Česká agentura pro standardizaci, státní příspěvková organizace, IČO: 06578705

se sídlem Biskupský dvůr 1148/5, Praha 1, PSČ 110 00

Provozní řád

Atestačního střediska pro elektronické systémy spisové služby

Část 3

Bezpečnostní politika Atestačního střediska

Verze: 1.1

Datum vydání: 21. 11. 2023

Datum účinnosti: 27. 11. 2023

Počet stran: 11

Nahrazuje: Provozní řád Atestačního střediska pro elektronické systémy spisové služby - Část 3: Bezpečnostní politika Atestačního střediska, verze 1.0

Bezpečnostní klasifikace: Veřejný dokument

Tento dokument je částí Provozního řádu Atestačního střediska zveřejněného na Internetových stránkách Atestačního střediska www.agentura-cas.cz/atestace

Vypracoval	**Datum:** 21. 11. 2023	**Jaromír Tvrzník** Bezpečnostní expert pro oblast kybernetické bezpečnosti
Schválil	**Datum:** 24. 11. 2023	**Zdeněk Veselý** Generální ředitel České agentury pro standardizaci

Seznam změn a revizí

Verze	Datum vydání	Charakter změny / revize	Datum účinnosti	Vypracoval Schválil
1.0	30. 6. 2023	Iniciální verze	1. 7. 2023	Jaromír Tvrzník Zdeněk Veselý
1.1	21. 11. 2023	Formální úpravy	27. 11. 2023	Jaromír Tvrzník Zdeněk Veselý

Obsah

1 Úvod

1.1 Účel Bezpečnostní politiky Atestačního střediska

Předložený dokument *„Provozní řád Atestačního střediska – Část 1: Metodika přípravy Atestačního prostředí“* je částí Provozního řádu Atestačního střediska vydaného na základě čl. 2 odst. 5 dokumentu *„Postup atestačního střediska pro elektronické systémy spisové služby při provádění atestace elektronického systému spisové služby, podmínky provádění atestace a výše úplaty za provedení atestace“* zveřejněného ve Věstníku MV čá. 10/2023 (dále jen dokument *„Postup Atestačního střediska“*) a dostupného též na Internetových stránkách Atestačního střediska v sekci *Důležité dokumenty a odkazy*.

Předložený dokument stanovuje závazné zásady, pravidla, požadavky a postupy řízení informační bezpečnosti, jejichž cílem je chránit prostředky Atestačního střediska, všech primárních a podpůrných aktiv, především informací v ukládaných nebo zpracovávaných Atestačním střediskem tak, aby byla zajištěna jejich důvěrnost, dostupnost a integrita, a to s ohledem na relevantní legislativní a organizační bezpečnostní požadavky.

Předložený dokument definuje požadavky na ochranu informací, a to v jakékoli podobě: mluvené, elektronické i papírové. Pod pojmem „informace“ jsou v rámci tohoto dokumentu chápána také data včetně jejich identifikačních údajů, například eSSL instalovaný na Atestační prostředí, zálohy tohoto systému / prostředí, přístupové certifikáty, údaje předávané mezi Objednatelem atestace a Atestačním střediskem apod.

1.2 Závaznost Bezpečnostní politiky Atestačního střediska

Bezpečnostní politika je (stejně jako celý Provozní řád, jehož je součástí) pro Objednatele závazná po celou dobu provádění atestace, od podání objednávky po obdržení výsledku atestace.

Předložený dokument je obsahově zaměřen na případy atestací, pro které byla zvolena varianta A) podle čl. 5 dokumentu *„Postup Atestačního střediska“,* tedy případy, kdy serverová část eSSL i Stanice pro klientské operace jsou instalovány a provozovány v rámci Atestačního prostředí realizovaného ve virtualizovaném hardwarovém prostředí Atestačního střediska.

Pokud byla pro provedení atestace zvolena varianta B) nebo C) podle čl. 5 dokumentu *„Postup Atestačního střediska“*, uplatní Objednatel atestace bezpečnostní zásady uvedené v tomto dokumentu přiměřeně. Objednatel plně odpovídá za technická opatření spojená s provozem eSSL v prostředí Objednatele. Atestační středisko nezodpovídá za nastavení bezpečnostních politik a technická opatření v prostředí Objednatele.

1.3 Související dokumenty

Pro správné pochopení textu předloženého dokumentu se Objednatel musí seznámit s dokumentem *„Vymezení použitých pojmů a zkratek“*, dostupným na internetových stránkách Atestačního střediska v sekci *Provozní řád*. Pojmy a zkratky uvedené v tomto dokumentu jsou používány ve všech částech Provozního řádu a související dokumentaci.

Objednatel je povinen seznámit se a řídit se následujícími dokumenty:

- *„Postup Atestačního střediska“ pro elektronické systémy spisové služby při provádění atestace elektronického systému spisové služby, podmínky provádění atestace a výše úplaty za provedení atestace* zveřejněný ve Věstníku MV čá. 10/2023
  (https://www.mvcr.cz/clanek/atestace-elektronickych-systemu-spisovych-sluzeb.aspx)

- *Provozní řád Atestačního střediska*
  Dostupný na internetových stránkách Atestačního střediska v sekci Provozní řád.
  Pozn.: Předložený dokument Metodika přípravy Atestačního prostředí je jednou ze tří částí Provozního řádu.

- *Formuláře pro atestace a doporučení pro jejich vyplnění*
  Závazné vzory formulářů jsou dostupné na internetových stránkách Atestačního střediska v sekci Formuláře pro atestace.

- *Provozní řád ISZR, Podmínky připojení AIS k ISZR, Příručka pro správce AIS a SSVÚ - připojení k základním registrům a související dokumenty*
  Dostupné na adrese https://www.szrcr.cz/cs/dulezite-dokumenty/

- *Provozní řád ISDS, Bezpečnostní upozornění pro uživatele datových schránek, dokumenty ze skupiny „Technické požadavky“*
  Dostupné na adrese https://info.mojedatovaschranka.cz/info/cs/80.html
  (https://info.mojedatovaschranka.cz/info/cs/ → položka menu DŮLEŽITÉ INFORMACE)

2 Cíl bezpečnosti Atestačního střediska

2.1 Ochrana aktiv s ohledem na kontinuitu činností Atestačního střediska

V rámci zajištění kontinuity činností Atestačního střediska je nezbytné software, hardware a zejména pak informační aktiva Atestačního střediska chránit tak, aby bylo minimalizováno riziko ohrožení jejich důvěrnosti, dostupnosti či integrity.

Požadované je rovněž řízení přístupu se zajištěním nepopiratelnosti při práci s aktivy takovým způsobem, aby veškerá aktiva byla využívána pouze oprávněnými uživateli, a to k účelům souvisejícím s plněním atestačních služeb. Míra ochrany daných aktiv musí být přímo úměrná jejich relativní hodnotě, úrovni předpokládaných hrozeb, kterým jsou vystavena, jejich zranitelnosti a výši rizika.

2.2 Soulad s právními normami a závazky

Kromě požadavků stanovených Provozním řádem jsou povinnosti Objednatele atestace upraveny právními normami. Z pohledu Atestačního střediska je nutné tyto normy a závazky brát v potaz při sběru, zpracování, uchovávání a distribuci informací v rámci Atestačního střediska. V opačném případě hrozí:

- poškození zaměstnanců Agentury (např. únikem osobních údajů);
- poškození dodavatelů / partnerů Atestačního střediska (např. únikem obchodního tajemství);
- poškození objednatelů (např. únikem obchodního tajemství, know-how Objednatele atestace či nekvalitně provedenou službou atestace s přímým finančním dopadem);
- poškození Atestačního střediska nebo Agentury (např. únikem obchodního tajemství);
- jiné porušení právní normy / smluvního závazku (např. autorského zákona apod.).

2.3 Strategie bezpečnosti Atestačního střediska

Strategie řízení bezpečnosti Atestačního střediska a na něj působících rizik se s ohledem na dané skutečnosti skládá z řízení rizik a dalších klíčových sub-procesů, kterými jsou pravidelná údržba, sledování aktivit uživatelů a správců, monitoring provozu Atestačního střediska, vyhodnocování logů, testování a eliminace zranitelností, zajištění obnovitelnosti, zpracování a evidence bezpečnostních incidentů.

2.4 Životní cyklus řízení bezpečnosti Atestačního střediska

Systém řízení bezpečnosti je proces, který podléhá neustálé kontrole a zlepšování. Tyto změny se dějí v cyklu (v tzv. PDCA cyklu), který se skládá z následujících aktivit:

a) Plánování

Přípravná fáze, definice strategické části bezpečnostní politiky, schválení této politiky Generálním ředitelem Agentury. Dále pak analýza rizik, návrh preventivních protiopatření, návrh opatření pro detekci a reakci na bezpečnostní incidenty.

b) Implementace

Zavedení protiopatření z předchozí fáze.

c) Kontrola

Audit a kontrola fází plánování i implementace, vyhodnocení, zda splňuje zadání vyplývající ze strategické části bezpečnostní politiky. Vyšetřování bezpečnostních incidentů.

d) Revize

Návrh na zlepšení bezpečnosti Atestačního střediska na základě fáze kontroly.

3 Oblast platnosti (rozsah)

Tato kapitola definuje aktiva spojená s Atestačním střediskem, na které se vztahuje řízení bezpečnosti informací a dále upravuje závazky ve vztahu ke Objednatelům.

3.1 Vymezení hranic Atestačního střediska

Hranice Atestačního střediska jsou určeny rozsahem, který pokrývá celý systém pro atestaci eSSL, všechna podpůrná a primární aktiva (fyzická i virtuální). Netýká se systémů Objednatele, pokud nejsou součástí Atestačního prostředí. Součástí jsou zejména všechny komunikační a výpočetní prostředky zapojené do dedikované interní sítě pro provoz Atestačního střediska (virtualizované hardwarové prostředí Atestačního střediska), jakož i mobilní prostředky výpočetní techniky, jež jsou do této dedikované sítě zapojovány a data v elektronické podobě na nich uložená nebo jejich prostřednictvím přenášená. Vztahuje se na všechny komponenty takto vymezeného informačního systému (hardware, software i případně listinné dokumenty), organizaci správy, provozu a zabezpečení síťové a datové infrastruktury, i na služby, které tato část informačního systému zajišťuje vlastními prostředky nebo prostřednictvím dodavatele.

Rozsah Atestačního střediska nezahrnuje výpočetní prostředí Objednatele. Toto je podstatné především ohledně možnosti provedení atestace prostřednictvím volby varianty B) nebo C) podle čl. 5 dokumentu *„Postup Atestačního střediska“.* Z technického pohledu zahrnuje rozsah Atestačního střediska pouze virtualizované hardwarové prostředí Atestačního střediska.

4 Klasifikace informací

4.1 Kritéria pro zařazování informací do skupin

4.1.1 Důvěrné

Důvěrné informace jsou určeny pro použití uvnitř Atestačního střediska a Objednatelem atestace v rozsahu potřebném pro přípravu atestace, popř. úzkému okruhu externistů (dodavatelů) se schváleným přístupem k těmto informacím. Jejich neoprávněné odhalení, zveřejnění nebo zničení může mít nepříznivý vliv na Atestační středisko, zaměstnance, obchodní partnery nebo Objednatele.

Jedná se o informace, jejichž zničení, vyzrazení (únik) nebo pozměnění znamená zhoršení schopnosti plnit základní cíle atestací nebo porušení obecně platného předpisu, zákona či normy nebo dokonce ohrožení Agentury nebo Objednatelů, zejména v oblasti obchodních aktivit.

Jedná se například o samotný instalovaný eSSL, zálohy Atestačního prostředí, dokumenty a data dokládající průběh atestace před jeho zveřejněním apod.

Označení

Důvěrné informace se neoznačují. Všechny neoznačené informace se pokládají za důvěrné, pokud zákonné požadavky nebo dokument *Postupy Atestačního střediska* nenařizuje jinak.

Omezení distribuce

Distribuce důvěrných informací je omezená na Objednatele a jednotlivé zaměstnance/externí partnery, kteří tyto údaje nezbytně potřebují k výkonu své práce, případně na velmi úzké skupiny speciálně vybíraných a proškolovaných zaměstnanců nebo externích partnerů.

Každému příjemci jsou přidělována co nejnižší přístupová práva v souvislosti s jeho požadavky na data potřebná k výkonu jeho práce.

Bezpečnostní opatření

Při práci s těmito informacemi je třeba dodržovat následující bezpečnostní opatření:

- Přístup k těmto informacím jen na základě průkazné autentizace.
- Důvěrné dokumenty v listinné podobě musí být uchovávány v uzamykatelných skříních nebo v uzamykatelných místnostech, kam má přístup pouze omezené množství osob. Zasílání listinných dokumentů musí být uskutečněno pouze doporučenou formou do vlastních rukou adresáta.
- Použití bezpečných způsobů doručení, které zajistí úplné a důvěrné doručení.
- Pokud je nutné tyto informace odesílat e-mailem, je doporučeno využívat šifrování, např. prostřednictvím zaheslovaného ZIP souboru. Heslo musí být doručeno jiným kanálem, např. zasláním SMS.
- Pokud je nutné tyto informace předat na přenosném médiu (např. USB flash disk, CD/DVD), je nutné zajistit úplné a důvěrné doručení do vlastních rukou adresáta s upozorněním na klasifikaci předaných informací.
- Ústní předávání těchto informací pouze na základě pracovních potřeb a zdůraznění stupně klasifikace těchto informací.
- Zajištění šifrování dat na nosičích těchto informací. Výjimkou jsou pouze listinné dokumenty.
- Bezpečná likvidace nosičů těchto informací. Data v listinné podobě jsou na konci jejich životního cyklu skartována. Pevné disky a další paměťová média musí být zlikvidována podle bezpečnostních zásad Agentury.

4.1.2 Veřejné

Veřejné informace jsou veškeré informace, se kterými se příjemci mohou setkat při výkonu své práce a které nejsou zařazeny do kategorie důvěrné a dále takové dokumenty, ze kterých je evidentní, že jsou určeny ke zveřejnění. Veřejnými jsou např.:

- provozní řád Atestačního střediska včetně příloh;
- vzory formulářů;
- informace o provedených atestacích podle dokumentu *„Postup Atestačního střediska“;*
- informace volně dostupné veřejnosti, např. související s marketingem a propagací;
- další informace a dokumenty zveřejněné na Internetových stránkách Atestačního střediska;
- informace a dokumenty, jejichž zveřejnění ukládá právní předpis.

Veřejné informace v písemné formě mohou být volně uloženy v nezabezpečených složkách apod. Rovněž mohou být zveřejněny na internetu.

Označení

Označení textem „Veřejný dokument“ na první straně nebo v záhlaví/zápatí dokumentu. Za označení dokumentu odpovídá vždy osoba, která má za dokument odpovědnost či jej vytvořila. Pokud to charakter informace neumožnuje, je označení realizováno obdobným způsobem např. na úrovni metadat nebo v názvu souboru.

V případě předávání veřejných informací v elektronické podobě mimo Atestační středisko (zákazníkům, partnerům) je doporučen needitovatelný formát dokumentu (např. PDF).

Bezpečnostní opatření

Žádná bezpečnostní opatření zde nejsou uplatňována.

5 Zabezpečení proti škodlivému softwaru

Pokud byla pro provedení atestace zvolena varianta A) podle čl. 5 dokumentu *„Postup Atestačního střediska“*, musí být všechny servery a pracovní stanice obsahující operační systém Windows zabezpečeny vhodným antivirovým programem proti škodlivému softwaru (viry, spyware). Aktualizace tohoto software a virové databáze musí být prováděna automaticky. Minimálně 1x týdně musí být spuštěn kompletní test proti škodlivému softwaru (viry, spyware). Uživatelům (včetně Objednatelů) je zakázáno jakkoliv měnit nastavení, případně vypínat antivirovou ochranu. Uživatel je povinen v případě výskytu neznámých nebo nesrozumitelných jevů (např. na monitoru) okamžitě přerušit práci a nahlásit tuto skutečnost prostřednictvím e-mailu nebo datové schránky Agentuře prostřednictvím formuláře *„Žádost o technickou pomoc při přípravě Atestačního prostředí“*, jehož závazný vzor je zveřejněn na Internetových stránkách Atestačního střediska v sekci *Formuláře pro atestace*.

Pokud byla pro provedení atestace zvolena varianta B) nebo C) podle čl. 5 dokumentu *„Postup Atestačního střediska“*, je Objednatel povinen dodržovat všechny zásady kybernetické bezpečnosti a nese plnou odpovědnost za kybernetickou bezpečnost jím provozovaného prostředí včetně dodržení podmínek stanovených v provozních řádech a související dokumentaci ISZR a ISDS.

6 Uživatelské povinnosti

Všichni uživatelé i správci jsou povinni se při zacházení s informacemi řídit pravidly týkajícími se klasifikace informací a zároveň jsou povinni dodržovat pravidla pro nakládání s klasifikovanými informacemi. Pokud byla pro provedení atestace zvolena varianta B) nebo C) podle čl. 5 dokumentu *„Postup Atestačního střediska“*, musí Objednatel v maximální možné míře respektovat pravidla uvedená v této politice podle technických možností použitého řešení. Objednatel je zároveň povinen dodržovat bezpečnostní pravidla nutná pro propojení s ISZR a ISDS, uvedená v dokumentech odkazovaných v bodě 1.3 „*Související dokumenty*“.

6.1 Přístup do Atestačního prostředí

Objednatel v průběhu instalace eSSL přistupuje k virtualizovanému hardwarovému prostředí Atestačního střediska prostřednictvím připojení přes VPN; údaje k tomuto připojení obdrží od Atestačního střediska.

Rozsah přístupových oprávnění (to, které části Atestačního střediska a na jaké úrovni bude Objednatel schopen využívat) je stanoven ze strany Atestačního střediska na základě údajů uvedených v příloze Objednávky atestace. Toto se týká i volby varianty A), B) nebo C) podle čl. 5 dokumentu *„Postup*

Atestačního střediska“, která rozhoduje o rozsahu instalace testovaného eSSL ve virtualizovaném hardwarovém prostředí Atestačního střediska.

Pokud byla pro provedení atestace zvolena varianta A) podle čl. 5 dokumentu „*Postup Atestačního střediska“*, je celé Atestační prostředí umístěno a provozováno Atestačním střediskem na virtualizovaném hardwarovém prostředí Atestačního střediska a Objednatel do něj instaluje jak serverovou část testovaného eSSL, tak i jeho klientskou část (Stanici pro klientské operace).

Pokud byla pro provedení atestace zvolena varianta B) nebo C) podle čl. 5 dokumentu „*Postup Atestačního střediska“*, je Atestační prostředí rozděleno na část poskytovanou a provozovanou Objednatelem, do které Objednatel instaluje serverovou část testovaného eSSL, a část poskytovanou Atestačním střediskem (Interní Atestační prostředí), do které Objednatel instaluje klientskou část testovaného eSSL (Stanici pro klientské operace).

V obou případech tedy Objednatel musí mít zřízen přístup do virtualizovaného hardwarového prostředí Atestačního střediska; výše uvedené varianty se však liší rozsahem tohoto přístupu.

Pro vytvoření přístupu do virtualizovaného hardwarového prostředí Atestačního střediska je Objednatel povinen stanovit osoby zastávající roli Zástupce Objednatele ve věcech technických a poskytnout Atestačnímu středisku osobní údaje těchto osob v rozsahu definovaném formulářem *„Poskytnutí informací Objednatele k vytvoření Atestačního prostředí“* v souladu s bodem 5.1 *„Zřízení přístupu Objednatele do virtualizovaného hardwarového prostředí Atestačního střediska“* dokumentu *„Provozní řád Atestačního střediska – Část 1: Metodika přípravy Atestačního prostředí“*.

Přístup do Atestačního prostředí mají ze strany Objednatele pouze osoby v roli Zástupce Objednatele ve věcech technických.

V případě, že Zástupce Objednatele ve věcech technických ztratí (zapomene) přístupové údaje, požádá Objednatel o jejich náhradu prostřednictvím formuláře *„Žádost o technickou pomoc při přípravě Atestačního prostředí“*, jehož závazný vzor je zveřejněn na Internetových stránkách Atestačního střediska v sekci *Formuláře pro atestace*.

Za účelem instalace eSSL do Atestačního prostředí dostanou osoby v roli Zástupce Objednatele ve věcech technických dočasně přiděleno administrátorské oprávnění potřebné pro provedení instalace. Po předání eSSL Atestačnímu středisku prostřednictvím formuláře *„Předávací protokol nainstalovaného eSSL“* jsou přístupová práva odebrána.

6.2 Ochrana osobních údajů objednatele atestace v rámci správy uživatelských přístupů

V rámci vytváření a správy uživatelských přístupů Objednatelů může docházet ke zpracování osobních údajů uživatelů ze strany Objednatele. Agentura se zavazuje tyto osobní údaje zpracovávat dle svých postupů, které jsou v souladu s nařízením GDPR a zákonem č. 110/2019 Sb. o zpracování osobních údajů v platném znění. Agentura aplikovala veškerá technická opatření sloužící k ochraně osobních údajů i pro prostředí Atestačního střediska. Podrobnější informace o zpracování osobních údajů jsou uvedeny na internetových stránkách Atestačního střediska v sekci „*Důležité dokumenty a odkazy*“.

Atestační středisko zpracovává osobní údaje uživatelů ze strany Objednatele atestace v rozsahu:

1) jméno a příjmení,
2) emailová adresa,
3) mobilní telefonní kontakt.

6.3 Omezení přístupu Objednatele k Atestačnímu prostředí

Po akceptaci eSSL k provedení atestace provede Atestační středisko přiměřená technická opatření k zamezení přístupu Objednatele do Atestačního prostředí. V souladu s čl. 6 dokumentu *„Postup Atestačního střediska“* je Objednatel povinen poskytnout Atestačnímu středisku nezbytnou součinnost k provedení tohoto kroku, včetně předání všech administrátorských a jiných přístupových oprávnění a technických prostředků nezbytných pro přístup k atestačnímu prostředí. Objednatel v

rámci předávacího protokolu potvrdí, že se nepokusí přistoupit k atestačnímu prostředí po celou dobu provádění atestace, pokud k tomu není písemně vyzván Atestačním střediskem. Porušení těchto povinností a závazků Objednatele zjištěné Atestačním střediskem je důvodem k okamžitému ukončení atestace bez vydání atestu, případně k okamžitému zneplatnění vydaného atestu.

6.4 Používání internetu ve virtualizovaném hardwarovém prostředí atestačního střediska

V rámci prováděných atestací nesmí uživatelé Objednatele ani Atestačního střediska měnit nastavení internetového prohlížeče na hardwarovém vybavení Atestačního střediska. Je výslovně zakázáno v rámci virtualizovaného hardwarového prostředí Atestačního střediska instalovat nebo spouštět jakékoliv nástroje pro vzdálenou správu mimo předem schválených aplikací, které jsou standardně dostupné v rámci schválené instalace prostředí Atestačního střediska. Internetový provoz v rámci atestační infrastruktury je monitorován a je zakázáno v rámci atestační infrastruktury přistupovat na jakékoliv závadné nebo potenciálně nebezpečné stránky.

V rámci informačního systému Atestačního střediska je zakázáno vytvářet nebo ukládat (kopírovat) data odporující zákonům ČR, normám a předpisům Atestačního střediska, dobrým mravům nebo obsahující jakékoli druhy pornografie, informace vedoucí k propagaci násilí, fašismu, rasismu a xenofobie, ohrožující práva a důstojnost osob nebo poškozující zájmy Atestačního střediska, České agentury pro standardizaci nebo České republiky.

6.5 Používání emailu v rámci infrastruktury Atestačního střediska

Objednatelům je umožněn přístup k e-mailovému serveru, který je součástí virtualizovaného hardwarového prostředí Atestačního střediska. Využití tohoto e-mailového serveru je možné pouze pro účely atestace. Tento e-mailový server **neslouží k provoznímu odesílání e-mailů mimo účely atestace.**

6.6 Instalace SW

Uživatel smí instalovat pouze legální software potřebný pro provedení atestace (testovaný eSSL a jeho komponenty a nevyhnutelně související software). Instalovat SW (pouze legální) mohou pouze uživatelé, jimž bylo k tomu přiděleno oprávnění; pro Objednatele toto jsou uživatelé v roli Zástupce Objednatele ve věcech technických.

V rámci předání instalovaného eSSL k provedení testů (viz kap. 6 *„Předání Atestačního prostředí Atestačnímu středisku po dokončení instalace eSSL“* dokumentu *„Provozní řád Atestačního střediska – Část 1: Metodika přípravy Atestačního prostředí“*) je Objednatel povinen doložit seznam jím instalovaného softwaru s ohledem na možná rizika bezpečnosti informací.

6.7 Odhlášení

Práce ve virtualizovaném hardwarovém prostředí Atestačního střediska vykonává Objednatel jen po dobu nezbytně nutnou. Po ukončení práce, nebo při jejím přerušení, je povinen relaci na virtualizovaném hardwarovém prostředí Atestačního střediska korektně uzavřít.

6.8 Autentizace

Autentizace uživatelů slouží k ověření jejich identity a opravňuje uživatele k získání požadovaných služeb a přístupu k aplikacím a datům. Uživatelé odpovídají za volbu a ochranu svých hesel. Hesla musí být uchovávána v tajnosti, nesmí být vyzrazena dalším uživatelům, zapsaná na papíře, uložena v systémech apod.

Heslo musí splňovat požadavek na složitost a komplexicitu:

- délka hesla nejméně 12 znaků;
- velká písmena (A až Z);

- malá písmena (a až z);
- čísla (0 až 9);
- ne-alfanumerické znaky (např. !, $, #, %).

Uživatelé jsou povinni si heslo po prvním přihlášení změnit.

6.9 Hlášení poruch, bezpečnostních incidentů, zranitelností (slabých míst), a mimořádných událostí

Bezpečnostní incident je událost, při které došlo k selhání nebo úmyslnému či neúmyslnému ohrožení informační bezpečnosti. Zranitelnost je slabé místo systému (aktiva), které může být využito hrozbou. Objednatel je povinen neprodleně hlásit jakýkoliv bezpečnostní incident (zjištěná nákaza virem, přítomnost ransomware, jakékoliv „podezřelé“ chování prostředí nebo softwaru apod.) nebo zranitelnost (nefunkční antivir, chybějící bezpečnostní záplaty apod.) v souladu s popisem uvedeným v kap. 2 *„Komunikace Objednatele a Atestačního střediska“* dokumentu *„Provozní řád Atestačního střediska – Část 1: Metodika přípravy Atestačního prostředí“* a to prostřednictvím formuláře *„Hlášení incidentu nebo události informační bezpečnosti“*, jehož závazný vzor je zveřejněn na internetových stránkách Atestačního střediska v sekci *Formuláře pro atestace*. Cílem je zajistit okamžité řešení incidentu a účinné snížení jeho následků.

7 Monitoring

7.1 Monitoring provozu virtualizovaného hardwarového prostředí Atestačního střediska

Monitoring provozu virtualizovaného hardwarového prostředí Atestačního střediska je prováděn kontinuálně IT specialisty Agentury. V případě zjištění, že Objednatel nedodržuje pravidla specifikovaná v této politice nebo v Provozním řádu Atestačního střediska jako celku (instalace neoprávněného softwaru, nedovolená modifikace virtualizovaného prostředí apod.) může dojít v souladu s článkem 6 odst. 2 dokumentu „Postup Atestačního střediska“ k pozastavení procesu atestace, případně k neudělení atestu.

7.2 Kontrola logů

Atestační středisko zajišťuje vhodným způsobem sběr a uchovávání logů provozní infrastruktury virtualizovaného hardwarového prostředí Atestačního střediska. Atestační středisko chrání a analyzuje logy, které zaznamenávají činnosti, výjimky, poruchy a další relevantní události v rámci provozu Atestačního střediska. Logy jsou uchovávány nejméně po dobu šesti měsíců od ukončení atestace a slouží zejména k monitoringu provozu a chování uživatelů v rámci Atestačního střediska.

Pokud byla pro provedení atestace zvolena varianta B) nebo C) podle čl. 5 dokumentu *„Postup Atestačního střediska“*, je Objednatel povinen rovněž sbírat logy a uchovávat je taktéž po dobu minimálně šesti měsíců od ukončení atestace a zpřístupnit je Atestačnímu středisku pro případnou kontrolu.