* | *Petr Správce* | Správce |  |
| 02 | *NTB Dell Latitude 5511* | *PV-01* | *V* | *2.5.2021* | *Jan Novák* | Novák | *2.5.2021* | *Petr Správce* | Správce |  |
| 03 |  |  |  |  |  |  |  |  |  |  |
| 04 |  |  |  |  |  |  |  |  |  |  |
| 05 |  |  |  |  |  |  |  |  |  |  |
| 06 |  |  |  |  |  |  |  |  |  |  |
| 07 |  |  |  |  |  |  |  |  |  |  |
| 08 |  |  |  |  |  |  |  |  |  |  |
| 09 |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |

Vzor č. 7: provozní deník pracoviště

provozní deník pracoviště

pro

pracoviště IS: *název pracoviště*

|  |  |  |  |
| --- | --- | --- | --- |
| Počet listů: | *15* |  |  |
| Vydáno dne: | *datum* |  | *titul jméno a příjmení* |
|  |  | *odpovědná osoba / bezpečnostní ředitel* |

| Datum(d.m.r) | Čas(od-do) | Popis činnosti | Jméno | Podpis |
| --- | --- | --- | --- | --- |
| *5.5.2021* | *10:30-11:40* | *Aktualizace antivirových řetězců* | *Petr Správce* | Petr Správce |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Vzor č. 8: specifikační list pracoviště

|  |
| --- |
| SPECIFIKAČNÍ LIST PRACOVIŠTĚ: *PV-01* |
| Provozovatel pracoviště: |
| Název organizace / firmy / podnikatele: |  |
| *První stavební s r.o.* |
| Adresa a umístění pracoviště: |
| město / obec: | část obce: | PSČ: |
| *Praha 6* | *Dejvice* | *160 00* |
| ulice: | číslo popisné / orientační: |
| *Stavební* | *35/192* |
| poschodí: | číslo / označení místnosti: |
| *3 NP* | *315b* |
| Fyzické zabezpečení[[9]](#footnote-9): |
| kategorie objektu[[10]](#footnote-10): | kategorie zabezpečené oblasti[[11]](#footnote-11): |
| *Vyhrazené* | *Vyhrazené* |
| Stupeň utajení informací: | VYHRAZENÉ |
| Bezpečnostní provozní mód: | s nejvyšší úrovní |
| Politika hesel: |  | varianta | Max stáří hesla | Min délka hesla | Uzamčení po |
| X | 1 | 90 | 9 | 3 |
|  | 2 | 730 | 12 | 7 |
| Personální zabezpečení: |
| Pověřený bezpečnostní správce[[12]](#footnote-12): | *Ing. Jan Novák* |
| Pověřený evidenční pracovník[[13]](#footnote-13): | *Ing. Petr Pavel* |

|  |
| --- |
| Seznam HW: |
| název: | sériové číslo: | výrobce / dodavatel |
| *NTB Dell Latitude 5511* | *CNG1254896* | *Dell* |
| *Myš optická drátová USB* |  | *HP* |
| *Klávesnice drátová USB* | *2546987526* | *HP* |
| *Monitor LG 24MP59G* | *GHF658LM85* | *LG* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Seznam SW: |
| název: | licence: | výrobce / dodavatel |
| *MS Windows 10 Professional* |  | *Microsoft* |
| *MS Office 2016 Professional* |  | *Microsoft* |
| *Adobe Reader 10* |  | *Adobe* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Vzor č. 9: test bezpečnosti

Test bezpečnosti

pracoviště IS: ***PV-01***

Personální bezpečnost

|  |  |  |
| --- | --- | --- |
| p.č. | Kontrola | Výsledek |
| 1.1 | Bezpečnostní správce je pověřen odpovědnou osobou nebo jí pověřenou osobou |  |
| 1.2 | Bezpečnostní správce splňuje podmínky přístupu fyzické osoby k utajované informaci minimálně stejného stupně, pro jaký je určen informační systém |  |
| 1.3 | Bezpečnostní správce vede seznam oprávněných a pověřených uživatelů |  |
| 1.4 | Bezpečnostní správce vede přehled pravidelných školení uživatelů |  |

Fyzická bezpečnost

|  |  |  |
| --- | --- | --- |
| p.č. | Kontrola | Výsledek |
| 2.1 | HW komponenty jsou umístěny v souladu požadavky fyzické bezpečnosti (kontrola projektu fyzické bezpečnosti) |  |
| 2.2 | HW komponenty jsou umístěny tak, aby bylo zamezeno neoprávněnému odezírání zpracovávaných informací |  |
| 2.3 | HW komponenty jsou označeny v souladu s popisem bezpečnosti |  |
| 2.4 | HW komponenty jsou opatřeny ochrannými prvky v souladu s popisem bezpečnosti |  |
| 2.5 | HW komponenty odpovídají seznamu na „Specifikačním listu pracoviště“ |  |

Administrativní bezpečnost

|  |  |  |
| --- | --- | --- |
| p.č. | Kontrola | Výsledek |
| 3.1 |  „Provozní deník“ je autorizován odpovědnou osobou  |  |
| 3.2 | „Evidenci nosičů informací“ je autorizována odpovědnou osobou |  |
| 3.3 | „Evidence uživatelů“ je autorizována odpovědnou osobou |  |
| 3.4 | Nosiče informací jsou označeny v souladu s popisem bezpečnosti |  |
| 3.5 | Hesla BIOS/UEFI a pevného účtu administrátora jsou uložena v zalepené obálce v příslušném úschovném objektu. |  |

Informační bezpečnost

|  |  |  |
| --- | --- | --- |
| p.č. | Kontrola | Výsledek |
| 4.1 | V BIOS/UEFI je nastaveno bootování pouze z pevného disku |  |
| 4.2 | V BIOS/UEFI jsou zakázány bezdrátové technologie, síťové adaptéry, a další nepotřebné rozhraní |  |
| 4.3 | BIOS/UEFI je chráněn heslem |  |
| 4.4 | HDD/SSD je naformátován na souborový svazek typu NTFS |  |
| 4.5 | Je nainstalován antivirový SW a má aktuální virové definice |  |
| 4.6 | Nainstalovaný SW souhlasí se seznamem na „Specifikačním listu pracoviště“ |  |
| 4.7 | Nastavení bezpečnostních charakteristik operačního systému bylo provedeno nástrojem AuTo4SeSe dodávaného NÚKIB |  |
| 4.8 | V rámci automatizovaného nastavení byla zvolena politika hesel:1 - Max stáří hesla (90 dnů), Min délka hesla (9 znaků), Prahová hodnota pro uzamčení účtu – 3 chybných pokusů o přihlášení2 - Max stáří hesla (730 dnů), Min délka hesla (12 znaků), Prahová hodnota pro uzamčení účtu – 7 chybných pokusů o přihlášení |  |
| 4.9 | V rámci automatizovaného nastavení byl vestavěný administrátorský účet:U – Uzamčen / O - Odemčen |  |
| 4.10 | V rámci automatizovaného nastavení byl zvolen přístup k CD/DVD zařízení:P – Povoleno / Z - Zakázáno |  |
| 4.11 | V rámci automatizovaného nastavení byl zvolen přístup k USB zařízení:P – Povoleno / Z - Zakázáno |  |
| 4.12 | Jsou správně nastavena oprávnění ke správě tisku:Users tisk + správa dokumentůAdministrators tisk + správa tiskárny + správa dokumentů |  |

|  |
| --- |
| Provedeno dne: *25.2.2021* |
| titul, jméno a příjmení člena komise | podpis |
| *Jan Novák* | *Jan Novák* |
| *Petr Správce* | *Petr Správce* |
|  |  |

BEZPEČNOSTNÍ NASTAVENÍ OPERAČNÍHO SYSTÉMU MS WINDOWS

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

Úvod

Vysvětlivky k použitým označením

* + 1. Příkaz Konzola znamená spuštění snap in modulu místní počítač – zásady v rámci konzoly mmc.exe - (Microsoft Management Console) nebo konzole GPEdit.msc.
		2. Příklad:
* Snap in modul místní počítač – zásady (dále jen konzola) / Místní počítač – zásady / Konfigurace počítače / Šablony pro správu / Systém / Přihlášení / Vždy použít klasické přihlašování (T02)
* Znamená: Spustit mmc.exe, menu: Soubor, volba Přidat nebo odebrat modul snap-in, přidat snap in modul Editor objektů zásad skupiny a dále editovat jednotlivé nastavení v rámci uvedeného snap in modulu nebo použít editor GPEdit.msc.
	+ 1. Označení např. (076), obecně (nnn), je odkazem na číslování bodů v části č. 2 a 3.
		2. Označení např. (L02), obecně (Lnn), je odkazem na číslování bodů v části č. 4.
		3. Označení např. (T02), obecně (Tnn), je odkazem na číslování bodů v části č. 5 a 6.
		4. Znaky --- znamenají, že položka není nakonfigurována.

|  |
| --- |
| **Povolené edice OS Windowd 10** |
| **Verze OS** | **Povolené edice** |
| Windows 10 | Professional, Enterprise, Education (64 bitová verze) |

Část první

Všeobecná nastavení OS MS Windows

Automatizované nastavení zabezpečení

* + 1. Bezpečnostní nastavení operačního systému popisované od článku 8 lze provést pomocí nástroje AuTo4SeSe, který poskytuje NÚKIB.

Příprava pevného disku

* + 1. Pevný disk je naformátován souborovým systémem NTFS, tak že nebyl prováděn převod z FAT nebo FAT 32.

Instalace operačního systému

* + 1. Při instalaci operačního systému byla provedena nová čistá instalace na nově vytvořené a naformátované oddíly (nebyl prováděn upgrade předchozích verzí Windows).

Nastavení antivirového programu

* + 1. Je zapnuta rezidentní ochranu počítače včetně testování FDD, CD, DVD a USB.

Použití technologie ReadyBoost

* + 1. Používání technologie ReadyBoost pro swapování pevného diku není povoleno.
		2. V dialogovém okně vlastnosti paměťového média (Flash disk) v záložce Ready Boost je zvolena volba Nepoužívat toto zařízení.

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.
		3. Nastavení povolení přístupu k WLAN pomocí systému Windows:

Ovládací panely / Síť a Internet / Centrum síťových připojení a sdílení / Změnit nastavení adaptéru / Ikona bezdrátové připojení k síti / Zakázat (členění podle kategorií).

Ovládací panely / Centrum síťových připojení a sdílení / Změnit nastavení adaptéru / Ikona bezdrátové připojení k síti / Zakázat (členění podle ikon)

Na pracovní stanici může být více adaptérů různého druhu (bezdrátové připojení k síti, mobilní širokopásmové připojení). Všechny tyto adaptéry musí být zakázány.

* + 1. Nastavení omezení síťových služeb: Ovládací panely / Nástroje pro správu / Služby:

Služba Automatická konfigurace sítě WLAN – zakázat

Služba Automatická konfigurace sítě WWAN – zakázat

* + 1. Správce zařízení: Nástroje pro správu / Správa počítače / Správce zařízení / Síťové adaptéry / Wireless Network Adapter – zakázat.

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.
		3. Nastavení povolení přístupu k Bluetooth pomocí systému Windows: Ovládací panely / Síť a Internet / Centrum síťových připojení a sdílení / Změnit nastavení adaptéru / Ikona síťové připojení Bluetooth / Zakázat.
		4. Nastavení omezení síťových služeb: Ovládací panely / Nástroje pro správu / Služby: Služba pro podporu technologie Bluetooth – zakázat.
		5. Správce zařízení: Nástroje pro správu / Správa počítače / Správce zařízení / Síťové adaptéry / Zařízení Bluetooth – zakázat.

Nastavení systémových služeb

* + 1. Ovládací panely / nástroje pro správu / služby
		2. Automatická konfigurace sítě WLAN:

typ spuštění - zakázáno

požadovaný stav služby – zastaveno

* + 1. Automatická konfigurace sítě WWAN:

typ spuštění - zakázáno

požadovaný stav služby – zastaveno

* + 1. Služba pro podporu technologie Bluetooth (mobilní zařízení)

 typ spuštění – zakázáno

 požadovaný stav služby – zastaveno

Nastavení přístupových práv k souborům a adresářům

* + 1. Nastavení práv k systémovým souborům a složkám je bezpečně nastaveno při instalaci OS.

Nastavení uživatelských účtů a skupin uživatelů

|  |  |
| --- | --- |
| Administrator | pevný účet (built in), defaultně zablokovaný |
| Guest | pevný účet (bulit in), defaultně zablokovaný |
| Správce počítače | člen skupiny Administrators |
| Bezpečnostní správce počítače | člen skupiny Users, člen skupiny Event Log Readers |
| Uživatel | člen skupiny Users |

Tiskárny

* + 1. Tiskárny a faxy / Vlastnosti (tiskárny) / Zabezpečení

|  |  |
| --- | --- |
| Tisk | Admistrators, Users – povolit |
| Správa tiskáren | Administrators – povolit |
| Správa dokumentů | Admistrators, Users – povolit |

Odinstalování nepotřebných aplikací (doporučení k zpřehlednění systému)

* + 1. Část nepotřebných moderních aplikací, které jsou součástí operačního systému lze z konkrétního účtu odinstalovat následujícím způsobem:

• Uživatelské prostředí Start / Nastavení / Systém / Aplikace a funkce, potom zvolit postupně jednotlivé aplikace a potvrdit volbu Odinstalovat.

• Použít aplikaci 10AppsManager vydavatele The Windows Club, která nevyžaduje instalaci.

• Použít příkazový řádek aplikace Windows PowerShell pod administrátorským oprávněním (Start / Všechny aplikace / Windows PowerShell – Spustit jako správce) následujícím způsobem.

* + 1. Odinstalování aplikací z konkrétního účtu:

Zjištění jména aplikace: Get-AppxPackage | Select Name, PackageFullName

Odinstalování aplikace: Get-appxpackage -Name Jméno\_aplikace (Name) | Remove-AppxPackage nebo Remove-AppxPackage Jméno\_aplikace (PackageFullName)

* + 1. Nepotřebné moderní aplikace lze z operačního systému odinstalovat provisioned způsobem.
		2. Odinstalování aplikací ze systému (Provisioned):

Zjištění jména aplikace: Get-AppxProvisionedPackage -Online | Select DisplayName, PackageName

Odinstalování aplikace: Remove-AppxProvisionedPackage –Online –PackageName Jméno\_aplikace (PackageName)

* + 1. Nově vytvořené účty již nebudou obsahovat aplikace odinstalované provisioned postupem. Tento postup je vhodný zvolit před zřízením uživatelských účtů, avšak po odstranění aplikací z již existujících účtů způsobem viz. Odinstalování aplikací z konkrétního účtu.

Část druhá

Zásady účtů

Zásady hesla

|  |
| --- |
| (001) Heslo musí splňovat požadavky na složitostPassword must meet complexity requirements |
| Default | NÚKIB | nastaveno |
| Zakázáno | Povoleno | *Povoleno* |

|  |
| --- |
| (002) Maximální stáří heslaMaximum Password Age |
| Default | NÚKIB | nastaveno |
| 42 | 90/730 | *90/730* |

|  |
| --- |
| (003) Minimální délka heslaMinimum Password Length |
| Default | NÚKIB | nastaveno |
| 0 | 9/12 | *9/12* |

|  |
| --- |
| (004) Minimální stáří heslaMinimum Password Age |
| Default | NÚKIB | nastaveno |
| 0 | 1 | *1* |

|  |
| --- |
| (005) Ukládat hesla pomocí reverzibilního šifrováníStore password using reversible encryption for all users in the domain |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
|  (006) Vynutit použití historie hesel Enforce Password History |
| Default | NÚKIB | nastaveno |
| 0 | 24 hesel | *24 hesel* |

Zásady uzamčení účtů

|  |
| --- |
| (007) Doba uzamčení účtuAccount Lockout Duration |
| Default | NÚKIB | nastaveno |
| Nelze použít | 0 minut | *0 minut* |

|  |
| --- |
| (008) Prahová hodnota pro uzamčení účtuAccount Lockout Threshold |
| Default | NÚKIB | nastaveno |
| 0 chybných pokusů | 3/7 chybné pokusy | *3/7* |

|  |
| --- |
| (009) Vynulovat čítač uzamčení účtu poReset account lockout counter after |
| Default | NÚKIB | nastaveno |
| Nelze použít | 60 minut | *60 minut* |

Část třetí

Místní zásady

Zásady auditu

|  |
| --- |
| (010) Auditovat používání oprávněníAudit privilege use |
| Default | NÚKIB | nastaveno |
| Bez auditování | Bez auditování | *Bez auditování* |

|  |
| --- |
| (011) Auditovat přístup k adresářové služběAudit directory service access |
| Default | NÚKIB | nastaveno |
| Bez auditování | Bez auditování | *Bez auditování* |

|  |
| --- |
| (012) Auditovat přístup k objektůmAudit object access |
| Default | NÚKIB | nastaveno |
| Bez auditování | Bez auditování | *Bez auditování* |

|  |
| --- |
| (013) Auditovat sledování procesůAudit process tracking |
| Default | NÚKIB | nastaveno |
| Bez auditování | Bez auditování | *Bez auditování* |

|  |
| --- |
| (014) Auditovat správu účtůAudit account management |
| Default | NÚKIB | nastaveno |
| Bez auditování | úspěšné pokusy,neúspěšné pokusy | *úspěšné pokusy,neúspěšné pokusy,* |

|  |
| --- |
| (015) Auditovat systémové událostiAudit system events |
| Default | NÚKIB | nastaveno |
| Bez auditování | úspěšné pokusy,neúspěšné pokusy | *úspěšné pokusy,neúspěšné pokusy,* |

|  |
| --- |
| (016) Auditovat události přihlášeníAudit logon events |
| Default | NÚKIB | nastaveno |
| Bez auditování | úspěšné pokusy,neúspěšné pokusy | *úspěšné pokusy,neúspěšné pokusy,* |

|  |
| --- |
| (017) Auditovat události přihlášení k účtuAudit account logon events |
| Default | NÚKIB | nastaveno |
| Bez auditování | úspěšné pokusy,neúspěšné pokusy | *úspěšné pokusy,neúspěšné pokusy,* |

|  |
| --- |
| (018) Auditovat změny zásadAudit policy change |
| Default | NÚKIB | nastaveno |
| Bez auditování | úspěšné pokusy,neúspěšné pokusy | *úspěšné pokusy,neúspěšné pokusy,* |

Přiřazení uživatelských práv

|  |
| --- |
| (019) Generovat audity zabezpečeníGenerate security audits |
| Default | NÚKIB | nastaveno |
| Local Service, Network Service | Local Service, Network Service | *Local Service, Network Service* |

|  |
| --- |
| (025) Obnovit soubory a adresářeRestore files and directories |
| Default | NÚKIB | nastaveno |
| Administrators,Backup Operators | Administrators | *Administrators* |

|  |
| --- |
| (026) Odepřít místní přihlášeníDeny logon locally |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Guests | *Guests* |

|  |
| --- |
| (032) Povolit místní přihlášeníAllow logon locally |
| Default | NÚKIB | nastaveno |
| Guest, Administrators, Users, Backup Operators | Administrators, Users | *Administrators, Users* |

|  |
| --- |
| (036) Provést úlohy údržby svazkuPerform volume maintenance tasks |
| Default | NÚKIB | nastaveno |
| Administrators | Administrators | *Administrators* |

|  |
| --- |
| (037) Převzít vlastnictví souborů a dalších objektůTake ownership of files or other objects |
| Default | NÚKIB | nastaveno |
| Administrators | Administrators | *Administrators* |

|  |
| --- |
| (042) Spravovat auditování a protokol zabezpečeníManage auditing and security log |
| Default | NÚKIB | nastaveno |
| Administrators | Administrators | *Administrators* |

|  |
| --- |
| (049) Vypnout systémShut down the system |
| Default | NÚKIB | nastaveno |
| Administrators,Backup Operators, Users | Administrators, Users | *Administrators, Users* |

|  |
| --- |
| (056) Zálohovat soubory a adresářeBack up files and directories |
| Default | NÚKIB | nastaveno |
| Administrators,Backup Operators | Administrators | *Administrators* |

|  |
| --- |
| (058) Změnit časové pásmoChange the time zone |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Local Service, Administrators | *Local Service, Administrators* |

|  |
| --- |
| (060) Změnit systémový čas Change the system time |
| Default | NÚKIB | nastaveno |
| Local Service, Administrators | Local Service, Administrators | *Local Service, Administrators* |

Možnosti zabezpečení

|  |
| --- |
| (063) Audit: Auditovat oprávnění k zálohování a obnovení dat Audit: Audit the use of Backup and Restore privilege |
| Default | NÚKIB | nastaveno |
| Zakázano | Zakázano | *Zakázáno* |

|  |
| --- |
| (064) Audit: Auditovat přístup globálních systémových objektůAudit: Audit the access of global system objects |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (065) Audit: Není-li možno protokolovat audity zabezpečení, vypnout okamžitě systémAudit: Shut down system immediately if unable to log security audits |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (066) Audit: Vynutit přednost nastavení podkategorie zásad auditování před nastavením kategorie zásad auditováníAudit: Force audit policy subcategory settings to override audit policy category settings |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Zakázáno(původní způsob auditování) | *Zakázáno* |

|  |
| --- |
| (073) Interaktivní přihlašování: Limit pro nečinnost počítačeInteractive logon: Machine inactivity limit |
| Default | NÚKIB | nastaveno |
| Nedefinováno | 900 s | *900 s* |

|  |
| --- |
| (076) Interaktivní přihlašování: Nadpis zprávy pro uživatele pokoušející se přihlásitInteractive logon: Message title for users attempting to log on |
| Default | NÚKIB | nastaveno |
| Blank | “Upozornění” | *„Upozornění“* |

|  |
| --- |
| (077) Interaktivní přihlašování: Nevyžadovat stisknutí kláves Ctrl+Alt+DelInteractive logon: Do not require CTRL+ALT+DEL |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (078) Interaktivní přihlašování: Nezobrazovat naposledy použité uživatelské jménoInteractive logon: Do not display last user name |
| Default | NÚKIB | nastaveno |
| Zakázáno | Povoleno | *Povoleno* |

|  |
| --- |
| (082) Interaktivní přihlašování: Text zprávy pro uživatele pokoušející se přihlásitInteractive logon: Message text for users attempting to log on |
| Default | NÚKIB | nastaveno |
| Blank | „Přihlašujete se do informačního systému nakládajícího s utajovanými informacemi podle zákona č. 412 / 2005 Sb. Nejste-li autorizováni pro práci v tomto systému, ihned se odhlaste, jinak se vystavujete možným sankcím podle tohoto zákona.“ | *Stejné jako doporučení NÚKIB* |

|  |
| --- |
| (083) Interaktivní přihlašování: Vyzvat uživatele ke změně hesla před jeho vypršenímInteractive logon: Prompt user to change password before expiration |
| Default | NÚKIB | nastaveno |
| 5 dnů | 14 dnů | *14 dnů* |

|  |
| --- |
| (084) Interaktivní přihlašování: Zobrazit informace o uživateli, pokud je relace uzamčenaInteractive logon: Display user information when the session is locked |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Zobrazované jméno uživatele, název domény a uživatelská jména | *Zobrazované jméno uživatele, název domény a uživatelská jména* |

|  |
| --- |
| (088) Konzola pro zotavení: Povolit automatické přihlášení správceRecovery console: Allow automatic administrative logon |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (089) Konzola pro zotavení: Povolit kopírování na disketu a přístup ke všem jednotkám a složkámRecovery console: Allow floppy copy and access to all drives and all folders |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (095) Nastavení systému: Volitelné podsystémySystem settings: Optional sybsystems |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Žádný | *Žádný* |

|  |
| --- |
| (110) Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro správce v Režimu schválení správceUser Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode |
| Default | NÚKIB | nastaveno |
| Vyzvat k souhlasu pro binární soubory neurčené pro systém Windows | Vyzvat k zadání souhlasu | *Vyzvat k zadání souhlasu* |

|  |
| --- |
| (111) Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro standardní uživateleUser Account Control: Behavior of the elevation prompt for standard users |
| Default | NÚKIB | nastaveno |
| Vyzvat k zadání pověření | Automaticky zamítnout požadavky na zvýšení | *Automaticky zamítnout požadavky na zvýšení* |

|  |
| --- |
| (112) Řízení uživatelských účtů: Povolit aplikacím UIAccess zobrazení výzvy ke zvýšení oprávnění bez použití zabezpečené plochyUser Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (113) Řízení uživatelských účtů: Při zobrazení výzvy ke zvýšení oprávnění přepnout na zabezpečenou plochuUser Account Control: Switch to the secure desktop when prompting for elevation |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

|  |
| --- |
| (114) Řízení uživatelských účtů: Režim schválení správce pro integrovaný účet správceUser Account control: Admin Approval Mode for the Bulit-in Administrator Account |
| Default | NÚKIB | nastaveno |
| Zakázáno | Povoleno | *Povoleno* |

|  |
| --- |
| (115) Řízení uživatelských účtů: Spustit všechny správce v Režimu schválení správceUser Account Contro: Run all administrators in Admin Approval Mode |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

|  |
| --- |
| (116) Řízení uživatelských účtů: Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelůUser Account control:Virtualize file and registry write failures to per-user locations |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

|  |
| --- |
| (117) Řízení uživatelských účtů: Zjistit instalace aplikací a zobrazit výzvu ke zvýšení oprávněníUser Account Control: Detect application installations and prompt for elevation |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

|  |
| --- |
| (118) Řízení uživatelských účtů: Zvýšit oprávnění pouze u aplikací UIAccess, které jsou nainstalovány v zabezpečených umístěníchUser Account Control: Only elevate UIAccess applications that are installed in secure locations |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

|  |
| --- |
| (119) Řízení uživatelských účtů: Zvýšit oprávnění pouze u podepsaných a ověřených spustitelných souborůUser Account Control: Only elevate executables that are signed and validated |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (128) Účty: Blokovat účty MicrosoftAccounts: Block Microsoft accounts |
| Default | NÚKIB | nastaveno |
| Nedefinováno | Uživatelé nemohou přidávat účty Microsoft ani se jejich pomocí přihlašovat | *Uživatelé nemohou přidávat účty Microsoft ani se jejich pomocí přihlašovat* |

|  |
| --- |
| (129) Účty: Omezit použití prázdného hesla místního účtu pouze pro přihlášení ke konzoleAccounts: Limit local account use of blank passwords to console logon only |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

|  |
| --- |
| (130) Účty: Přejmenovat účet GuestAccounts: Rename guest account |
| Default | NÚKIB | nastaveno |
| Guest | guest\_anonymous(nebo zvolit vlastní jméno) | *Quest\_anonymous* |

|  |
| --- |
| (131) Účty: Přejmenovat účet správceAccounts: Rename administrator account |
| Default | NÚKIB | nastaveno |
| Administrator | admin\_root (nebo zvolit vlastní jméno) | *Admin\_root* |

|  |
| --- |
| (132) Účty: Stav účtu hostaAccounts: Guest account status |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (133) Účty: Stav účtu správceAccounts: Administrator account status |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno / Povoleno | *Povoleno* |

|  |
| --- |
| (134) Vypnutí: Povolit vypnutí systému bez nutnosti přihlášeníShutdown: Allow system to be shut down without having to log on |
| Default | NÚKIB | nastaveno |
| Povoleno | Povoleno | *Povoleno* |

V souvislosti s touto zásadou je nutné nastavit tyto dvě navazující zásady:

|  |
| --- |
| Konfigurace počítače/Šablony pro správu/Systém/Řízení spotřeby/Nastavení tlačítka/Vybrat akci při stisknutí tlačítka napájení (napájení ze sítě) |
| Default | NÚKIB | nastaveno |
| Není nakonfigurováno | Povoleno(Neprovádět žádnou akci) | *Povoleno* |

|  |
| --- |
| Konfigurace počítače/Šablony pro správu/Systém/Řízení spotřeby/Nastavení tlačítka/Vybrat akci při stisknutí tlačítka napájení (napájení z baterie) |
| Default | NÚKIB | nastaveno |
| Není nakonfigurováno | Povoleno(Neprovádět žádnou akci) | *Povoleno* |

|  |
| --- |
| (135) Vypnutí: Vymazat stránkovací soubor virtuální pamětiShutdown: Clear virtual memory pagefile |
| Default | NÚKIB | nastaveno |
| Zakázáno | Zakázáno | *Zakázáno* |

|  |
| --- |
| (157) Zařízení: Zabránit uživatelům instalovat ovladače tiskárenDevices: Prevent users from installing printer drivers |
| Default | NÚKIB | nastaveno |
| Zakázáno | Povoleno | *Povoleno* |

Část čtvrtá

Služba protokolu událostí

Místní počítač – zásady / Konfigurace počítače / Šablony pro správu /

Součásti systému Windows / Služba protokolu událostí

* + 1. Aplikace

|  |
| --- |
| (L01) Řídit umístění souboru protokoluControl the location of the log file |
| Default | NÚKIB | nastaveno |
| --- | --- | *---* |

|  |
| --- |
| (L02) Zadat maximální velikost souboru protokolu (kB)Specify the maximum log file size |
| Default | NÚKIB | nastaveno |
| --- | Povoleno, 50 048 kBjako minimum | *Povoleno, 50 048 kB* |

Uvedená hodnota je nastavitelná i v aplikaci Prohlížeč událostí.

|  |
| --- |
| (L03) Automaticky zálohovat protokol při naplněníBackup up log automatically when full |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (L04) Konfigurovat přístup k protokoluConfigure log access |
| Default | NÚKIB | nastaveno |
| --- | --- | *---* |

|  |
| --- |
| (L05) Řídit chování služby Protokol událostí, když soubor protokolu dosáhne maximální velikostiControl Event Log behaviour when the log file reaches its maximum size |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

* + 1. System

|  |
| --- |
| (L06) Řídit umístění souboru protokoluControl the location of the log file |
| Default | NÚKIB | nastaveno |
| --- | --- | *---* |

|  |
| --- |
| (L07) Zadat maximální velikost souboru protokolu (kB)Specify the maximum log file size |
| Default | NÚKIB | nastaveno |
| --- | povoleno, 50 048 kBjako minimum | *Povoleno, 50 048 kB* |

Uvedená hodnota je nastavitelná i v aplikaci Prohlížeč událostí.

|  |
| --- |
| (L08) Automaticky zálohovat protokol při naplněníBackup up log automatically when full |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (L09) Konfigurovat přístup k protokoluConfigure log access |
| Default | NÚKIB | nastaveno |
| --- | --- | *---* |

|  |
| --- |
| (L10) Řídit chování služby Protokol událostí, když soubor protokolu dosáhne maximální velikostiControl Event Log behaviour when the log file reaches its maximum size |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

* + 1. Zabezpečení

|  |
| --- |
| (L11) Řídit umístění souboru protokoluControl the location of the log file |
| Default | NÚKIB | nastaveno |
| --- | --- | *---* |

|  |
| --- |
| (L12) Zadat maximální velikost souboru protokolu (kB)Specify the maximum log file size |
| Default | NÚKIB | nastaveno |
| --- | Povoleno, 100 096 kBjako minimum | *Povoleno, 100 096 kB* |

Uvedená hodnota je nastavitelná i v aplikaci Prohlížeč událostí.

|  |
| --- |
| (L13) Automaticky zálohovat protokol při naplněníBackup up log automatically when full |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (L14) Konfigurovat přístup k protokoluConfigure log access |
| Default | NÚKIB | nastaveno |
| --- | --- | *---* |

|  |
| --- |
| (L15) Řídit chování služby Protokol událostí, když soubor protokolu dosáhne maximální velikostiControl Event Log behaviour when the log file reaches its maximum size |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Část pátá

Šablony pro správu – konfigurace počítače

Místní počítač – zásady / Konfigurace počítače / Šablony pro správu

Součásti systému Windows / Možnost přihlášení k systému Windows

 Windows Components / Windows Logon Options

|  |
| --- |
| (T03) Zobrazit informace o předchozích přihlášeních během přihlášení uživateleDisplay information about previous logons during user logon |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T04) Automaticky přihlásit posledního interaktivního uživatele po restartování vyvolaném systémemSign-in last interactive user automatically after a system-initiated restart |
| Default | NÚKIB | nastaveno |
| --- | Zakázáno | *Zakázáno* |

Součásti systému Windows / OneDrive

 Windows Components / OneDrive

|  |
| --- |
| (T06) Bránit používání OneDrivu jako úložiště souborůPrevent the usage of OneDrive for file storage |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Součásti systému Windows / Uživatelské rozhraní pověření

 Windows Components / Credential User Interface

|  |
| --- |
| (T60) Zabránit použití bezpečnostních otázek pro místní účtyPrevent the use of security questions for local accounts |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Součásti systému Windows / Zásady automatického přehrávání

 Windows Components / Autoplay Policies

|  |
| --- |
| (T07) Vypnout automatické přehráváníTurn off Autoplay |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Systém / Přihlášení

 System / Logon

|  |
| --- |
| (T11) Zapnout přihlášení praktickým PIN kódemTurn on convenience PIN sign-in |
| Default | NÚKIB | nastaveno |
| --- | Zakázáno | *Zakázáno* |

|  |
| --- |
| (T12) Vypnout přihlášení pomocí obrázkového heslaTurn off picture password sign-in |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T13) Vypnout oznámení aplikací na zamykací obrazovceTurn off app notifications on the lock screen |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T14) Skrýt vstupní body pro Rychlé přepínání uživateleHide Entry points for fast user switching |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T15) Vždy použít klasické přihlašování Always use classic logon |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |
| *Tato zásada není v nových verzích již nadále podporována* |

Systém / Zásady skupiny

 System / Group Policy

|  |
| --- |
| (T17) Vypnout zpracování místních objektů Zásad skupinyTurn off Local Group Policy Objects processing |
| Default | NÚKIB | nastaveno |
| --- | Zakázáno | *Zakázáno* |

|  |
| --- |
| (T18) Vypnout protokolování výsledné sady zásadTurn off Resultant Set of Policy logging |
| Default | NÚKIB | nastaveno |
| --- | Zakázáno | *Zakázáno* |

Systém / Instalace zařízení / Omezení pro instalaci zařízení

 System / Device Installation / Device Installation Restrictions

|  |
| --- |
| (T19) Povolit správcům přepsat zásady Omezení pro instalaci zařízeníAllow administrators to override Device Installation Restriction policies |
| Default | NÚKIB | nastaveno |
| --- | Zakázáno | *Zakázáno* |

|  |
| --- |
| (T22) Zobrazit vlastní zprávu v případě, že nastavení zásad znemožní instalaciDisplay a custom message when installation is prevented by policy setting |
| Default | NÚKIB | nastaveno |
| --- | Povolit(Zadat text: Instalace nepovoleného zařízení) | *Povoleno(text: „Instalace nepovoleného zařízení“)* |

|  |
| --- |
| (T23) Zobrazit nadpis vlastní zprávy v případě, že nastavení zásad znemožní instalaci zařízeníDisplay a custom message title when installation is prevented by policy setting |
| Default | NÚKIB | nastaveno |
| --- | Povolit(Zadat titulek: Upozornění) | *Povoleno(text: „Upozornění“)* |

|  |
| --- |
| (T24) Povolit instalaci zařízení s těmito identifikačními čísly zařízení Allow installation of devices that match any of these device Ids |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Zakázáno* |

|  |
| --- |
| (T26) Zakázat instalaci vyměnitelných zařízeníPrevent installation of removable devices |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno* |

|  |
| --- |
| (T27) Zakázat instalaci zařízení nepopsaných v jiných nastaveních zásadPrevent installation of devices not described by other policy settings |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno* |

Systém / Přístup k vyměnitelnému úložišti

 System / Removable Storage Access

|  |
| --- |
| (T29) Disk CD a DVD: Odepřít oprávnění ke spouštění CD and DVD: Deny execute access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T30) Disk CD a DVD: Odepřít přístup ke čteníCD and DVD: Deny read access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno / Zakázáno* |

|  |
| --- |
| (T31) Disk CD a DVD: Odepřít přístup pro zápisCD and DVD: Deny write access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno / Zakázáno* |

|  |
| --- |
| (T34) Disketové jednotky: Odepřít oprávnění ke spouštěníFloppy Drives: Deny execute access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T35) Disketové jednotky: Odepřít přístup ke čteníFloppy Drives: Deny read access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno* |

|  |
| --- |
| (T36) Disketové jednotky: Odepřít přístup pro zápisFloppy Drives: Deny write access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno* |

|  |
| --- |
| (T37) Vyměnitelné disky: Odepřít oprávnění ke spouštěníRemovable Disks: Deny execute access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T38) Vyměnitelné disky: Odepřít přístup ke čteníRemovable Disks: Deny read access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno / Zakázáno* |

|  |
| --- |
| (T39) Vyměnitelné disky: Odepřít přístup pro zápisRemovable Disks: Deny write access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno / Zakázáno* |

|  |
| --- |
| (T40) Všechny třídy vyměnitelného úložiště: Odepřít veškerý přístup All Removable Storage classes: Deny all access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Zakázáno* |

|  |
| --- |
| (T42) Páskové jednotky: Odepřít oprávnění ke spouštěníTape Drives: Deny execute access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T43) Páskové jednotky: Odepřít přístup ke čteníTape Drives: Deny read access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno* |

|  |
| --- |
| (T44) Páskové jednotky: Odepřít přístup pro zápisTape Drives: Deny write access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno / Zakázáno(v souladu s bezpečnostní politikou IS) | *Povoleno* |

|  |
| --- |
| (T45) Zařízení WPD: Odepřít přístup ke čteníWPD Devices: Deny read access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T46) Zařízení WPD: Odepřít přístup pro zápisWPD Devices: Deny write access |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Ruční nastavení restrikcí pro USB zařízení typu Mass Storage

* + 1. Při aplikaci uvedeného postupu se použije freewarová utilita USBDeview od společnosti NirSoft (testováno s verzí USBDeview v2.75). Tato utilita poskytuje přehled o instalovaných a připojených USB zařízeních, včetně podrobných informací o jednotlivých zařízeních, jejich instalaci a posledním připojení.
		2. Uvedené nastavení operačních systémů rodiny MS Windows umožňuje připojovat do informačního systému pouze zaregistrované USB nosiče. Tento postup byl otestován i pro případ, že se jedná o zařízení stejného typu, včetně verze firmware.
		3. Postup nastavení:

zkontrolovat, že zásada (T26) Zakázat instalaci vyměnitelných zařízení je nastavena na hodnotu „Není nakonfigurováno“ nebo „Zakázáno“.

odpojit všechny USB zařízení typu Mass Storage od USB portů,

odinstalovat všechny ovladače Mass Storage zařízení. Pro odinstalaci použít freewarovou utilitu USBDeview - pravým tlačítkem myši kliknout na příslušné zařízení a v menu vybrat volbu Uninstall Selected Devices.

postupně připojit všechny evidované nosiče k USB portům (všechny, které mají být v informačním systému povoleny). Vždy počkat až proběhne instalace ovladače (nosič se načte v Průzkumníku systému Windows).

zásadu (T26) Zakázat instalaci vyměnitelných zařízení nastavit na hodnotu „Povoleno“.

Automatické nastavení restrikcí pro USB zařízení typu Mass Storage

* + 1. Nástroj AuTo4SeSe umožňuje nastavení restrikcí pro USB zařízení typu Mass Storage.
		2. Nástroj zajistí automatické odinstalování dříve použitých USB zařízení typu Mass Storage a pak umožní postupnou instalaci nových.
		3. Nástroj umožňuje i přidávání nových USB zařízení typu Mass Storage bez odinstalování již nainstalovaných.

Systém / Obnovení

 System / Recovery

|  |
| --- |
| (T47) Povolit obnovení systému do výchozího stavuAllow restore of systém to default state |
| Default | NÚKIB | nastaveno |
| --- | Zakázáno | *Zakázáno* |

Systém / Obnovení systému

 System / System Restore

|  |
| --- |
| (T48) Vypnout konfiguraciTurn off Configuration |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T49) Vypnout nástroj Obnovení systémuTurn off System Restore |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Ovládací panely / Přizpůsobení

 Control Panel / Personalization

|  |
| --- |
| (T50) Nezobrazovat zamykací obrazovku Do not display the lock screen |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T51) Bránit povolení kamery na zamykací obrazovcePrevent enabling lock screen camera |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T52) Bránit povolení prezentace na zamykací obrazovcePrevent enabling lock screen slide show |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Část šestá

Šablony pro správu – konfigurace uživatele

Místní počítač – zásady / Konfigurace uživatele / Šablony pro správu

Ovládací panely / Přizpůsobení

 Control Panel / Personalization

|  |
| --- |
| (T53) Povolit šetřič obrazovkyEnable screen saver |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T54) Zabránit změnám šetřiče obrazovkyPrevent changing screen saver |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T55) Chránit šetřič obrazovky heslemPassword protect the screen saver |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

|  |
| --- |
| (T56) Časový limit šetřiče obrazovkyScreen saver timeout |
| Default | NÚKIB | nastaveno |
| --- (0) | Povoleno 900 (15 min) | *Povoleno 900* |

|  |
| --- |
| (T57) Vynutit konkrétní šetřič obrazovkyForce specific screen saver |
| Default | NÚKIB | nastaveno |
| --- | Povoleno(Mystify.scr) | *Povoleno**(Mystify.scr)* |

Součásti systému Windows / Průzkumník Windows /

 Windows Components / File Explorer

|  |
| --- |
| (T58) Nepřesouvat odstraněné soubory do koše Do not move deleted files to the Recycle Bin |
| Default | NÚKIB | nastaveno |
| --- | Povoleno | *Povoleno* |

Část sedmá

Aktivace OS Windows 10 bez připojení k Internetu

Postup aktivace

* + 1. Pod účtem administrátora spustit příkazový řádek s administrátorským právem.
		2. Přesunout se do podadresáře C:\Windows\System32.
		3. Spustit příkaz **cscript slmgr.vbs /dti > C:\ID.txt**.
		4. Instalační číslo ID (63 číslic) se nachází v textovém souboru ID.TXT. Rozdělit číslo do 9 skupin po 7 číslicích.
		5. Zavolat na telefonní číslo Microsoft Product Activation Center (**800 100 074** nebo **225 990 844**).
		6. Následovat instrukce a poskytnout instalační číslo ID (63 číslic) po jednotlivých skupinách.
		7. Zapsat si potvrzovací ID číslo poskytnuté telefonním aktivačním systémem (48 číslic bez mezer).
		8. Spustit příkaz **cscript slmgr.vbs /atp potvrzovací\_ID**. Jestliže se zobrazí kód chyby **0x2a 0xC004F04D** pak instalační ID neodpovídá potvrzovacímu ID.
		9. Spustit příkaz **cscript slmgr.vbs /dlv**.
		10. Zkontrolovat, zda je **Stav licence** rovný hodnotě **Licencováno**.

Část osmá

Aktualizace OS Windows 10 bez připojení k Internetu

Příprava aktualizačního média

* + 1. Stáhnout nástroje MediaCreationTool z webového serveru Microsoftu
		2. Spustit nástroje MediaCreationTool pod účtem administrátora
		3. Odsouhlasit licenční podmínky.
		4. V menu „Co chcete udělat“ zvolit „**Vytvořit instalační média pro jiný počítač**“
		5. V menu „Vyberte jazyk, architekturu a edici“ zvolit **jazyk čeština**, **edice Windows 10**, **architektura** **32 bitů (x86)** nebo **64 bitů (x64)**.
		6. V menu „Zvolte médium, které chcete použít“ zvolit **USB flash disk** nebo **soubor ISO**.
		7. V případě USB flash disku vybrat USB flash disk (Vybrat ze seznamu), po vytvoření instalačního USB flash disku stisknout volbu Dokončit.
		8. V případě souboru ISO určit umístění souboru a po vytvoření souboru lze ISO soubor vypálit na DVD.
		9. Odstranění předchozí verze Windows 10

Deset dnů po upgradování na Windows 10 se vaše předchozí verze Windows automaticky odstraní z vašeho počítače. Pokud ale potřebujete uvolnit místo na disku a víte, že máte soubory a nastavení tam, kde je ve Windows 10 chcete mít, můžete ji bezpečně odstranit sami. Upozorňujeme, že odstraníte složku Windows.old, která obsahuje soubory umožňující vrátit se k předchozí verzi Windows. Odstranění předchozí verze Windows je nevratné.

* Do vyhledávacího pole na hlavním panelu napište nastavení a pak ho zvolte ze seznamu výsledků.
* Vyberte Systém > Úložiště > a potom v seznamu přejděte dolů a zvolte Dočasné soubory.

V části Odebrat dočasné soubory zaškrtněte políčko Předchozí verze Windows a potom vyberte Odebrat soubory. Odkaz na nastavení: ms-settings:storagesense

Vlastní aktualizace OS Windows 10 pomocí DVD

* + 1. Spustit počítač a vložit instalační DVD.
		2. Spustit soubor setup.exe s oprávněním správce z instalačního DVD.
		3. V menu „Získat důležité aktualizace“ zvolit **Stáhnout a nainstalovat aktualizace**.
		4. Odsouhlasit licenční podmínky.
		5. V menu „Připraveno k instalaci“ zvolit **Nainstalovat** (zachovat osobní soubory a aplikace) nebo volbou **Změnit co se má zachovat** provést upřesnění postupu.
		6. Vyčkat do ukončení instalačního procesu.

Vlastní aktualizace OS Windows 10 pomocí USB flash disku

* + 1. Spustit počítač a připojit instalační USB flash disk.
		2. Spustit soubor setup.exe s oprávněním správce u instalačního USB flash disku.
		3. V menu „Získat důležité aktualizace“ zvolit **Stáhnout a nainstalovat aktualizace**.
		4. Odsouhlasit licenční podmínky.
		5. V menu „Připraveno k instalaci“ zvolte **Nainstalovat** (zachovat osobní soubory a aplikace) nebo volbou **Změnit co se má zachovat** provést upřesnění postupu.
		6. Vyčkat do ukončení instalačního procesu.

SMĚRNICE BEZPEČNOSTNÍHO SPRÁVCE

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

Úvodní ustanovení

* + 1. Směrnice bezpečnostního správce popisuje jednotlivé činnosti výkonu bezpečnostní správy informačního systému s odkazy na kapitolu „Popis bezpečnosti“.
		2. Bezpečnostní správce je zaměstnanec splňující podmínky přístupu k utajované informaci minimálně stupně utajení Vyhrazené, který je písemně pověřen oprávněnou osobou nebo jí pověřenou osobou a který vykonává správu bezpečnosti informačního systému.
		3. Pověření do role bezpečnostního správce slouží zároveň jako pověření do role uživatele.

Povinnosti bezpečnostního správce

* + 1. Bezpečnostní správce odpovídá za dodržování bezpečnostních opatření definovaných v kapitole popisu bezpečnosti.
		2. Bezpečnostní správce:

připravuje, spravuje a aktualizuje provozní a provozně bezpečnostní dokumentaci informačního systému (č. 25 odst. 2),

vede evidenci nosičů informací (čl. 23 odst. 1 a 2),

vede evidenci pověřených uživatelů, provádí jejich školení (čl. 5 odst. 6), zajišťuje vytváření, správu a rušení uživatelských účtů v informačním systému,

zajišťuje označení a evidenci HW komponent pracoviště (čl. 19 odst. 1 a 2),

zajišťuje opatření HW komponent pracoviště ochrannými prvky (čl. 20 odst. 1 a 2),

zajišťuje nastavení bezpečnostních parametrů BIOS/UEFI v souladu s požadavky NÚKIB a dokumentem „Bezpečnostní nastavení BIOS/UEFI“,

zajišťuje nastavení bezpečnostních mechanismů operačního systému v souladu s kapitolami „Výsledky analýzy rizik“, „Popis bezpečnosti“ a „Bezpečnostních nastavení operačního systému MS Windows“,

před uvedením pracoviště do provozu provádí test bezpečnosti, aby ověřil, zda jsou bezpečnostní mechanismy aplikovány správně (čl. 29 odst. 1),

účastní se případné obhlídky pracoviště prováděné pracovníkem NÚKIB před ukončením certifikace,

zaznamenává veškerou svou činnost na pracovišti do „Provozního deníku pracoviště“,

kontroluje dodržování režimových opatření a bezpečnostních opatření,

zajišťuje nebo provádí aktualizaci virových řetězců, a to v intervalu 1x měsíčně, nebo v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací (čl. 12 odst. 1 a 2),

zajišťuje nebo provádí archivaci auditních záznamů, a to v intervalu 1x měsíčně, nebo v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací (čl. 9 odst. 2),

provádí kontrolu auditních záznamů, za účelem identifikace případných bezpečnostních incidentů,

účastní se řešení vzniklých krizových situací a bezpečnostních incidentů (čl. 27),

cestou odpovědné osoby nebo jí pověřené osoby hlásí NÚKIB veškeré změny při provozování pracoviště (čl. 28)

zajišťuje mazání a likvidaci nosičů informací (čl. 11 a 24),

přijímá, v rámci svých možností, taková opatření, aby zajistil požadovanou dostupnost,

podílí se v rámci svých možností na údržbě a opravách komponent informačního systému.

SMĚRNICE PROVOZNÍHO SPRÁVCE

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

Úvodní ustanovení

* + 1. Směrnice provozního správce popisuje jednotlivé činnosti výkonu provozní správy informačního systému.
		2. Provozní správce je zaměstnanec splňující podmínky přístupu k utajované informaci minimálně stupně utajení Vyhrazené, který je písemně pověřen oprávněnou osobou nebo jí pověřenou osobou a vykonává provozní správu informačního systému.
		3. Pověření do role provozního správce slouží zároveň jako pověření do role uživatele.

Povinnosti provozního správce

* + 1. Provozní správce odpovídá za správnou instalaci operačního systému a aplikačního SW.
		2. Provozní správce:

dokládá bezpečnostnímu správci údaje o instalovaném SW a HW jako podklad pro vyplnění „Specifikačního listu pracoviště“,

zaznamenává veškerou svou činnost na pracovišti do „Provozního deníku pracoviště“,

provádí aktualizaci virových řetězců, a to v intervalu 1x měsíčně, nebo v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací (čl. 12 odst. 1 a 2),

provádí archivaci auditních záznamů, a to v intervalu 1x měsíčně, nebo v případě nevyužívání pracoviště po delší časové období, vždy před započetím zpracování utajovaných informací (čl. 9 odst. 2),

je nápomocen při řešení vzniklých krizových situací a bezpečnostních incidentů (čl. 27),

přijímá, v rámci svých možností, taková opatření, aby zajistil požadovanou dostupnost,

zajišťuje a provádí údržbu a opravy komponent informačního systému,

spolupracuje s bezpečnostním správcem.

SMĚRNICE UŽIVATELE

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

Úvodní ustanovení

* + 1. Tato směrnice uživatele popisuje základní povinnosti uživatelů při práci v informačním systému.
		2. Uživatel musí splňovat podmínky přístupu k utajované informaci minimálně stupně utajení Vyhrazené, musí být písemně pověřen oprávněnou osobou nebo jí pověřenou osobou a musí být proškolen bezpečnostním správcem.

Povinnosti uživatele

* + 1. Uživatel při práci na pracovišti informačního systému odpovídá za dodržování zákonných pravidel při zpracování utajovaných informací.
		2. Uživatel při své práci na pracovišti informačního systému dodržuje režimová opatření stanovená v platném projektu fyzické bezpečnosti.
		3. Uživatel je povinen:

řídit se zejména touto směrnicí a pokyny bezpečnostního správce,

před započetím práce provést kontrolu neporušenosti ochranných prvků,

identifikovat a autentizovat se pomocí svého platného přístupového jména a hesla (viz článek 4),

při přerušení práce na dobu kratší než 30 minut zamknout pracovní stanici (klávesami Ctrl + Alt + Delete) a zajistit pracoviště před vstupem neoprávněných osob,

při ukončení práce nebo při jejím přerušení na dobu delší než 30 minut ukončit provozované aplikace, vypnout síťové vypínače sestavy (včetně tiskárny) a zabezpečit zpracované dokumenty a vyjímatelné nosiče informací,

zajišťovat bezpečnost zpracovávaných utajovaných informací z hlediska administrativní bezpečnosti,

používat pouze evidované nosiče informací,

hlásit neprodleně bezpečnostnímu správci každé podezření na neoprávněnou manipulaci s daty, uživatelským účtem nebo sestavou,

hlásit neprodleně bezpečnostnímu správci jakékoliv hlášení antivirového softwaru o detekci viru nebo jiného škodlivého SW,

používat pouze SW nainstalovaný bezpečnostním správcem,

neprodleně hlásit všechny HW a SW poruchy bezpečnostnímu správci,

bezodkladně informovat bezpečnostního správce o zjištění krizové situace nebo bezpečnostního incidentu a dále nepokračovat v práci (viz článek 5).

Zakázané činnosti uživatele

* + 1. Uživateli je při používání pracoviště zakázáno:

provádět na sestavě jinou činnost než tu, kterou má povolenu a která vyplývá z jeho pracovních povinností,

používat přístupová práva, která mu nebyla přidělena,

používat neevidované nosiče informací,

spouštět na pracovní stanici SW, který nebyl schválen bezpečnostním správcem,

modifikovat SW (instalovat, vymazávat) pracovní stanice,

modifikovat HW (vkládat, vyjímat HW komponenty) sestavy,

přistupovat k datům jiných uživatelů nebo aplikacím, ke kterým nemá povolen přístup,

vypínat, odinstalovat nebo modifikovat nastavení antivirového SW,

provádět neoprávněné kopie dat.

Přístupové heslo

* + 1. Přístupové heslo:

musí být chráněno, jako utajovaná informace stupně utajení Vyhrazené,

musí obsahovat minimálně 9 nebo 12 znaků (podle zvolené varianty),

musí obsahovat min. 3 typy znaků (malá písmena, velká písmena, číslice nebo speciální znaky)

musí být určeno uživatelem,

nesmí obsahovat přihlašovací jméno uživatele ani ve změněné formě,

nesmí být odvozeno ze jmen příbuzných nebo známých uživatele,

nesmí být odvozeno ze žádné informace, která má vztah k uživateli (číslo vozu, telefonní číslo, osobní číslo, značka auta, jméno ulice atd.),

nesmí být použito v jiném informačním systému,

nesmí být sdíleno s jiným uživatelem,

nesmí být snadno zapamatovatelné,

je platné max. 90 nebo 730 dnů (podle zvolené varianty).

* + 1. Uživatel je odpovědný za jakékoli zneužití svého účtu třetí osobou, pokud prokazatelně k zneužití účtu došlo v důsledku jeho nedbalosti, anebo nedodržením ustanovení vnitřních předpisů upravujících bezpečnost utajovaných informací.

Krizové situace a bezpečnostní incidenty

* + 1. Za krizovou situaci se považuje porucha zařízení, požár nebo jiná živelní pohroma, teroristický útok nebo jeho hrozba.
		2. V případě vzniku krizové situace musí uživatel zajistit, aby nedošlo k porušení povinnosti při ochraně utajované informace zejména, aby se neoprávněné osoby nemohly seznámit s utajovanými informacemi. Ukončí práci na sestavě, a pokud to okolnosti dovolí, vyjme z pracovní stanice vyjímatelné nosiče informací, odebere z tiskárny všechny listy vytištěných dokumentů, zamkne pracoviště a dále se řídí příslušnými směrnicemi objektu.
		3. V případě požáru uživatel odpojí sestavu od síťového napájení, pokud možno vyjme z pracovní stanice vyjímatelné nosiče informací, odebere z tiskárny všechny listy vytištěných dokumentů, za které odpovídá a dále se řídí příslušnou požární směrnicí objektu.
		4. Bezpečnostní incident je událost, která měla nebo může mít za následek ohrožení bezpečnosti nebo porušení povinnosti při ochraně utajované informace.
		5. Za bezpečnostní incident se považuje zejména:

porušení některého z bezpečnostních mechanismů,

porušení ochranných prvků,

ztráta nebo neoprávněné nakládání s nosičem utajovaných informací,

ztráta HW komponenty,

porucha HW nebo SW,

výskyt viru nebo jiného škodlivého SW,

vyzrazení přístupového hesla,

porušení platných bezpečnostních směrnic,

další události, které mohou mít vliv na bezpečnost zpracovávaných utajovaných informací.

* + 1. Uživatel bezodkladně informuje bezpečnostního správce o zjištění krizové situace nebo bezpečnostního incidentu a dále nepokračuje v práci. Bezpečnostní správce rozhodne o dalším postupu.

Ukládání a manipulace s vyjímatelnými nosiči utajovaných informací nebo s přenosným PC

* + 1. Vyjímatelné nosiče utajovaných informací nebo přenosné PC se ukládají do příslušného úschovného objektu v zabezpečené oblasti příslušné kategorie.
		2. Před započetím práce si uživatel vyzvedne vyjímatelné nosiče utajovaných informací nebo přenosné PC proti podpisu u bezpečnostního správce.
		3. Po ukončení práce uživatel odevzdá vyjímatelné nosiče utajovaných informací nebo přenosné PC proti podpisu bezpečnostnímu správci, který zajistí jejich uložení.
1. ) zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. [↑](#footnote-ref-1)
2. ) vyhláška č. 479/2024 Sb., o informační bezpečnosti. [↑](#footnote-ref-2)
3. ) § 2 písm. d) zákona č. 412/2005 Sb. [↑](#footnote-ref-3)
4. ) § 19 odst. 4 a 5 vyhlášky č. 479/2024 Sb., [↑](#footnote-ref-4)
5. ) zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. [↑](#footnote-ref-5)
6. ) vyhláška č. 479/2024 Sb., o informační bezpečnosti. [↑](#footnote-ref-6)
7. ) § 6 vyhlášky č. 479/2024 Sb. [↑](#footnote-ref-7)
8. ) § 19 odst. 4 a 5 vyhlášky č. 479/2024 Sb., [↑](#footnote-ref-8)
9. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů [↑](#footnote-ref-9)
10. Odst. 3 § 3 vyhlášky č. 528/2005 Sb. [↑](#footnote-ref-10)
11. Odst. 4 § 3 vyhlášky č. 528/2005 Sb. [↑](#footnote-ref-11)
12. § 18 vyhlášky č. 479/2024 Sb., o informační bezpečnosti [↑](#footnote-ref-12)
13. § 13 odst. 2 vyhlášky č. 479/2024 Sb. [↑](#footnote-ref-13)