|  |
| --- |
| **Formulář pro vyplnění opatření, kterými poskytovatel splňuje bezpečnostní kritéria používaná při certifikaci (ex-ante kontrole)**  **Verze 1.3 z 1. 6. 2021**  **(rozšíření o prodejce, který je současně poskytovatelem SaaS, jehož SaaS běží na platformě jiného materiálního dodavatele)** |

**Pokyny pro vyplnění formuláře**:

1. Formulář uvádí bezpečnostní kritéria, která musí splnit poskytovatel služeb IaaS, PaaS a SaaS a umožňuje poskytovateli popsat, jak požadovaná kritéria splňuje. Poskytovatel vyplňuje pouze žlutě zvýrazněná pole.
2. Splnění požadovaných opatření (kritérií) dokladuje poskytovatel cloud computingu, kterým je jednak „prodejce“ (reseller nebo integrátor při nepřímém obchodním modelu – subjekt, který bude vstupovat do smluvního vztahu se zákazníkem) a jednak každý materiální dodavatel (subjekt, u kterého jsou trvale uložena zákaznická data a provozní údaje za účelem poskytování služby cloud computingu a který materiálně zajišťuje nabízenou službu cloud computingu).
3. Prodejce a materiální dodavatel mohou být totožný subjekt. V tomto případě dokládá dokumenty, které se vztahují na prodejce i na materiálního dodavatele.
4. Za všechny své materiální dodavatele v dodavatelském řetězci formulář vyplňuje prodejce (viz sloupce „Popis realizace kritéria materiálním dodavatelem č. x“). Doklady, které přikládá poskytovatel k žádosti o zápis nabídky, musí v případě, že se týkají materiálního dodavatele, obsahovat stejnou identifikaci materiálního dodavatele, jakou poskytovatel uvádí v této příloze – viz údaj „zkratka materiálního dodavatele“. V předaných materiálech musí být jasně identifikován skutečný materiální dodavatel – celé obchodní jméno, sídlo, IČO nebo jiný identifikátor používaný v zemi, kde sídlí materiální dodavatel.
5. Je-li prodejce současně dodavatelem aplikačního „softwaru jako služba“ (SaaS), který je provozován na IaaS/PaaS jiného materiálního dodavatele, pak prodejce za sebe dokládá nejen splnění kritérií označených „X“, ale i kritérií označených „S“ (viz sloupec „Dokládá za sebe prodejce“). Jedná se např. o doložení (nebo čestné prohlášení), že daná aplikace využívá požadované vlastnosti, kterými IaaS/PaaS disponuje.
6. Pro poskytovatele aplikačního „softwaru jako služba“ (SaaS), vyvíjeného na míru pro účely výkonu veřejné správy (viz definice ISVS v §2 ZoISVS) a v případech, kdy takový poskytovatel není současně poskytovatelem nižších vrstev služeb IaaS/PaaS, je požadovaný rozsah ISMS (Information Security Management System) omezen na bezpečný vývoj a údržbu systémů, a na další domény / kontrolní body standardů ISO, které odpovídají rozsahu odpovědnosti daného poskytovatele. Takový poskytovatel služby SaaS musí doložit separátně certifikace a bezpečnostní dokumentaci k opatřením v rámci nižších vrstev služeb IaaS/PaaS pocházející od materiálního dodavatele, kterého skutečně využívá. V případě, že poskytovatel a jeho IaaS/PaaS služby již byly certifikovány, tj. zapsány v katalogu cloud computingu, stačí, když poskytovatel SaaS uvede odkaz na jím využívané služby z katalogu. Jestliže poskytovatel SaaS ještě nedisponuje platnými certifikáty ISO 27001, ISO 27017, ISO 27018 pro celý rozsah svých nabízených služeb SaaS, avšak ostatní kritéria splňuje, může pro účely certifikace přiložit závaznou objednávku nebo uzavřenou smlouvu s některým akreditovaným certifikačním orgánem na výše uvedené certifikace. Služby SaaS budou v tomto případě zapsány do katalogu podmíněně na dobu 9 měsíců.
7. Konkrétní způsob pokrytí daného bezpečnostního opatření se pro konkrétní služby eGC, deklarované na jednom listu IaaS/PaaS nebo SaaS, mohou lišit vzhledem k vlastnostem konkrétní služby. Tak např. konkrétně použité šifrovací algoritmy a délky jejich klíčů se u služeb deklarovaných na jednom listu mohou lišit v rámci souladu s „Minimálními požadavky na šifrovací algoritmy NÚKIB…“. V takovém případě musí být v rámci daného ex-ante kritéria přiložen přehled, který detailně popisuje odlišnosti splnění daného kritéria pro konkrétní služby eGC, a to nejlépe výčtem nebo tabulkou.
8. Soulad s Nařízením Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) označovaným zkráceným názvem GDPR (General Data Protection Regulation) není součástí ex-ante kontroly. Pokud informační systém veřejné správy zpracovává osobní data, soulad s GDPR musí zajistit správce informačního systému veřejné správy v rámci podmínek obsažených v zadávací dokumentaci veřejné zakázky obsahující jako předmět plnění zakázky nebo její části cloud computing, v obsahu smlouvy na dodávané služby cloud computingu a během provozu informačního systému veřejné správy využívajícího cloud computingu.
9. Smluvní podmínky versus bezpečnostní kritéria: dle připomínek zadavatelů veřejných zakázek jsou z kritérií uvedených v eGC SAZ kap. 6.2.2 vyčleněny smluvní podmínky Sm1 až Sm8, které bude poskytovatel cloud computingu v rámci ex-ante kontroly pouze souhrnně akceptovat s tím, že za jejich začlenění do smlouvy je vždy odpovědný každý zadavatel veřejné zakázky. Smluvní podmínky Sm1 až Sm7 a Sm7 musí akceptovat i všichni materiální dodavatelé, neboť toto jsou smluvní podmínky vhodné k přenosu smluvních závazků od prodejce na jeho materiální dodavatele.
10. Jestliže se popis realizace daného kritéria odvolává na jiný dokument poskytovatele, předá poskytovatel relevantní část tohoto dokumentu v pdf formátu v samostatné příloze nabídky. Tyto dokumenty v příloze budou rozděleny do samostatných složek označených stejnou identifikací, jako je identifikace daného kritéria (viz Metodika). Současně poskytovatel jasně označí nebo uvede ty pasáže předaného dokumentu, které prokazují splnění požadovaného kritéria. Dokumenty mohou být v češtině, slovenštině nebo angličtině.
11. Z důvodu zjednodušení náročnosti ověřování podkladů v ex-ante kontrole, byla z kritérií z eGC SAZ kap. 6.2.2 pro účely ex-ante kontroly použita ta kritéria, která lze jasně doložit z certifikátů a citacemi z auditních zpráv dle uvedených standardů – to jsou kritéria zde uvedená jako ID1 až ID 18. Ostatní kritéria uvedená v eGC SAZ kap. 6.2.2 byla přesunuta na závěr tohoto dokumentu do bodu „Kritéria doporučené ke zvážení zadavatele v rámci veřejné zakázky“, kde jsou okomentovaná, proč se nehodí pro jednoduchou ex-ante kontrolu (jejíž výsledkem musí být jasné vyhodnocení splňuje či nesplňuje). Tyto požadavky mohou být upřesněny zadavatelem až ve veřejné zakázce a v rámci ex-post kontroly NÚKIB dle připravované „Cloudové vyhlášky“ nebo kontroly ze strany MV dle ZoISVS.
12. Vyplněný formulář bude považován za důvěrnou informaci v rámci funkce MV jakožto gestora ZoISVS včetně kontrolních a řídících funkcí dle ZoISVS §4 odst. 2. MV bude vyplněné formuláře (Přílohy č. 3) sdílet pouze v rozsahu certifikačního řízení, při spolupráci s NÚKIB a při případné spolupráci s dalšími kontrolními orgány veřejné správy v ČR

**Formulář pro vyplnění opatření, kterými poskytovatel splňuje bezpečnostní kritéria používaná při certifikaci (ex-ante kontrole)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Identifikace a popis kritéria ex-ante kontroly** | **Regulace/norma** | **Bezpečnostní úroveň, ve které je kritérium aplikováno** | | | **Způsob ověření** | **Poznámka** | **Realizace** | **Dokládá za sebe prodejce** | **Dokládá prodejce za všechny zúčastněné materiální dodavatele** | **Popis realizace kritéria prodejcem - *zkratka prodejce*** | **Popis realizace kritéria materiálním**  **dodavatelem č. 1 - *zkratka materiálního dodavatele č. 1*** |
| **N (1)** | **S (2)** | **V (3)** |  |  |
| **Část Smluvní podmínky mezi zákazníkem a poskytovatelem služby eGC** | | | | | | | | | | |  |
| Sm1 - Součástí smluvních podmínek je SLA, zahrnující úroveň dostupnosti (vazba na SAZ, přílohu č. 5 *Minimální smluvní podmínky* a přílohu č. 4 *Metodika hodnocení bezpečnostních dopadů*) | ČSN ISO/IEC 27001 A.15 | 96,16% | 99,45% | 99,90% | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele | Poskytovatel služeb eGC musí nabízet služby v této úrovni SLA, avšak v případě požadavku zákazníka může v dané bezpečnostní úrovni nabízet alternativu služby s nižší nebo vyšší úrovní dostupnosti v SLA. | Citace ze standardně nabízené SLA (která je součástí smluvní dokumentace), kde se poskytovatel zavazuje k úrovni dostupnosti, která je rovna nebo lepší než hodnoty v dané bezpečnostní úrovni, a to dle bližší specifikace v Příloze 5 SAZ, kap. 2.1.  Dále citace ze smlouvy nebo citace a link na obecné podmínky o podpoře služby, a to minimálně s uvedením denní doby podpory, s úrovněmi nabízené podpory a s prioritizací incidentů dle Přílohy 5 SAZ, kap. 2.2. | X | X | akceptuji/neakceptuji | akceptuji/neakceptuji |
| Sm2 - Smlouva obsahuje závazek účinného zavedení bezpečnostních opatření v rozsahu dané bezpečnostní úrovně | ČSN ISO/IEC 27001 A.15; ZoISVS §5b; VKB Příloha 7 bod a). | X | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele |  | Citace ze smluvních podmínek, uvádějící závazek zavedení bezp. opatření, která odpovídají rozsahu opatření dané bezp. úrovně. Pro BÚ 2 a 3: Účinnost těchto opatření musí být ověřena auditními zprávami podle mezinárodních standardů, uvedených dále v těchto kritériích. | X | X |
| Sm3 - Smlouva uvádí způsob poskytnutí informací o zavedených bezpečnostních opatřeních | ČSN ISO/IEC 27001 A.15, ZoISVS §5b | X | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele | Poskytovatel služeb eGC dá zadavatelům vhodným způsobem k dispozici popis, jakým způsobem jsou bezpečnostní opatření realizována. Může být podmíněn uzavřením NDA. | Citace smluvních podmínek poskytovatele, uvádějící informaci, resp. odkaz na podrobnější dokumentaci, jakým způsobem jsou bezpečnostní opatření realizována. Přístup k této informaci může být podmíněn uzavřením NDA. | X | X |
| Sm4 - Smluvní podmínky jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR, včetně pravidel pro zákaznický audit. | GDPR čl. 28 – Zpracovatel; zejména pak bod 3 h) a dále VKB Příloha 7 bod d). |  | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele | Uplatnit všeobecně. Většina IS bude zpracovávat osobní údaje a služby eGC publikované v katalogu eGC by na to měly být připraveny. V kategorii “nízká” nebude možné zpracovávat osobní údaje, viz kapitola 6.2 | Citace smluvních podmínek poskytovatele, která prokazuje soulad s požadavky na zpracovatele dle čl. 28 nařízení GDPR. Smluvní podmínky poskytovatele musí zahrnovat umožnění zákaznického auditu v souladu s čl. 28 bod 3 h), resp. VKB Příloha 7 bod d). | X | X |
| Sm5 - Smlouva obsahuje povinnost informovat zákazníka eGC o bezpečnostních incidentech, týkajících se daného zákazníka eGC, a spolupracovat při jejich zvládání | ČSN ISO/IEC 27001 A.16.1.2; VKB č. 82/2018 Sb. Příloha 7 odst. i) bod 1. | X | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele |  | Citace smluvních podmínek poskytovatele, obsahující povinnost informovat správce ISVS – zákazníka dané služby eGC o bezpečnostních incidentech, týkajících se daného zákazníka eGC. Rozsah definice bezpečnostního incidentu musí obsahovat ztrátu, znečitelnění (zničení) nebo neautorizovanou změnu (ztrátu integrity), nebo únik (vyzrazení – ztrátu důvěrnosti) zákaznických dat, včetně ztráty přístupu k těmto datům (ztrátu dostupnosti). Smlouva též musí obsahovat závazek vyšetřit bezpečnostní incident, poskytnout zákazníkovi podrobné informace o incidentu, a spolupracovat při jejich zvládání za účelem zmírnění následků resp. minimalizace škod. | X | X |
| Sm6 – Smlouva obsahuje povinnost materiálního dodavatele informovat zákazníka eGC v případech, kdy o vydání zákaznických dat požádají orgány činné v trestním řízení, a to ve všech případech, kdy informování zákazníka není v rozporu se zákonem. |  | X | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele |  | Citace smluvních podmínek poskytovatele, obsahující tento závazek. | X | X |
| Sm7 – Smlouva obsahuje povinnost poskytovatele dodržovat veškeré zákony a předpisy, které se vztahují k provozování služeb cloud computingu v segmentu zákazníků veřejné správy. |  | X | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele |  | Citace smluvních podmínek poskytovatele, obsahující tento závazek. | X | X |
| Sm8 – Standardní smlouva prodejce není v rozporu s minimálními smluvními podmínkami - viz Příloha 4. | Příloha 4. | X | X | X | Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele |  |  | X |  |  |
| **Výše uvedené smluvní požadavky budou v rámci ex-ante kontroly do Katalogu cloud computingu akceptovány „en bloc“, tak jak se uplatní na prodejce nebo materiální dodavatele cloud computingu jsou současně předány zadavatelům veřejných zakázek jako metodické doporučení MV.** | | | | | | | | | | |  |
| **Bezpečnostní kritéria pro ex-ante kontrolu (ID1 až ID18)**  **Opatření: Důvěryhodnost osoby poskytovatele** | | | | | | |  |  |  |  |  |
| ID1 - Poskytovatel má sídlo nebo bydliště v členském státě EU/EHS nebo má určeného svého zástupce ve členském státě EU obdobně dle čl. 27 GDPR.(Určený zástupce není materiálním dodavatelem). |  | X | X | X | Předložení dokumentu |  | Výpis z obchodního rejstříku nebo obdobné zahraniční evidence, nebo písemné čestné prohlášení v rozsahu údajů obsažených v obchodním rejstříku v případě, že není v obchodním rejstříku zapsán | X | X |  |  |
| ID2 – Proti poskytovateli nebylo za posledních 5 let vydáno pravomocné rozhodnutí o spáchání přestupku dle zákona o kybernetické bezpečnosti. |  | X | X | X | Předložení dokumentu |  | Poskytovatel předloží čestné prohlášení statutárního zástupce organizace. Pro poskytovatele usazené v jiných zemích EU/EHS může být toto prohlášení vyhotoveno i statutárním zástupcem české dceřiné společnosti daného poskytovatele nebo společnosti, která je k takovým úkonům zmocněna. | X | X |  |  |
| **Opatření: Normy, průmyslové standardy, certifikáty a auditní zprávy** | | | | | | | **Poskytovatel prokáže zavedení bezpečnostních opatření dle základních norem a předpisů, a to předložením podkladové dokumentace v některém elektronickém formátu dle standardů ISO (např. PDF, OOXML, ODF). Podkladová dokumentace může být v jazyce českém, slovenském nebo anglickém.** |  |  |  |  |
| ID3 – ČSN ISO/IEC 27001 | Důvodová zpráva k VKB č. 82/2018 Sb., lze uvést i mapovací tabulku požadavků VKB na opatření ISO/IEC 27001.  Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019. |  | X | X | Předložení dokumentu |  | 1. Poskytovatel předloží certifikát ve formátu PDF, do jehož certifikovaného rozsahu náleží všechny posuzované služby cloud computingu.  Rozsah certifikátu: certifikát se musí vztahovat na nabízené služby cloud computingu bez omezení; pokud certifikát obsahuje konkrétní výčet služeb cloud computingu, ale neobsahuje slovní spojení, které by výslovně omezovalo rozsah certifikace na přiložený výčet služeb, lze další služby cloud computingu stejné třídy, oblasti nebo typu, jako jsou uvedené na certifikátu doložit čestným prohlášením poskytovatele, že výčet služeb cloud computingu uvedený na certifikátu je vázán na datum provedení certifikace a další služby cloud computingu stejné třídy, oblasti nebo typu, které byly zavedeny a jsou poskytovány po datu vydání tohoto certifikátu, jsou podřazeny stejnému platnému systému řízení bezpečnosti informací poskytovatele, jehož soulad s mezinárodním standardem ISO/IEC 27001 byl vydaným certifikátem ověřen a jsou poskytovány z datových center poskytovatele, na které se vztahuje rozsah certifikátu.  Pro poskytovatele usazené v jiných zemích EU/EHS může být toto čestné prohlášení vyhotoveno i statutárním zástupcem české dceřiné společnosti daného poskytovatele nebo společnosti, která je k takovým úkonům zmocněna.  Datum poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů). Po nouzových opatřeních (Covid-19) může tato doba poslední revize být výjimečně až 18 měsíců, pouze do 1/10/19, dále již standardně 15 měsíců. V případě vydání certifikátu s dobou platnosti delší než 12 měsíců předložit poslední auditní zprávu ne starší 15 měsíců (resp. 18 měsíců za podmínek výše) a jiným způsobem prokázat aktivní stav platnosti certifikátu dle podmínek příslušné certifikační organizace.  Dále viz Poznámka 1 pod tabulkou (omezení rozsahu pro poskytovatele SaaS vyvíjeného na míru pro výkon veřejné správy.  2. Předložení SOA (Prohlášení o aplikovatelnosti) k certifikaci ČSN ISO/IEC 27001.  3. Předložení a auditní zprávy k certifikaci ČSN ISO/IEC 27001.  Pro BÚ 2: předložit SOA a auditní zprávu k certifikaci, zahrnující všechny domény ISO/IEC 27001:2013 s výjimkou A10 a A14. Pro BÚ  3 a 4: předložit SOA a auditní zprávu k certifikaci, zahrnující všechny domény daného ISO standardu.  Společnost provádějící certifikaci ISO/IEC 27001 musí mít akreditaci od akreditačního orgánu, který je členem IAF viz [https://www.iaf.nu//articles/IAF\_MEMBERS\_SIGNATORIES/4](https://www.iaf.nu/articles/IAF_MEMBERS_SIGNATORIES/4). Doložit výpisem z webu od koho má využitá certifikační společnost akreditaci, a zda je daný akreditační orgán uveden jako člen IAF.  Jestliže poskytovatel SaaS ještě nedisponuje platným certifikátem ISO 27001, pro celý rozsah svých nabízených služeb SaaS avšak ostatní kritéria splňuje, může pro účely certifikace přiložit závaznou objednávku nebo uzavřenou smlouvu s některým akreditovaným certifikačním orgánem na výše uvedené certifikace – viz pokyny bod 6. | S | X |  |  |
| ID4 - Deklarace minimálních bezpečnostních opatření pro BÚ 1 |  | X |  |  | Předložení dokumentu |  | Předložení deklarace poskytovatele o zavedených bezpečnostních opatřeních a popis těchto bezpečnostních opatření minimálně v doménách ISO/IEC 27001:2013 A7, A9, A12, A13, A15, A16, A18 a to na úrovni požadavku tohoto standardu. | S | X |  |  |
| ID5 – ČSN ISO/IEC 27017 | Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019. |  | X | X | Předložení dokumentu |  | 1. Poskytovatel předloží certifikát ve formátu PDF (může být také rozšířením certifikátu ISO/IEC 27001), do jehož certifikovaného rozsahu náleží všechny posuzované služby cloud computingu.  Pro Rozsah certifikátu platí totéž, co je uvedeno u ID-3.  Datum poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů). Po nouzových opatřeních (Covid-19) může tato doba poslední revize být výjimečně až 18 měsíců, pouze do 1/10/19, dále již standardně 15 měsíců. V případě vydání certifikátu s dobou platnosti delší než 12 měsíců předložit poslední auditní zprávu ne starší 15 měsíců (resp. 18 měsíců za podmínek výše) a jiným způsobem prokázat aktivní stav platnosti certifikátu dle podmínek příslušné certifikační organizace.  Dále viz Poznámka 1 pod tabulkou (omezení rozsahu pro poskytovatele SaaS vyvíjeného na míru pro výkon veřejné správy.)  2. Předložení SOA (Prohlášení o aplikovatelnosti) k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27017.  3. Předložení auditní zprávy k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27017.  Společnost provádějící certifikaci ISO/IEC 27017 musí mít akreditaci od akreditačního orgánu, který je členem IAF viz [https://www.iaf.nu//articles/IAF\_MEMBERS\_SIGNATORIES/4](https://www.iaf.nu/articles/IAF_MEMBERS_SIGNATORIES/4). Doložit výpisem z webu od koho má využitá certifikační společnost akreditaci, a zda je daný akreditační orgán uveden jako člen IAF.  Jestliže poskytovatel SaaS ještě nedisponuje platným certifikátem ISO 27017, pro celý rozsah svých nabízených služeb SaaS avšak ostatní kritéria splňuje, může pro účely certifikace přiložit závaznou objednávku nebo uzavřenou smlouvu s některým akreditovaným certifikačním orgánem na výše uvedené certifikace – viz pokyny bod 6.. | S | X |  |  |
| ID6 – ČSN ISO/IEC 27018 | Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019. |  | X | X | Předložení dokumentu |  | 1. Poskytovatel předloží certifikát ve formátu PDF (může být také rozšířením certifikátu ISO/IEC 27001), do jehož certifikovaného rozsahu náleží všechny posuzované služby cloud computingu.  Pro Rozsah certifikátu platí totéž, co je uvedeno u ID-3.  Datum poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů). Po nouzových opatřeních (Covid-19) může tato doba poslední revize být výjimečně až 18 měsíců, pouze do 1/10/19, dále již standardně 15 měsíců. V případě vydání certifikátu s dobou platnosti delší než 12 měsíců předložit poslední auditní zprávu ne starší 15 měsíců (resp. 18 měsíců za podmínek výše) a jiným způsobem prokázat aktivní stav platnosti certifikátu dle podmínek příslušné certifikační organizace.  2. Předložení SOA (Prohlášení o aplikovatelnosti) k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27018.  3. Předložení auditní zprávy k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27018.  Společnost provádějící certifikaci ISO/IEC 27018 musí mít akreditaci od akreditačního orgánu, který je členem IAF viz [https://www.iaf.nu//articles/IAF\_MEMBERS\_SIGNATORIES/4](https://www.iaf.nu/articles/IAF_MEMBERS_SIGNATORIES/4). Doložit výpisem z webu od koho má využitá certifikační společnost akreditaci, a zda je daný akreditační orgán uveden jako člen IAF.  Jestliže poskytovatel SaaS ještě nedisponuje platným certifikátem ISO 27017, pro celý rozsah svých nabízených služeb SaaS avšak ostatní kritéria splňuje, může pro účely certifikace přiložit závaznou objednávku nebo uzavřenou smlouvu s některým akreditovaným certifikačním orgánem na výše uvedené certifikace – viz pokyny bod 6.. | S | X |  |  |
| ID7 – Auditní zpráva SSAE18 SOC 2 Type II (sledování po dobu min. 6 měsíců z roku, viz [www.ssae-18.org](http://www.ssae-18.org) ) | Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019. Dále VKB §16 |  |  | X | Předložení dokumentu | Pozn.: SSAE18 je od r. 2017 novější verzí formátu SSAE16 | ODLOŽENÁ ÚČINNOST: toto kritérium bude účinné (tedy bude aplikováno) až od uplynutí 3 let od nabytí účinnosti probíhající novelizace ZoISVS projednávané v PS PČR (sněmovní tisk 756): Poskytovatel předloží celou auditní zprávu ve formátu PDF, v doménách Security, Availability, Processing Integrity, Confidentiality, Privacy. Pokud se jedná o službu typu SaaS vyvíjeného na míru jako ISVS (viz definice v ZoISVS § 2 písm. b)) využívající vrstvy IaaS nebo PaaS, které již tuto auditní zprávu mají, pak stačí doložit pouze auditní zprávu SSAE18 SOC 2 Type II na tyto podkladové vrstvy IaaS/PaaS (auditní zpráva SSAE 18 SOC 2 Type II se pro vrstvu aplikačního SW vyvíjeného na míru pro potřeby veřejné správy nevyžaduje). |  | X |  |  |
| ID8 – Zpráva o provedených penetračních testech (ne starší 3 let) | ČSN ISO/IEC 27001 A.18, A.12,  VKB § 25 |  |  | X | Předložení dokumentu |  | Poskytovatel předloží zprávu o penetračních testech:  1) v případě IaaS/PaaS dle standardu NIST SP 800-115, nebo dle standardu OSSTMM <https://www.isecom.org/OSSTMM.3.pdf>.  2) v případě SaaS se zahrnutím OWASP Top Ten zranitelností: <https://owasp.org/www-project-top-ten/>. | S | X |  |  |
| **Opatření: Upřesnění realizace vybraných bezpečnostních opatření** | | | | | | | **Poskytovatel deklaruje splnění těchto opatření formou prohlášení (zakliknutí checkboxu) a citací příslušné auditní zprávy a jejich podkladovou dokumentaci (v jazyce českém, slovenském nebo anglickém).** |  |  |  |  |
| ID9 - Deklarace místa uložení zákaznických dat v rámci jurisdikce EU a ošetření případného předávání údajů do třetích zemí |  | X | X | X | Předložení dokumentu | Viz také poznámka č. 2 pod tabulkou. | Citace smluvních podmínek poskytovatele, uvádějící závazek místa trvalého uložení zákaznického obsahu (jako jsou databáze, dokumenty, obsahy emailů atd. včetně jejich záloh) v rámci jurisdikce EU/EHS.  Pokud mohou nastat případy uložení a zpracování zákaznických dat mimo EU nebo EHS, poskytovatel tuto možnost deklaruje (uvede seznam datových center a jejich adres) a doloží způsob zajištění bezpečnosti předávaných údajů do těchto zemí (jakým způsobem jsou data zabezpečena).  Poskytovatel v Katalogu označí jako „globální CC“ takové služby CC, které kromě uložení zákaznických dat v jurisdikci EU/EHS mohou z funkčních důvodů ukládat a zpracovávat části zákaznického obsahu vícenásobně, a to i mimo jurisdikci EU/EHS (pozn. může se jednat např. o služby vyhledávání, jazykového překladu, nebo o služby pokročilého zabezpečení s korelací dat ze senzorů v globálním měřítku). | S | X |  |  |
| ID10 - Poskytovatel musí umožňovat synchronní replikaci dat alespoň do jednoho (jiného) záložního datového centra, které je z hlediska kapacity a zajištěné konektivity dostatečné k převzetí všech služeb, poskytovaných z primárního datového centra. | ČSN ISO/IEC 27001 A.11.1.4, A.12.3.1  VKB § 15, § 17 |  |  | X | Předložení dokumentu |  | **Pro IaaS:** Poskytovatel doloží citací z auditní zprávy ISO 27001 nebo ISO 22301 nebo SSAE 18 SOC 2 Type II připravenost záložního datového centra, které je kapacitně dostatečné k převzetí všech služeb poskytovaných z primárního datového centra.  **Pro PaaS:** deklarovat totéž pro ty služby PaaS, pro které je tento požadavek relevantní.  Pro **SaaS**: Odkaz na technickou dokumentaci služby SaaS, která tuto schopnost popisuje. Současně je třeba doložit, že IaaS/PaaS, na které je SaaS provozována, tuto schopnost nabízí – viz výše. | S | X |  |  |
| ID11 - Materiální dodavatel zajišťuje, že primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo je přijato adekvátní bezpečnostní opatření, nebo se primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, nacházejí ve vzájemné vzdálenosti nejméně 50 km, a jsou umístěna v lokalitách, které svým geografickým charakterem vylučují současné nebo následné škodlivé působení přírodních vlivů nebo jevů vyvolaných činností člověka vedoucích k poškození nebo zničení zákaznických dat anebo vyžadujících provedení záchranných prací. | ČSN ISO/IEC 27001 A.17.1.2, A.17.2.1  VKB § 15, § 17; Vzdálenost 50km: Zák. č. 499/2004 Sb. § 61 bod (2); Dále viz [doporučení Advisera ISO 27001 Academy](https://microsoft.sharepoint.com/teams/Strategické_projekty_PS_Czech/Shared%20Documents/NTO/National%20Cloud%20CZ/eGC%20Board/•%09https:/advisera.com/27001academy/knowledgebase/disaster-recovery-site-what-is-the-ideal-distance-from-primary-site/) |  | X | X | Předložení dokumentu |  | Odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci nebo výňatek z auditní zprávy ISO 27001 nebo SOC 2 Type 2, ze které bude patrné zajištění alespoň jedno záložního datového centra, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra  +  zpráva nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, která obsahuje náležitosti uvedené v příloze č. 5, nebo  odkaz na tu část platné certifikace ISO 27001 nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ze kterých je služba cloud computingu poskytována a čestné prohlášení, že primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, jsou umístěna v lokalitách, které svým geografickým charakterem vylučují současné nebo následné škodlivé působení přírodních vlivů nebo jevů vyvolaných činností člověka vedoucích k poškození nebo zničení zákaznických dat anebo vyžadujících provedení záchranných prací | S | X |  |  |
| ID12 - Primární i záložní datové centrum se nacházejí buď obě v České republice nebo ve dvou různých státech EU (EHS). | Viz zdůvodnění v předchozím ID12. |  |  | X | Předložení dokumentu |  | Poskytovatel doloží citací z auditní zprávy ISO 27001 nebo ISO 22301 nebo SSAE 18 SOC 2 Type II, ze kterých musí být zřejmé umístění primárního a záložního datového centra (minimálně s uvedením katastrálního území či obce a země). | S | X |  |  |
| ID13 - Poskytovatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu pro zajištění dostupnosti uvedené v bodě ID1 | ČSN ISO/IEC 27001 A.17, VKB §15 |  |  | X | Předložení dokumentu |  | Poskytovatel doloží svým Plánem zajištění kontinuity provozu a obnovy po havárii, který byl součástí certifikace ISO/IEC 27001 domény A.17 nebo certifikace ISO/IEC 22301, obojí s citací z příslušné auditní zprávy. Alternativně může doložit citací příslušných opatření ze zprávy SSAE 18 SOC 2 Type II. Každá taková auditní zpráva musí obsahovat kontrolní bod, podle kterého se provádí pravidelné testy výpadku provozního systému s přechodem zátěže do záložního nebo standby systému (tzv. Failover exercise). | S | X |  |  |
| ID14 – Poskytovatel má zaveden v rámci cloudových služeb systém sledování a vyhodnocování bezpečnostních událostí (např. SIEM) a umožní zpřístupnění prioritních událostí zákazníkovi | Umožnit správcům ISVS sběr a vyhodnocování kybernetických bezpečnostních událostí dle VKB § 24; Viz kontrolní bod A.12.4.1, lze doložit citací ze SSAE 18 SOC 2 |  | X | X | Předložení dokumentu | Upřesnění realizace opatření | Poskytovatel prokáže některou auditní zprávou ISO/IEC 270XX, SSAE 18 SOC 2 Type II, nebo jinou nezávislou auditní zprávou, že má zaveden systém sledování a vyhodnocování bezpečnostních událostí služby (např. SIEM), a poskytne technickou dokumentaci (nebo URL link), prokazující zpřístupnění prioritních událostí zákazníkovi služby.  Prodejce dokládá splnění tohoto požadavku tehdy, když nabízí tuto službu jako nadstavbu nad službou materiálního dodavatele. | S | X |  |  |
| ID15 – Služby centra bezpečnostního dohledu 24x7x365 pro sledování, vyhodnocování a řešení bezpečnostních událostí (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany) | ČSN ISO/IEC 27001 subdoména A.12.4., lze doložit citací ze SSAE 18 SOC 2 |  |  | X | Předložení dokumentu | Upřesnění realizace opatření | Poskytovatel prokáže některou auditní zprávou ISO/IEC 270XX, SSAE 18 SOC 2 Type II, nebo jinou nezávislou auditní zprávou, že využívá služby centra bezpečnostního dohledu 24x7x365 pro sledování, vyhodnocování a řešení bezpečnostních událostí (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany).  Prodejce dokládá splnění tohoto požadavku tehdy, když nabízí tuto službu jako nadstavbu nad službou materiálního dodavatele. | X | X |  |  |
| ID16 - Šifrování při přenosech dat po externí datové síti (přes Internet) | ČSN ISO/IEC 27001 A.10.1.1; VKB § 18 c) | X | X | X | Předložení dokumentu | Upřesnění realizace opatření | BÚ2 a BÚ3: Poskytovatel prokáže technickou dokumentací k certifikaci ČSN ISO/IEC 27001 nebo auditní zprávou SSAE 18 SOC 2 Type II, že má zavedeno vynucení šifrování protokolem TLS při externích přenosech dat s vyloučením možnosti fall-backu na protokol HTTP (bez šifrování).  BÚ1: Poskytovatel předloží čestné prohlášení statutárního zástupce organizace, že má zavedeno vynucení šifrování protokolem TLS při externích přenosech dat s vyloučením možnosti fall-backu na protokol HTTP (bez šifrování).  Pro všechny: Použité šifry a hašovací algoritmy musí splňovat [Minimální požadavky na kryptografické algoritmy](https://nukib.cz/download/uredni-deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf) publikované na webu NÚKIB GovCERT.  Prodejce dokládá splnění tohoto požadavku tehdy, když nabízí tuto službu jako nadstavbu nad službou materiálního dodavatele. | X | X |  |  |
| ID17 – Ochrana dat šifrováním v úložištích v cloudové službě algoritmem uvedeným v doporučení v oblasti kryptografických prostředků, které je zveřejněno na internetových stránkách NÚKIB; v případě uložení šifrovacích klíčů mimo perimetr zákazníka umožní poskytovatel uložení klíčů v certifikovaném Hardware security modulu (HSM) úrovně ochrany FIPS 140-2 level 2 (nebo vyšší) nebo certifikaci dle Common Criteria minimálně na EAL 4 a vyšší, který je pod virtuální správou orgánu veřejné moci. (Využití HSM modulu může představovat volitelnou službu za příplatek) | ČSN ISO/IEC 27001 A.10.1.2;  Odvozeno od požadavku VKB Příloha 4 – Likvidace dat pro úroveň aktiv „Vysoká“. |  |  | X | Předložení dokumentu |  | 1) Poskytovatel předloží technickou dokumentaci k bodu A.10.1.2 ISO/IEC 27001 nebo prokáže auditní zprávou SSAE 18 SOC 2, že v případě uložení šifrovacích klíčů mimo perimetr zákazníka, má zákazník možnost uložit šifrovací klíče pod svojí virtuální správou v HSM modulu definované úrovně ochrany.  Dokumentace musí ukázat, že použité šifry a hašovací algoritmy musí splňovat [Minimální požadavky na kryptografické algoritmy](https://nukib.cz/download/uredni-deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf) publikované na webu NÚKIB GovCERT.  2) Poskytovatel deklaruje, že tímto bodem je možné splnit požadavky na bezpečnou likvidaci dat pro úroveň důvěrnosti aktiv „vysoká“ v souladu s VKB Příloha 4. | S | X |  |  |
| ID18 – Definovaná dostupnost služby  CC prostřednictvím NIX.CZ nebo jiného peeringového uzlu v ČR |  | X | X | X | Předložení výpisu | Prokázat peering v ČR pomocí www.peeringdb.com nebo jiným srovnatelným způsobem. Deklarovat šířku pásma [Gb/s], kterou má daný poskytovatel do peeringového bodu k dispozici. | Dodavatel služby eGC deklaruje svoje možnosti peeringu v ČR, a to výpisem z [www.peeringdb.com](http://www.peeringdb.com) nebo jiným srovnatelným způsobem. Deklarovat šířku pásma [Gb/s], kterou má daný poskytovatel služby z datového centra (nebo center) do peeringového bodu k dispozici. | S | X |  |  |

**S1: Seznam materiálních dodavatelů, kteří jsou poddodavateli vykazujícího poskytovatele:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Poř.č.** | **Celé obchodní jméno** | **Sídlo** | **Zkratka materiálního dodavatele používaná v tabulce výše** | **IČO nebo jiný identifikátor používaný v zemi, kde sídlí materiální dodavatel** | **Odkaz na přiložený dokument dokládající, že vykazující poskytovatel je oprávněn materiálního dodavatele v této věci zastupovat** |
| **1.** |  |  |  |  |  |

**S2: Seznam systematických zpracovatelů, kteří jsou poddodavateli vykazujícího poskytovatele (**vztah s každým systematickým zpracovatelem musí být ošetřen dle čl. 28 GDPR):

|  |  |  |  |
| --- | --- | --- | --- |
| **Poř.č.** | **Celé obchodní jméno** | **Sídlo** | **IČO nebo jiný identifikátor používaný v zemi, kde sídlí materiální dodavatel** |
| **1.** |  |  |  |

**Kritéria doporučené ke zvážení pro zadavatele v rámci veřejné zakázky:**

**Kritéria z eGC SAZ kap. 6.2.2 nezařazená do metodiky, které mohou zvážit zadavatelé (OVS) dle svojí potřeby ve veřejných zakázkách:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Identifikace a Popis opatření** | **Regulace/norma** | **N (1)** | **S (2)** | **V (3)** | **ZD** | **Poznámka** | **Realizace / způsob ověření** |
| U.3 – Rozhraní (API) pro předávání provozních záznamů (logů) minimálně pro vnitřní síťovou infrastrukturu relevantní pro danou eGC službu, pro kontrolu stavu virtuálních výpočetních prostředků a datových úložišť, a případně pro aplikace, pokud jsou součástí dané služby. | Umožnit správcům ISVS zaznamenávání událostí dle VKB § 22 (může být sporné, jestli je deklarovaná funkčnost dostatečná pro splnění požadavku VKB) |  | X | X | Předložení dokumentu | Upřesnění realizace opatření | Dodavatel předloží nebo poskytne URL odkaz na technickou dokumentaci k rozhraní API pro předávání provozních záznamů (logů). Tyto logy musí obsahovat (podle úrovní služby IaaS/PaaS/SaaS) minimálně monitoring vnitřní síťové infrastruktury relevantní pro danou službu, monitoring stavu virtuálních výpočetních prostředků a datových úložišť, a případně monitoring stavu aplikací, pokud jsou součástí dané služby.  Splnění tohoto bodu technickou dokumentací nemusí ukázat dostatečnou funkčnost a úplnost rozhraní pro předávání provozních záznamů. NECHAT NA PŘESNĚJŠÍ SPECIFIKACI VE VZ A PŘÍPADNOU EX-POST KONTROLU NÚKIB – na základě VKB § 22 |
| U.5 – Opatření pro zajištění úrovně dostupnosti – použití nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany) | ČSN ISO/IEC 27001 A.12.1.3. avšak obtížné prověřit míru splnění |  | X | X | Předložení dokumentu | Upřesnění realizace opatření | Dodavatel prokáže obchodní nabídkou a technickou dokumentací, že má k dispozici nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany).  Míru splnění tohoto bodu může být obtížné posoudit ve fázi ex-ante kontroly. NECHAT NA SPECIFIKACI VE VZ A PŘÍPADNOU EX-POST KONTROLU NÚKIB dle VKB § 27 bod b) (zde jen obecný požadavek) |
| U.9 – Součástí služby musí být možnost silné (např. dvoufázové nebo dvoufaktorové) autentizace uživatelů – popsat mechanismus. | ČSN ISO/IEC 27001 A.9.4.2; Vyhláška č. 82/2018 Sb., §19 |  |  | X | Předložení dokumentu | Upřesnění realizace opatření | Dodavatel prokáže obchodní nabídkou a technickou dokumentací, že u služeb eGC zařazených do bezp. úrovně 3 nebo 4 dává zákazníkovi možnost využít silné autentizace uživatelů a administrátorů (dvoufázová nebo dvoufaktorová autentizace) Dodavatel předloží popis těchto mechanismů v dokumentaci.  Poskytovatelé dnes běžně nabízí několik variant vícefaktorové autentizace, avšak nabízené metody nemusí vždy vyhovovat konkrétním požadavkům zadavatelů. NECHAT NA PŘESNĚJŠÍ SPECIFIKACI VE VZ A PŘÍPADNOU EX-POST KONTROLU NÚKIB – na základě VKB § 19 |
| U.10 – Poskytovatel služby eGC deklaruje a technicky objasní možnost průběžné replikace zákaznických dat do prostředí on-premise nebo do státní části eGC. Poskytovatel dále umožní službu typu „bulk import/export dat“ pro import či export velkých objemů dat prostřednictvím zaslání šifrovaných paměťových médií. | ČSN ISO/IEC 27001 A.17, ZoKB/vyhláška č. 82/2018 Sb. §27 |  | X | X | Předložení dokumentu | Upřesnění realizace opatření | Dodavatel služby eGC prokáže technickou dokumentací možnost průběžné replikace zákaznických dat do prostředí on-premise nebo do státní části eGC. Dále prokáže technickou a provozní dokumentací existenci služby pro import a export velkých objemů dat prostřednictvím zaslání šifrovaných paměťových médií.  Poskytovatelé dnes běžně nabízí různé varianty replikace dat do on-premise prostředí zákazníka, včetně bulk přenosů dat. Vzhledem k tomu, že je v rámci ex-ante kontroly obtížné obecně rozhodnout jestli konkrétně nabízená metoda replikace dat nebo bulk přenosů bude odpovídat požadavkům konkrétních zákazníků, navrhujeme NECHAT NA PŘESNĚJŠÍ SPECIFIKACI VE VZ A PŘÍPADNOU EX-POST KONTROLU NÚKIB – na základě VKB § 27 |
| U.11 – Poskytovatel služby eGC předá popis realizace kontejnerové technologie. Její využití musí být v souladu s výsledky analýzy rizik s ohledem na hodnocení důvěrnosti zákaznických dat (kontejnerová technologie může snížit úroveň separace tenantů v cloudu) | ISO 27017 CLD 12.4.5 |  |  | X |  | Upřesnění realizace opatření | Pouze pro nabídky platformních služeb (PaaS) v oblasti kontejnerových technologií: Dodavatel služby eGC předá v rámci dokumentace služby popis realizace kontejnerové technologie. Její využití musí být v souladu s výsledky analýzy rizik s ohledem na hodnocení důvěrnosti zákaznických dat (kontejnerová technologie může snížit úroveň separace tenantů v cloudu)  Míru zabezpečení kontejnérové technologie je obtížné vyhodnotit ve fázi ex-ante kontroly. NECHAT NA SPECIFIKACI VE VZ dle požadavků analýzy rizik konkrétního řešení. |
| Část „K“ – Bezpečnostní požadavky na komunikační sítě. Dodavatel splní technickým popisem a případně odkazem na prováděcí technickou dokumentaci. | | | | | | |  |
| K.1 – Zajištění a registrace fixní IP adresy v CMS z důvodu whitelistingu |  | X | X | X | Předložení dokumentu |  | Dodavatel služby eGC prokáže provozně-technickou dokumentací, jakým způsobem lze pro správce systému zajistit fixní IP adresu služby za účelem whitelistingu v CMS.  Tento požadavek je příliš složitý na doložení, neboť způsob realizace fixní adresy směrem do Internetu se může lišit podle konkrétní služby, zejména v oblasti PaaS. V některých scénářích využití CC bude tento požadavek irelevantní (např. elektronická pošta), v jiných případech bude záležet na konkrétním scénáři řešení. |
| K.2 – Podpora VPN dle podmínek připojení v katalogu služeb CMS |  | X | X | X | Předložení dokumentu | www.mvcr.cz , dále volba „eGovernment“, dále volba „Komunikační infrastruktura veřejné správy a Centrální místo služeb“, dále volba „CMS“. | Dodavatel služby eGC poskytne prohlášení a odkazy na provozně-technickou dokumentaci, jakým způsobem splní požadavky na VPN dle publikovaných podmínek připojení v Katalogu služeb CMS, viz www.mvcr.cz , dále volba „eGovernment“, dále volba „Komunikační infrastruktura veřejné správy a Centrální místo služeb“, dále volba „CMS“.  Většina cloudových poskytovatelů již dnes poskytuje služby VPN, které však mohou být za příplatek. Obecně není problém pro jakéhokoli poskytovatele CC takovou VPN s požadovanými vlastnostmi zajistit, a proto je vhodnější nechat tento požadavek až na konkrétní specifikaci zadavatelem dle konkrétního řešení. |
| K.4 – Splnění podmínek pro připojení do projektu FENIX  (viz https://www.nix.cz/cs/file/NIX\_PRAVIDLA\_FENIX) – požadavek na poskytovatele připojení | Akční plán NBÚ k Národní strategii kybernetické bezpečnosti ČR 2015 až 2020, C.3.12 |  |  | X |  | Jedná se v zásadě o požadavek na poskytovatele služeb internetové konektivity. Na poskytovatele komerčních cloudových služeb se uplatní pouze v případech, kde je služba internetové konektivity součástí cloudové služby. V opačných případech tento požadavek uplatní zadavatel na svého poskytovatele služby internetové konektivity. | Poskytovatel internetové konektivity prokáže tento požadavek členstvím v projektu FENIX, viz <https://fe.nix.cz/> (tento požadavek je třeba právně ověřit, jestli není diskriminační z hlediska ZZVZ).  Požadavek na připojení do projektu FENIX se principiálně týká poskytovatelů internetové konektivity. Vzhledem k tomu, že služby internetové konektivity (jako takové) nejsou předmětem katalogů CC (IaaS, PaaS, SaaS), musí si tento požadavek zajistit zadavatelé u svých dodavatelů konektivity. |