Česká republika
Nejvyšší kontrolní úřad

SMLOUVA O DÍLO

na dodávku a implementaci software pro centrální správu a řízení rizik

(dále jen „Smlouva“)

Číslo smlouvy Dodavatel	Číslo smlouvy Objednatele
15/2019	**47/160/2019**

Software 42, s.r.o. **(dále jen „Dodavatel“)**			**ČR - Nejvyšší kontrolní úřad** **(dále jen „Objednatel“)**	
Se sídlem:	Kyjevská 2522/3? 251 01 Říčany		Se sídlem:	Jankovcova 1518/2, 170 04 Praha 7
Zastoupený:	Mgr. Vladimírem Slavíkem		Jejímž jménem jedná:	PhDr. Radek Haubert
Funkce:	jednatel		Funkce:	vrchní ředitel správní sekce
Kontaktní osoby:	Mgr. Vladimír Slavík		Kontaktní osoba:	Mgr. Gabriela Kiššová
Funkce:	jednatel		Funkce:	vedoucí oddělení aplikací a databází
Tel.:	+420 724 003 138		Tel.:	+420 233 045 220
E-mail:	slavik@software42.cz		E-mail:	Gabriela.kissova@nku.cz
IČO:	05527171		IČO:	49370227
DIČ:	není plátce DPH		DIČ:	není plátce DPH
Zapsaná v obchodním rejstříku:	vedeném Městským soudem v Praze, oddíl C, vložka 264797		Zapsaná v obchodním rejstříku:	Nezapsán
Bank. spojení:	Fio banka, 2601093475/2010		Bank. spojení:	Česká národní banka 30027-001/0710
Identifikátor datové schránky:	55t5pdv		Identifikátor datové schránky:	s3caayq

(společně též „Smluvní strany“)

Smluvní strany uzavírají následující Smlouvu o dílo podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“).

PREAMBULE

Tuto Smlouvu uzavírá Dodavatel s Objednatelem jakožto vítězným vybraným dodavatelem zadávacího řízení vypsaného Objednatelem na zakázku malého rozsahu s názvem „RISK - 2019, dodávku a implementaci software pro centrální správu a řízení rizik“.

Dodavatel prohlašuje, že se při zpracování nabídky se zadávací dokumentací veřejné zakázky seznámil a považuje ji za dostatečný podklad pro plnění předmětu Smlouvy.

Účelem této Smlouvy je právní úprava předmětu plnění této Smlouvy v souladu s vůlí Objednatele a Dodavatele, příslušnými platnými právními předpisy tak, aby Smluvní strany měly možnost při nejvyšší možné míře právní jistoty realizovat práva a plnit povinnosti touto Smlouvou založené.

Dodavatel prohlašuje, že má, respektive jeho poddodavatelé mají zákonem vyžadovanou odbornou způsobilost pro splnění předmětu této Smlouvy. Tato způsobilost se týká zejména vzdělání a odborné kvalifikace Dodavatele. Odborná způsobilost musí být platná po celou dobu trvání Smlouvy.

Smluvní strany prohlašují, že identifikační údaje uvedené ve Smlouvě a taktéž oprávnění k podnikání jsou v souladu s právní skutečností v době uzavření Smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení druhé Smluvní straně.

Smluvní strany prohlašují, že osoby podepisující tuto Smlouvu jsou k tomuto úkonu oprávněny.

I.

Účel Smlouvy

Účelem Smlouvy je zajistit centralizaci dosavadního systému evidence rizik jednotlivými organizačními útvary Objednatele z důvodu přehledné a aktuální informovanosti o stavu řízení rizik u Objednatele.

II.

Předmět a rozsah Smlouvy

(1) Předmětem plnění dle této Smlouvy je dodávka, implementace a poskytování servisní podpory zajišťující provoz sytému / webové aplikace pro centrální správu a řízení rizik Objednatele (dále jen „SW Rizika“), které sestávají z/ze:

a) dodávky trvalých licencí SW Rizika, včetně převodu nevýhradního práva užívat Dodavatelem dodaný SW Rizika na Objednatele, a to po dobu trvání autorských práv,
b) implementace a konfigurace SW Rizika v testovacím a provozním prostředí Objednatele,
c) vytvoření a dodání technické, administrátorské a uživatelské dokumentace SW Rizika v českém jazyce,
d) základní proškolení administrátorů Objednatele v rozsahu 10 hodin (10 x 60 minut),
e) poskytování servisní podpory zajišťující provoz a údržbu SW Rizika,
f) realizace rozvojových požadavků zadaných Objednatelem v rozsahu 30 hodin za období 12 měsíců.

(2) Bližší specifikace předmětu plnění a požadavky na implementaci SW Rizika se nachází v příloze č. 2 této Smlouvy.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(3) Předmětem plnění této Smlouvy není dodávka licencí produktů Microsoft, zejména dodávka licencí databázového enginu (SQL) a operačního systému (OS) na platformě Microsoft.

(4) Objednatel zajistí Dodavateli potřebné hardwarové a softwarové zdroje - servery, operační systém a databázový engine potřebný k provozu SW Rizika.

(5) Dodavatel se zavazuje plnit své povinnosti s odbornou péčí, na své náklady a na své nebezpečí, ve stanovených termínech řádně a včas a v požadované kvalitě, v souladu se zájmy Objednatele a svými kvalifikovanými pracovníky.

(6) Realizace implementace SW Rizika bude Smluvními stranami probíhat ve lhůtách stanovených v časovém harmonogramu. Návrh časového harmonogramu zpracuje Dodavatel a předá ho Objednateli k připomínkám do 5 pracovních dnů od uzavření Smlouvy. Konečné znění harmonogramu Smluvní strany odsouhlasí do 10 dnů od uzavření Smlouvy na společném jednání. Změny časového harmonogramu jsou možné po odsouhlasení oběma Smluvními stranami.

(7) Milníky pro realizaci SW Rizika:

a) schválení Cílového konceptu realizace SW Rizika před zahájením implementace SW Rizika Smluvními stranami,
b) akceptace dodávky, instalace a konfigurace SW Rizika v testovacím prostředí Objednatele, termín dle časového harmonogramu,
c) akceptace testovacího provozu SW Rizika, termín dle časového harmonogramu,
d) akceptace instalace a konfigurace SW Rizika v provozním prostředí Objednatele, termín dle časového harmonogramu,
e) předání SW Rizika do běžného provozu Objednateli dle časového harmonogramu,
f) odstranění případných výhrad zjištěných v rámci akceptace ve stanovených lhůtách uvedených v akceptačních protokolech nebo předávacím protokolu.

(8) Řešení SW Rizika bude předáno Objednateli na základě podepsaného předávacího protokolu, jehož přílohami budou všechny dodací listy a další dokumenty prokazující splnění předmětu Smlouvy, zejména:

a) seznam licencí s přesným názvem včetně verze, množstvím licencí, typem licenčního omezení (například zda se jedná o jednotlivé nebo síťové licence, freeware, multilicence omezené i neomezené, v případě OEM, ke které HW komponentě) a originálních instalačních médií, pokud je s nimi dodáván,
b) akceptační protokoly z akceptací jednotlivých milníků provedení SW Rizika.

(9) Objednatel je povinen převzít od Dodavatele pouze plně funkční SW Rizika včetně dokumentace (technická, administrátorská a uživatelská) a proškolení administrátorů, pokud SW Rizika splňuje všechny požadavky stanovené touto Smlouvou a zadávacími podmínkami.

(10) Pokud při převzetí díla bude Objednatelem zjištěno, že SW Rizika má vady nebo nedodělky nebránící užívání SW Rizika v běžném provozu, je na vůli Objednatele, zda takové převzetí potvrdí, či nikoliv. V předávacím protokolu budou Objednatelem stanoveny lhůty, ve kterých Dodavatel všechny zjištěné vady a nedodělky odstraní.

(11) Servisní podpora SW Rizika začíná běžet následující po převzetí SW Rizika do běžného provozu Objednatelem.

(12) Dodavatel se zavazuje upozornit Objednatele na všechny okolnosti, které by mohly vést při plnění Smlouvy k omezení činnosti nebo ohrožení chodu informačního systému Objednatele.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(13) Dodavatel prohlašuje, že je odborně způsobilý k předmětu plnění dle této Smlouvy a má oprávnění na území České republiky poskytovat za úplatu všechny služby, jejichž poskytnutí je předmětem této Smlouvy.

III.

Doba a místo plnění

(1) Místem plnění je sídlo Objednatele.

(2) Předmět plnění bude Dodavatel zajišťovat v testovacím a provozním prostředí Objednatele.

(3) Servisní podpora SW Rizika bude prováděna v režimu 5x8, tj. v pracovní dny v době od 9:00 hod. do 17:00 hod. (dále jen „pracovní doba“) prostřednictvím vzdáleného přístupu nebo v místě provozování SW Rizika. Po dohodě Smluvních stran může být servisní podpora SW Rizika prováděna i mimo pracovní dobu.

(4) K plnění předmětu Smlouvy je pracovníkům Dodavatele umožněný vzdálený přístup do testovacího a produktivního prostředí SW Rizika Objednatele. Pracovníci Dodavatele bezpodmínečně akceptují pravidla Objednatele pro poskytování a práci pomocí vzdáleného přístupu, která jsou uvedena v příloze č. 3 této Smlouvy. Dodavatel je povinen nahlásit změnu těchto pracovníků neprodleně, nelze vzdálený přístup jednoho pracovníka využívat pro jiného pracovníka Dodavatele.

IV.

Poskytování servisní podpory zajišťující provoz a údržbu SW Rizika

(1) Poskytování servisní podpory zajišťující provoz a údržbu SW Rizika sestává z/ze:

a) odstraňování havarijních stavů, provozních problémů a incidentů,
b) nahrání aktualizace nebo nové verze produktu (maintenance produktu), na kterém je provozován SW Rizika,
c) re-konfigurace SW Rizika spojená se změnami souvisejícími při odstraňování havarijních stavů, problémů a incidentů, při nahrání aktualizace nebo nové verze produktu, při změně ve webových prohlížečích, změnou operačního systému nebo databázového enginu,
d) provádění údržby databází a navazujících služeb,
e) průběžná aktualizace uživatelské, administrátorské a technické dokumentace, zálohovacích plánu a plánu obnovy po havárii.

(2) Nahráním aktualizace nebo nové verze produktu se rozumí instalace dostupných aktualizačních balíčků na provozovaném hardwaru s ohledem na zajištění provozuschopnosti SW Rizika.

(3) Údržbou databází se rozumí zejména kontrola datové konzistence a integrity databáze, správa log souborů, kontrola indexace.

(4) Odstraňováním havarijních stavů, provozních problémů a incidentů se rozumí lokalizace příčiny a odstranění této příčiny, která způsobila celkovou nebo omezenou funkčnost SW Rizika.

Havarijním stavem se rozumí stav, který znemožňuje fungování SW Rizika.

Provozním problémem se rozumí stav, který znemožňuje řádné fungování určité základní funkce SW Rizika u některého koncového uživatele.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

Incidentem se rozumí stav, kdy některé funkce SW Rizika fungují omezeně.

(5) Servisním zásahem se rozumí zahájení činností k odstranění havarijního stavu, provozního problému, nahrání aktualizací, provádění údržby databází, nebo re-konfigurace SW Rizika.

(6) Objednatel oznamuje požadavek na servisní zásah Dodavateli telefonicky nebo elektronicky. Dodavatel je povinen obratem Objednateli potvrdit doručení požadavku na servisní zásah e-mailem.

(7) Lhůty pro zahájení a odstranění servisního zásahu jsou uvedeny v Příloze č. 1 Service Level Agreement (SLA).

(8) Dodavatel je povinen přijmout požadavek na servisní zásah i mimo pracovní dobu. V případě doručení požadavku mimo pracovní dobu, běží lhůta pro zahájení práce od 9:00 hodin následujícího pracovního dne.

(9) V odůvodněných případech na základě požadavku Dodavatele může Objednatel dodatečně poskytnout delší lhůtu pro ukončení servisního zásahu. Dodavatel je povinen ukončit servisní zásah v co nejkratší době.

(10) Ukončení servisního zásahu je definováno jako:

a) odstranění nahlášeného provozního problému, nebo
b) poskytnutí přijatelného náhradního řešení, nebo
c) převedení daného problému do nižší kategorie, nebo
d) rozhodnutí, že se jedná o nový rozvojový požadavek.

(11) Pokud Dodavatel neukončí servisní zásah ani v dodatečně Objednatelem poskytnuté lhůtě má Objednatel právo vyřešit havarijní stav nebo provozní problém prostřednictvím třetí osoby na náklady Dodavatele. Prodlení s ukončením servisního zásahu bude považováno za podstatné porušení této Smlouvy.

(12) Součástí servisní podpory SW Rizika jsou i činnosti v tomto článku výslovně nespecifikované, které však jsou k řádné funkčnosti systému nezbytné, a o kterých Dodavatel vzhledem ke své kvalifikaci a zkušenostem měl nebo mohl vědět.

V.

Realizace rozvojových požadavků

(1) Realizace rozvojových požadavků bude reflektovat na plánovaný rozvoj SW Rizika. Rozvojové požadavky budou realizovány podle skutečných potřeb a požadavků Objednatele. Objednatel není povinen vyčerpat všechny stanovené hodiny v průběhu trvání této Smlouvy.

(2) Objednatel specifikuje rozvojový požadavek popisem požadované funkcionality a elektronicky tento požadavek odešle Dodavateli. Dodavatel neprodleně potvrdí přijetí požadavku v elektronické podobě.

(3) Dodavatel na základě specifikovaného rozvojového požadavku Objednatele analyzuje rozsah dopadů požadavku na celé řešení SW Rizika, připraví návrh řešení a upřesní dobu potřebnou k realizaci rozvojového požadavku. Do pěti (5) pracovních dnů od potvrzení přijetí požadavku předá Objednateli návrh na řešení rozvojového požadavku.

(4) Objednatel na žádost Dodavatele je oprávněn stanovit při podání požadavku delší lhůtu pro reakci Dodavatele, než je uvedeno v odst. 3 tohoto článku.

(5) V případě nejasností si obě Smluvní strany poskytnou operativní součinnost.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(6) Návrh řešení rozvojového požadavku musí Objednatel schválit.

(7) Po realizaci prací Dodavatelem provedou Smluvní strany akceptaci, která bude zaznamenána v protokolu o akceptaci realizaci prací.

(8) Dodavatel je povinen úpravy SW Rizika na základě realizovaného rozvojového požadavku evidovat a v návaznosti na to aktualizovat dokumentaci (technickou, administrátorskou a uživatelskou) SW Rizika. Aktualizovanou dokumentaci zašle Dodavatel pověřenému správci IS Objednatele elektronicky nejpozději do 30 dnů od ukončení realizace rozvojového požadavku.

(9) Nevyčerpané hodiny práce pro realizaci rozvojových požadavků v rámci období 12 měsíců je možné vyčerpat v následujícím období.

VI.

Další povinnosti Smluvních stran

(1) Dodavatel je povinen zajistit bezpečnost dat a údajů při provádění servisní podpory SW Rizika.

(2) Objednatel se zavazuje zajistit Dodavateli nezbytnou součinnost k plnění předmětu této Smlouvy a za poskytnutí předmětu plnění řádně uhradit Dodavateli cenu uvedenou v článku VII.

(3) Dodavatel odpovídá Objednateli za škodu způsobenou porušením povinností Dodavatele stanovených touto Smlouvou.

(4) Za účelem provádění servisní podpory SW Rizika je Dodavatel oprávněn užívat vyhrazené prostředky Objednatele, na nichž se Smluvní strany dohodnou, nebo které jsou pro zabezpečení servisní podpory SW Rizika nezbytné.

(5) Za účelem provádění servisní podpory bude po předchozím odsouhlasení Objednatele umožněn vstup Dodavateli do objektů Objednatele. Požadavek na vstup do určených objektů je Dodavatel povinen oznámit Objednateli nejméně 1 den před vstupem. Objednatel je povinen řádně oznámený vstup Dodavateli zajistit a umožnit. Při vstupu do objektů Objednatele bude vždy u příslušné servisní podpory SW Rizika přítomen zaměstnanec Objednatele.

(6) Dodavatel vede dokumentaci o všech provedených změnách v elektronické podobě na Objednatelem vyhrazeném úložišti. V případě nedostupnosti úložiště Objednatele předá Dodavatel dokumentaci prostřednictvím elektronické pošty kontaktní osobě Objednatele.

(7) Dodavatel veškeré zdrojové kódy, které byly vyvinuté speciálně pro potřeby Objednatele za účelem plnění předmětu Smlouvy, bezodkladně předá na vyhrazené úložiště Objednatele. V případě nedostupnosti úložiště Objednatele předá Dodavatel zdrojové kódy Objednateli prostřednictvím CD nosiče.

(8) Smluvní strany jsou povinny navzájem se předem informovat o veškerých skutečnostech důležitých pro plnění předmětu této Smlouvy.

VII.

Cenové a platební podmínky

(1) Celková cena za plnění předmětu Smlouvy je stanovena jako nejvýše přípustná. V celkové ceně jsou zahrnuty úplné a veškeré náklady Dodavatele na splnění předmětu plnění této

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

Smlouvy. Žádné další ani související náklady nebudou Objednatelem uhrazeny, s výjimkou změny sazby DPH.

(2) Celková cena za dodávku trvalých licencí SW Rizika dle článku II, bodu 1), písm. a) činí 0 Kč bez DPH (bezplatně), neplátce DPH. Platba se uskuteční po předání SW Rizika na základě elektronické faktury, jejíž přílohou bude kopie předávacího protokolu.

(3) Celková cena za implementaci a konfiguraci SW v testovacím a provozním prostředí dle článku II, bodu 1), písm. b) včetně vytvoření a dodání technické, administrátorské a uživatelské dokumentace dle článku II, bodu 1), písm. c) a základního proškolení administrátorů v rozsahu 10 hod. dle článku II, bodu 1), písm. d) činí 462 600 Kč bez DPH, neplátce DPH. Platba se uskuteční po předání SW Rizika na základě elektronické faktury, jejíž přílohou bude kopie předávacího protokolu.

(4) Cena za poskytování servisní podpory dle článku II, bodu 1), písm. e) za 1 měsíc činí 4 000 Kč bez DPH, neplátce DPH. Platba bude hrazena 1 x čtvrtletně od převzetí SW rizika Objednatelem za předchozí kalendářní čtvrtletí (leden – březen, duben – červen, červenec – září, říjen – prosinec), ve výši 12 000 Kč bez DPH, neplátce DPH.

(5) Cena za realizaci rozvojových požadavků zadaných Objednatele za 1 hodinu práce činí 900 Kč bez DPH, neplátce DPH. Cena za realizovaný rozvojový požadavek bude hrazena po provedení akceptace realizace rozvojových požadavků Objednatelem.

(6) Objednatel je povinen uhradit jen skutečně obdržené věcné plnění, a to do výše poskytnutého plnění.

(7) V průběhu plnění smlouvy může dojít k navýšení celkové ceny plnění SW Rizika při změně sazby DPH a právě o tuto změnu. Žádné další ani související náklady nebudou Objednatelem uhrazeny.

(8) Objednatel bude hradit cenu za plnění na základě daňových dokladů – elektronických faktur vystavovaných Zhotovitelem.

(9) Faktura bude obsahovat číslo smlouvy Objednatele a všechny údaje uvedené v § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dále údaje ve smyslu ustanovení § 435 občanského zákoníku. Faktura bude zaslána Objednateli elektronicky do datové schránky Objednatele nebo na e-mailovou adresu: podatelna@nku.cz.

(10) K ceně bude účtována DPH ve výši stanovené platnými právními předpisy.

(11) V případě, že elektronická faktura nebude obsahovat náležitosti uvedené v této smlouvě a/nebo stanovené právními předpisy, bude-li obsahovat nesprávné údaje nebo nebudou-li k faktuře doloženy požadované přílohy nebo bude obsahovat jiné cenové údaje, je Objednatel oprávněn fakturu vrátit Dodavateli k opravě, či novému vystavení. V takovém případě lhůta splatnosti v celé sjednané délce začne plynout až dnem doručení faktury obsahující správné údaje a všechny náležitosti podle této smlouvy Objednateli.

(12) Splatnost elektronické faktury je sjednána na 15 kalendářních dnů od data předání elektronické faktury Objednatelem Dodavateli. Dnem úhrady se rozumí den, kterým je fakturovaná částka odepsaná z účtu Objednatele ve prospěch účtu Dodavatele. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu Objednatele.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(13) Pokud Objednatel obdrží od Dodavatele fakturu se všemi náležitostmi a požadovanými přílohami po 15. prosinci příslušného roku, prodlužuje se lhůta splatnosti takovéto faktury z 15 kalendářních dnů na 90 kalendářních dnů.

(14) V případě, že se Objednatel ocitne v platební neschopnosti z důvodu rozpočtového provizoria, má se za to, že není v prodlení s plněním peněžitých závazků splatných v době rozpočtového provizoria. Splatnost všech daňových dokladů se v případě vzniku rozpočtového provizoria posouvá na patnáctý (15.) den po uvolnění rozpočtových prostředků pro rozpočtovou kapitolu Objednatele, nejpozději však do 30. června příslušného kalendářního roku.

(15) V případě nezaplacení faktury ve lhůtě splatnosti ani po předchozím písemném upozornění na prodlení má oprávněná Smluvní strana nárok na zaplacení úroku z prodlení ve výši, která se stanoví dle ustanovení § 1802 a násl. občanského zákoníku.

(16) Úrok z prodlení v případě prodlení jedné ze Smluvních stran s úhradou peněžité částky bude ve výši stanovené Nařízením vlády č. 351/2013 Sb., v platném znění.

(17) Cena za plnění předmětu Smlouvy se bude vždy k 1. lednu příslušného kalendářního roku upravovat o částku odpovídající vývoji inflace/deflace, vyjádřené průměrným ročním indexem příslušných spotřebitelských cen v České republice (dále jen „index“) za kalendářní rok bezprostředně předcházející roku, ve kterém je cena za předmět upravena, avšak pouze pokud se index po 1. 1. 2023 nebo předchozí úpravě ceny předmětu Smlouvy dle tohoto bodu změní o více než dva procentní body. Úpravu ceny předmětu plnění Smlouvy uplatní Dodavatel písemným oznámením Objednateli o úpravě s uvedením částky, o kterou se cena za předmět plnění smlouvy mění. Oznámení o úpravě musí obsahovat přesné procentní vyjádření změny indexu a přesnou finanční částku nové ceny.

(18) Záloha nebude Dodavateli poskytnuta.

VIII.
Vlastnictví a užívání řešení HSM

(1) Objednatel nabývá vlastnické právo k SW Rizika po podpisu předávacího protokolu zástupci obou smluvních stran.

(2) Objednatel dnem podpisu předávacího protokolu nabývá na celou dobu trvání autorských práv nevýhradní právo užívat dodaný SW Rizika, jakož i veškerá plnění dodaná Dodavatelem na základě této Smlouvy, která mají charakter autorského díla, a to pro svoji potřebu bez jakýchkoliv dalších licenčních poplatků nebo jiných plateb nad rámec ceny SW Rizika. Právo užívat autorská díla zahrnuje i oprávnění tato díla zpřístupnit při odstraňování jejich vad a/nebo vad díla v nezbytném rozsahu třetím osobám.

(3) Dodavatel je povinen zajistit, aby Objednatel byl oprávněn dodaná autorská díla užívat za účelem plnění povinností a uplatňování svých práv podle této smlouvy. Odměna za poskytnutí práv užívání (licence) je zahrnuta v ceně SW Rizika.

(4) Právo užívat autorské dílo zahrnuje i oprávnění dílo zpřístupnit třetím osobám, zejména za účelem údržby, opravy anebo rozvoje.

(5) Dodavatel garantuje, že vykonává autorské právo k poskytnutému SW a je oprávněn k poskytnutí a převodu nevýhradních časově neomezených užívacích práv (licence) Objednateli k SW, které poskytne jako součást předmětu plnění. Nevýhradní časově neomezená užívací práva (licence) k SW jsou dále nazývána „nevýhradní práva k SW“.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(6) Dodavatel se zavazuje nevýhradní práva k SW Objednateli poskytnout a na Objednatele nevýhradní práva k SW převést.

(7) Dodavatel prohlašuje, že plněním závazků podle této Smlouvy neporušuje práva duševního a průmyslového vlastnictví třetích osob. V případě, že třetí osoba, včetně zaměstnanců a pracovníků Dodavatele, uplatní nárok vůči Objednateli z titulu porušení práv duševního nebo průmyslového vlastnictví v souvislosti s realizací nebo užíváním díla nebo jeho části, Dodavatel je povinen poskytnout Objednateli účinnou pomoc. Pokud uplatnění nároku třetí osobou bude úspěšné, Dodavatel odpovídá Objednateli za škodu, která mu tímto vznikla, a Objednatel je oprávněn odstoupit od Smlouvy.

IX.

Záruční podmínky

(1) Dodavatel odpovídá za to, že dílo je bez faktických a právních vad, je zhotoveno v souladu se Smlouvou a jejím účelem a příslušnými právními předpisy a v kvalitě Smlouvou dohodnuté a Objednatelem požadované.

(2) Za právní vady díla se považují zejména jakákoliv práva třetích osob zatěžující dílo, která by omezovala Objednatele v řádném užívání díla dle této Smlouvy.

(3) Za faktickou vadu díla se považuje zejména stav, kdy funkčnost programového vybavení (resp. jeho části) nebo technického vybavení dodaného na základě této Smlouvy a požívaného v souladu s jeho dokumentací neodpovídá funkčním specifikacím uvedeným v předmětné dokumentaci. To neplatí, jestliže programové nebo technické vybavení byly modifikovány Objednatelem nebo třetí stranou.

(4) Dodavatel poskytuje záruku za jakost díla na celý předmět plnění v trvání 2 let (dále jen „záruční doba“) ode dne předání a převzetí celého díla dle této Smlouvy.

(5) Záruční doba počíná plynout dnem následujícím po předání a převzetí kompletního dokončeného díla, stvrzeném podepsaným předávacím protokolem Smluvními stranami.

(6) Dodavatel odpovídá za vady, které má dílo v době jeho předání Objednateli, a za vady, které vzniknou nebo se objeví v průběhu záruční doby.

(7) Dodavatel odpovídá za vady vzniklé v rámci poskytování servisní podpory podle příslušných ustanovení občanského zákoníku. Dodavatel poskytuje na kvalitu svých plnění záruku v trvání 3 měsíců.

(8) Objednatel je oprávněný písemně reklamovat nedostatky či vady v záruční lhůtě. Objednatel má právo na bezplatné odstranění reklamovaného nedostatku či vady.

(9) V případě uplatnění vady díla Objednatelem v záruční době se Dodavatel zavazuje k jejímu bezplatnému odstranění. Termín a způsob odstranění této vady závisí na povaze vady a vzájemné dohodě Dodavatele a Objednatele.

(10) Záruka se nevztahuje na poruchy, které byly způsobeny neodbornou obsluhou a údržbou ze strany Objednatele, vyšší moci, nedodržením návodu od výrobce, nedodržením provozních podmínek nebo jiným způsobem než obvyklým provozem.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

X.

Povinnost mlčenlivosti

(1) Smluvní strany jsou povinny zavázat k utajování informací všechny zaměstnance a osoby Dodavatele, které pověří úkoly v souvislosti s realizací činnosti dle této Smlouvy tak, aby i tito byli plnohodnotně zavázáni ve smyslu tohoto ustanovení. Pro případ porušení povinnosti mlčenlivosti těmito osobami přebírá příslušná Smluvní strana plně odpovědnost za tyto osoby a případnou škodu způsobenou těmito osobami poškozené straně nahradí.

(2) Dodavatel je povinen zachovat mlčenlivost o technickém vybavení a osobních údajích osob činných u Objednatele bez ohledu na dobu trvání této Smlouvy.

(3) Za porušení povinnosti mlčenlivosti se nepovažuje, je-li Smluvní strana povinna příslušnou informaci sdělit na základě zákonem stanovené povinnosti.

(4) Povinnost mlčenlivosti trvá bez ohledu na účinnost nebo platnost této Smlouvy. Smluvní strana, která porušila povinnost mlčenlivosti, je povinna uhradit druhé Smluvní straně škodu a vydat bezdůvodné obohacení.

XI.

Sankce

(1) V případě nedodržení lhůt v rámci implementace SW Rizika dle odsouhlaseného harmonogramu je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 5 000 Kč za každý den prodlení.

(2) V případě nemožnosti oznámení vady nebo požadavku Dodavateli na servisní zásah je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 1 000 Kč za každou pracovní hodinu nemožnosti oznámení vady.

(3) V případě prodlení Dodavatele se zahájením jakéhokoli servisního zásahu je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 500 Kč za každou započatou hodinu prodlení a za každý případ.

(4) V případě prodlení Dodavatele s ukončením jakéhokoli servisního zásahu je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 1 000 Kč za každou započatou hodinu prodlení a za každý případ.

(5) Při prodlení Dodavatele s odstraněním oznámené vady delším než čtrnáct pracovních dnů je oprávněn zajistit si opravu prostřednictvím třetí osoby, na riziko a náklady Dodavatele. V případě odstranění vady třetí osobou je Dodavatel v prodlení se svým plněním až do doby skutečného odstranění vady, Dodavatel je oprávněn poskytnout třetí osobě součinnost.

(6) Dodavatel není v prodlení se zahájením a ukončením servisního zásahu v případě, že Objednatel neposkytl potřebnou součinnost dle Service Level Agreement (SLA) uvedené v příloze č. 1.

(7) Dodavatel odpovídá za škodu způsobenou vadným plněním této Smlouvy v rozsahu stanoveném českým právním řádem, zejména pak občanským zákoníkem.

(8) Žádná ze Smluvních stran není odpovědná za prodlení způsobené okolnostmi vylučujícími odpovědnost. Za okolnosti vylučující odpovědnost se považuje překážka, jež nastala nezávisle na vůli povinné strany a brání jí ve splnění její povinnosti, jestliže nelze rozumně předpokládat, že by povinná strana tuto překážku nebo její následky odvrátila nebo překonala a dále, že by v době vzniku překážku předvídala. Odpovědnost nevylučuje překážka, která vznikla teprve v době, kdy povinná strana byla v prodlení s plněním své

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

povinnosti nebo vznikla z jejích hospodářských poměrů. Účinky vylučující odpovědnost jsou omezeny pouze na dobu, dokud trvá překážka, s níž jsou tyto povinnosti spojeny.

(9) Smluvní pokuta je splatná do 30 kalendářních dnů od data, kdy byla povinné Smluvní straně doručena písemná výzva k jejich zaplacení oprávněnou Smluvní stranou, a to na účet oprávněné Smluvní strany uvedené v písemné výzvě.

(10) Smluvní sankce vůči Objednateli nejsou přípustné.

XII.

Náhrada škody

(1) Dodavatel odpovídá za škodu způsobenou vadným plněním této Smlouvy v rozsahu stanoveném českým právním řádem, zejména pak občanským zákoníkem.

(2) Rozsah odpovědnosti Dodavatele lze omezit nejvýše na dvojnásobek ceny díla.

(3) Žádná ze Smluvních stran není v prodlení a ani nemá povinnost nahradit škodu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bránila-li jí v jejich splnění nějaká z překážek, vylučující povinnost k úhradě ve smyslu § 2913 odst. 2 občanského zákoníku.

(4) Uplatněním nároku z odpovědnosti za vady plnění není dotčen nárok Objednatele na náhradu škody.

XIII.

Kontaktní osoby

(1) Smluvní strany určují pro vzájemnou komunikaci v jednotlivých oblastech působnosti kontaktní osoby (příp. službu) a kontaktní údaje. Tyto jsou uvedeny na seznamu kontaktů, který je přiložen ke Smlouvě. Každá Smluvní strana je povinna aktualizovat své kontaktní údaje a kontaktní osoby. Taková změna, písemně druhé Smluvní straně sdělená, není změnou Smlouvy a nevyžaduje uzavření dodatku ke Smlouvě.

Kontaktními osobami Smluvních stran jsou:

za Objednatele

Hlášení poruch v pracovní dny v době 9:00 – 17:00 hod.	*Gabriela Kiššová*	*233 045 220*	*Gabriela.kissova@nku.cz*
	Filip Chroust	*233 045 211*	*Filip.chroust@nku.cz*
Hlášení poruch nepřetržitě	*Helpdesk*	*233 045 333*	*160@nku.cz*
Zadávání rozvojových požadavků	*Gabriela Kiššová*	*233 045 220*	*Gabriela.kissova@nku.cz*

za Dodavatele

Příjem hlášení poruch v pracovní dny v době 9:00 – 17:00 hod.	*Kristýna Schnablová*	*737 337 993*	*schnablova@software42.cz*
Příjem hlášení poruch nepřetržitě	*Helpdesk*		*podpora@software42.cz*
Realizace rozvojových požadavků	*Vladimír Slavík*	*724 003 138*	*slavik@software42.cz*

(2) Dodavatel je povinen zajistit v případě nepřítomnosti odpovědného pracovníka Dodavatele z jakéhokoliv důvodu zástupce tohoto pracovníka po dobu jeho nepřítomnosti.

(3) V případě výměny pracovníků Dodavatele je Dodavatel povinen nahradit pracovníka novým pracovníkem ve stejné znalostní a zkušenostní úrovni jako byl původní pracovník Dodavatele.

XIV.

Doručování

(1) Není-li dohodnuto jinak, doručování písemností podle této Smlouvy bude uskutečňováno na adresu Smluvní strany uvedenou v záhlaví v této Smlouvě, případně na adresu, kterou Smluvní strana písemně druhé Smluvní straně oznámí, případně datovou schránkou nebo e-mailem. V případě doručování e-mailem je doručení účinné pouze v případě, že druhá Smluvní strana přijetí zprávy následně potvrdí. Za řádně doručenou se považuje též písemnost, kterou adresát odmítne převzít nebo se jako nedoručená vrátí zpět z adresy uvedené v záhlaví této Smlouvy nebo adresy později oznámené, a to dnem doručení odmítnuté nebo nepřevzaté zásilky zpět odesílateli.

(2) Kontaktní informace uvedené v této Smlouvě (tel. čísla, adresy atd.) mohou být Smluvními stranami jednostranně písemně měněny s účinností ode dne doručení druhé Smluvní straně, pokud v oznámení není uvedeno datum pozdější. Na adresu sídla Smluvní strany je možné doručovat vždy.

XV.

Doba trvání Smlouvy a její ukončení

(1) Smlouva se uzavírá na dobu neurčitou a nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami.

(2) Každá ze Smluvních stran může od Smlouvy odstoupit ze zákonných důvodů. Dodavatel není oprávněn tyto důvody rozšiřovat ani omezovat.

(3) Výpověď Smlouvy nabývá právní účinnosti dnem doručení písemného oznámení o výpovědi Smlouvy druhé Smluvní straně. Smlouvu lze ukončit výpovědí podanou alespoň tři měsíce předem.

(4) Odstoupením od této Smlouvy není dotčena platnost ani účinnost ustanovení této Smlouvy, která se týkají autorských práv, povinnosti mlčenlivosti, nároku na náhradu škody vzniklé porušením Smlouvy, nároku na zaplacení smluvní pokuty a řešení sporů.

(5) V případě odstoupení či výpovědi Smlouvy je Dodavatel povinen předat Objednateli dokumentaci o veškerých provedených změnách Dodavatelem a seznam všech přístupových účtů a hesel do jednoho měsíce od ukončení Smlouvy.

(6) Za podstatné porušení Smlouvy ze strany Objednatele se považuje neplnění závazků spočívajících zejména v neuhrazení dlužné částky po dobu 30 dnů od splatnosti daňového dokladu (faktury).

(7) Za podstatné porušení Smlouvy ze strany Dodavatele se považuje neplnění závazků spočívajících zejména v nedodržení termínů plnění Smlouvy delší než 30 dnů nebo realizace předmětu plnění Smlouvy v rozporu s ustanoveními Smlouvy anebo jiných závažných dokumentů, či právních předpisů.

XVI.

Závěrečná ujednání

(1) Tato Smlouva se řídí právním řádem České republiky, zejména příslušnými ustanoveními občanského zákoníku.

(2) Nevylučuje se využití poradních a expertních služeb dalších osob.

(3) Dodavatel je oprávněn plnit Smlouvu prostřednictvím poddodavatele. Případná změna poddodavatele nebo rozsahu plnění Smlouvy poddodavatelem vyžaduje písemný předchozí souhlas Objednatele.

(4) Objednatel nemá povinnost jednat s jakoukoliv třetí osobou kromě Dodavatele.

(5) Dodavatel není oprávněn postoupit práva, povinnosti, závazky ani pohledávky z této Smlouvy třetí osobě nebo jiným osobám bez předchozího písemného souhlasu Objednatele.

(6) Veškeré změny Smlouvy musí být odsouhlaseny v písemných, postupně číslovaných dodatcích s podpisem zástupců obou Smluvních stran oprávněných podepsat Smlouvu.

(7) Změnu oprávněných osob jsou Smluvní strany povinny si neprodleně písemně oznámit. Tato změna nevyžaduje formu dodatku k této Smlouvě.

(8) V případě rozporu při plnění závazků ze Smlouvy, a to zejména v případech neupravených Smlouvou, platí zadávací podmínky veřejné zakázky stanovené Objednatelem v zadávací dokumentaci, nabídky Dodavatele a občanského zákoníku, a to v tomto uvedeném pořadí.

(9) Smluvní strany se dohodly, že veškeré spory vyplývající ze vzniku, výkladu, realizace a ukončení této Smlouvy, jakož i veškeré sporné vztahy mezi Smluvními stranami z této Smlouvy vyplývající (dále jen „spory“), se budou snažit řešit nejprve smírnou cestou.

(10) Veškeré spory související s touto Smlouvou se Smluvní strany zavazují řešit především na úrovni oprávněných osob, popř. osob jim funkčně nadřízeným. Nepodaří se spor vyřešit ani zástupcům podepisujícím Smlouvu ve lhůtě alespoň třicet (30) dnů, bude spor postoupen k rozhodnutí příslušnému obecnému soudu České republiky na návrh kterékoliv Smluvní strany.

(11) Dodavatel vyslovuje souhlas s tím, že Objednatel v rámci transparentnosti Smlouvu (včetně případných dodatků) zveřejní způsobem, umožňující nepřetržitý vzdálený přístup.

(12) Dojde-li ke změně statutu (změna právní formy právnické osoby, fúze právnických osob, rozdělení právnické osoby) Dodavatele, je tento povinen oznámit nové skutečnosti Objednateli ve lhůtě 14 dnů od právní moci takové změny.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(13) Dodavatel bere na vědomí, že je podle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

(14) Tato Smlouva je vypracována v elektronickém vyhotovení a podepsána elektronickými podpisy.

(15) Smluvní strany prohlašují, že tato Smlouva je projevem jejich pravé a svobodné vůle a na důkaz dohody o celém obsahu této Smlouvy připojují své podpisy.

Příloha č. 1 Smlouvy - Service Level Agreement (SLA)

Příloha č. 2 Smlouvy - Požadavky na předmět dodávky a implementace CDE

Příloha č. 3 Smlouvy - Seznámení externího uživatele se zásadami bezpečnosti užívání ICT u Objednatele

PhDr. Radek Haubert
DN: P23249, Radek, Haubert, PhDr. Radek Haubert, 100,2488, Nejvyšší kontrolní úřad [IČ 49370227], NTRCZ-49370227, CZ
06.08.2019 10:49:04

V Říčanech dne 30. 7. 2019

Vladimír Slavík

Digitálně podepsal Vladimír Slavík
Datum: 2019.07.30 07:56:43 +02'00'

.....

Česká republika - Nejvyšší kontrolní úřad

PhDr. Radek Haubert

vrchní ředitel správní sekce

.....

Software 42, s.r.o.

Mgr. Vladimír Slavík

jednatel

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

Příloha č. 1 - Service Level Agreement (SLA)

Stupeň závažnosti	Definice	Opatření Dodavatele	Opatření Objednatele	Doba potvrzení	Doba zásahu
1.	Praktické užívání SW Rizika bylo přerušeno nebo je vážně narušeno a podstatná část uživatelů nemůže přiměřeně pokračovat ve své práci. SW Rizika není použitelný ve svých základních funkcích.	Zajistí, aby byli jeho pracovníci nepřetržitě k dispozici, dokud nebude nalezeno přijatelné řešení, kterým lze problém obejít. Takové přijatelné řešení znamená, že nebude působit významné potíže při používání SW Rizika.	Objednatel poskytne po dobu trvání problému k dispozici určené pracovníky, kteří budou zodpovídat dotazy a poskytovat relevantní informace (např. protokolové soubory, výtisky obrazovky, data) nutné k tomu, aby oddělení podpory Dodavatele mohlo problém vyřešit, v opačném případě bude stupeň závažnosti problému snížen na úroveň 2.	Do 1 hodiny	do 8 hodin
2.	Důležité funkce SW Rizika nejsou k dispozici a nelze je nijak obejít. Praktická použití jsou narušena, ale nikoli přerušena. Je vážně narušena produktivita značného počtu uživatelů nebo úrovně služby Objednatele.	Zajistí pracovníky během pracovní doby, dokud nebude nalezeno přijatelné řešení. Takové přijatelné řešení znamená, že nebude působit významné potíže při používání SW Rizika.	Objednatel během své pracovní doby poskytne veškeré relevantní informace (např. protokolové soubory, výtisky obrazovek, data) nutné k tomu, aby dodavatel mohl problém vyřešit, v opačném případě bude stupeň závažnosti problému snížen na úroveň 3.	Do 1 hodiny	do 16 hodin
3.	Nejsou k dispozici důležité funkce SW Rizika, ale je možné je obejít, nebo nejsou k dispozici méně důležité funkce softwaru, které však nelze obejít. Objednatel utrpěl mírnou ztrátu funkčnosti SW Rizika.	Zváží řešení, kterým by bylo možné problém obejít, a případně doplnění, které bude obsaženo v následné Aktualizaci.	Objednatel během své pracovní doby poskytne veškeré relevantní informace (např. protokolové soubory, výtisky obrazovek, data) nutné k tomu, aby Dodavatel mohl problém vyřešit.	Do 1 hodiny	do 40 hodin
4.	Objednatel zjistil menší vadu nebo žádá o informace, doplnění nebo vysvětlení dokumentace týkající se funkčnosti SW Rizika s tím, že provoz SW Rizika není narušen nebo je narušen jen minimálně.	Zváží doplnění softwaru, které bude obsaženo v následné Aktualizaci.	Objednatel během své pracovní doby poskytne veškeré relevantní informace (protokolové soubory, výtisky obrazovek, data) nutné k tomu, aby Dodavatel mohl problém vyřešit.	Do 1 hodiny	do 80 hodin

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

Příloha č. 2 – Požadavek na předmět dodávky a implementace software pro centrální správu a řízení rizik

Správa a řízení rizik probíhá na základě řízení rizik jednotlivými organizačními útvary Úřadu (cca 33 organizačních útvarů), kde každý organizační útvar identifikuje, analyzuje a řídí rizika spadajících do působnosti daného organizačního útvaru – rizika Úřadu. Správa rizik Úřadu je definovaná interním předpisem (Metodický pokyn k analýze rizik) a je specifikovaná v části 2.1 této přílohy.

Správa a řízení rizik kybernetické bezpečnosti probíhá na základě vyhlášky č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat – rizika kybernetické bezpečnosti. Správa rizik kybernetické bezpečnosti je specifikovaná v části 2.2 této přílohy.

1. Obecné požadavky - technologie a architektura

a) Pro provoz bude dodána konfigurovatelná webová aplikace zaměřená na správu a řízení rizik a dalších procesů nad nimi.
b) Webová aplikace bude založena na architektuře klient – server, kde klientem je webový prohlížeč a serverem je webový server.
c) Veškerá komunikace mezi klientem a webovým serverem bude probíhat výhradně přes šifrované HTTPS spojení. Komunikace bude probíhat na Objednatelem zadaném portu.
d) Webová aplikace bude zprovozněna na infrastruktuře (na operačním systému a databázi / souborovém systému) bez dalších licenčních nákladů. Hardwarové zdroje poskytne Objednatel – poskytne virtuální servery provozované na Platformě VMWare.
e) Databáze / souborový systém nejsou přímo přístupné pro koncové uživatele, pro přístup k datům koncovým uživatelem se uplatňují přístupová práva prostřednictvím webové aplikace.
f) Koncový uživatel nebude instalovat klientskou aplikaci k užívání webové aplikace. Webová aplikace je centrálně distribuována prostřednictvím jednotného image na uživatelskou stanici. Instalaci klientské části webové aplikace bude možné provést v silent modu.
g) Webová aplikace bude pro koncového uživatele dostupná prostřednictvím webového rozhraní spustitelné primárně v prohlížeči Internet Explorer.
h) Webové rozhraní aplikace pro administrátora umožní konfiguraci a řízení uživatelských práv.
i) Webová aplikace bude kompletně v českém jazyce, včetně návodů k použití.
j) Integrace webové aplikace s IS NKÚ bude možná prostřednictvím adresářových služeb (AD, LDAP) k zajištění synchronizace uživatelů. Uživatelé IS NKÚ se nebudou zakládat ručně.
k) Přihlášení uživatele k webové aplikace bude prostřednictvím SSO autentizace, uživatel nebude zadávat přihlašovací údaje (logonname, password) do webové aplikace.
l) Z/do webová aplikace bude možné provádět exporty/importy dat ve standardních formátech (požadováno CSV, XML, XLS), nebo na úrovni databáze formou databázových view s možností automatické synchronizace.
m) Data uložená ve webové aplikaci lze exportovat do jednoduchých sestav v MS Excel a formátu HTML.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

2. Funkční požadavky na správu a řízení rizik

2.1 Správa a řízení rizik Úřadu

a) Rizika se zaznamenávají do dokumentu/záznamu – Karta rizika. Karta rizika definuje a klasifikuje potenciální nebo v praxi se vyskytující riziko, stupeň významnosti rizika, strategii jeho řízení a vyhodnocení strategie řízení rizika.

b) Karta rizika obsahuje minimálně následující položky:
   - ID rizika – textové pole, identifikační číslo (pořadové číslo),
   - Název rizika – textové pole o délce max. 150 znaků,
   - Vlastník rizika – textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Popis rizika – textové pole,
   - Pravděpodobnost výskytu – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-5),
   - Dopad rizika – číselná hodnota, hodnota se vybírá z předem definovaného seznamu (hodnota 1-5),
   - Stupeň významnosti – číselná hodnota, který je vypočítaný definovaným vzorcem (pravděpodobnost výskytu x dopad rizika),
   - Kategorie – textové pole, hodnota se vybírá z předem definovaného číselníku, je možné vybrat více hodnot v rámci této položky,
   - Aktivum – textové pole, hodnota se vybírá z předem definovaného číselníku, je možné vybrat více hodnot v rámci této položky,
   - Strategie řízení rizika – textové pole, hodnota se vybírá z předem definovaného číselníku (hodnoty: redukce stupně významnosti, udržení stupně významnosti, přenos rizika, akceptovatelné (reziduální) riziko), je možné vybrat pouze jednu hodnotu v rámci této položky,
   - Poznámka – textové pole,
   - Dílčí úkoly – hypertextový odkaz na nový dokument/záznam Dílčí úkoly (= Opatření).

c) Opatření se zaznamenávají do dokumentu/záznamu – Dílčí úkoly. Karta Dílčí úkoly definuje dílčí úkoly s termínem plnění.

d) Karta Dílčí úkoly obsahuje minimálně následující položky:
   - Název dílčího úkolu – textové pole o délce max. 150 znaků,
   - Řešitel - textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Termín splnění – datumové pole,
   - Vyhodnocení úkolu - textové pole, hodnota se vybírá z předem definovaného číselníku (hodnoty: splněno, nesplněno), je možné vybrat pouze jednu hodnotu v rámci této položky,
   - Příloha – vložení hypertextového odkazu, vložení dokumentu ve formátu PDF, WORD, EXCEL, JPG.

e) Při vytvoření nového dokumentu/záznamu webová aplikace přiradí číslo číselné řady – jednoznačný identifikátor.

f) Formát číselných řad může obsahovat fixní i proměnné části, v proměnných částech lze použít sekvence čísel i písmen.

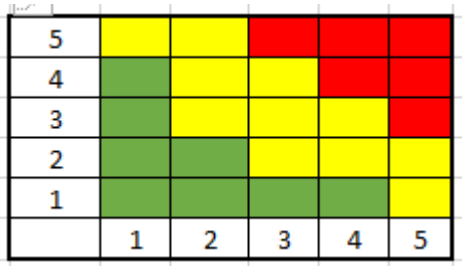
g) Pomocí položek v dokumentech/záznamech lze dokumenty/záznamy třídit, pomocí filtrů lze dokumenty/záznamy vyhledávat, a to jednoduchým filtrem i rozšířeným filtrováním s libovolně složitými filtrovacími podmínkami.

h) Webová aplikace bude zaznamenávat provedená změny v dokumentech/záznamech.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

i) Ke každému dokumentu/záznamu lze jednoduše zobrazit historii akcí, které s ním byly provedeny (např. kdy byl dokument/záznam do systému vložen, kdo a jak upravil dokument/záznam, a další).
j) K hlavnímu dokumentu/záznamu (= Karta rizika, Dílčí úkoly) lze do webové aplikace uložit i další dokumenty formou přílohy (ve formátu PDF, DOCX, XLSX).
k) Každý dokument/záznam bude uložen pouze jednou v primární složce. V dalších dokumentech/záznamech bude možný na primární dokument/záznam odkazovat (např. formou URL nebo zástupce).
l) Pro prohlížení PDF dokumentů bude stačit uživateli webový prohlížeč bez dalších závislostí. PDF dokument je možné prohlédnout celý.
m) Dokumenty/záznamy (Karty rizika, Karty Dílčí úkoly) bude možné seskupit do většího celku (= Agendy, cca 33 typů agend).
n) Každá Agenda bude mít svého správce – role Správce agendy.
o) Všechny dokumenty/záznamy ohledně správy rizik budou dostupná v souhrnném Katalogu rizik bez ohledu na zařazení v Agendě.
p) Všechny dokumenty/záznamy ohledně správy dílčích úkolů budou dostupná v souhrnném Katalogu dílčích úkolů bez ohledu na zařazení v Agendě.
q) Ve webové aplikaci bude možné vyhledávat fulltextově.
r) Správa a řízení rizik probíhají následovně:
    i. Vedoucí zaměstnanec příslušného organizačního útvaru průběžně identifikuje rizika. Identifikovaná rizika zaznamenává v Kartě rizika.
    ii. Odbor interního auditu 1 x ročně ve stanoveném termínu připravuje seznam všech zaznamenaných rizik, včetně strategie řízení, které se budou v daném termínu dál spravovat a řídit. Seznam rizik odbor interního auditu předává prezidentovi ke schválení.
    iii. Vedoucí zaměstnanec příslušného organizačního útvaru (na základě schváleného podkladu dle bodu ii.) zaznamená dílčí úkoly v Kartě dílčího úkolu k relevantním rizikům. V Kartě dílčího úkolu se zaznamená termín splnění úkolu a průběžně se zaznamenává stav plnění. Týden (7 kalendářních dní) před uplynutím termínu splnění úkolu se zašle Vedoucímu zaměstnanci příslušného organizačního útvaru a Řešiteli dílčího úkolů (v případě, že Řešitelem není vedoucí zaměstnanec) emailová notifikace o blížícím se termínu pro splnění úkolu.
    iv. Vedoucí zaměstnanec příslušného organizačního útvaru v termínu pro splnění dílčího úkolu opětovně přehodnocuje stav plnění dílčího úkolu a strategii řízení relevantního rizika.
    v. V případě, že Vedoucí zaměstnanec příslušného organizačního útvaru zaznamená u rizika v položce strategie řízení hodnotu akceptovatelné (reziduální) riziko, riziko je považováno za uzavřené a dál se s tímto rizikem v dalším období nepracuje. Za uzavřené se považují i související dílčí úkoly, i když jsou ještě ve stavu plnění. Uzavření u dílčích úkolů proběhne automaticky, kde stav dílčího úkolu se změní na stav uzavřen, bez nutnosti zásahu (editace v Kartě dílčí úkoly) Vedoucího zaměstnance příslušného organizačního útvaru.
s) Předpřipravené reporty pro uživatele, kde uživateli se zobrazí data dle oprávnění:
    i. Mapa rizik – grafické zobrazení všech rizik ve vzájemném poměru jeho pravděpodobnosti zapůsobení a míry dopadu, zobrazení v sítí 5x5 s rozlišením ve třech barvách dle významnosti, např. dle uvedeného obrázku,

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz



ii. Rizika dle významnosti – přehledová tabulka rizik s názvem rizika, vlastníkem rizika, významností,
iii. Rizika dle kategorie – přehledová tabulka rizik s názvem rizika, vlastníkem rizika na základě předem definované kategorie,
iv. Rizika dle snížení významnosti – přehledová tabulka rizik s názvem rizika, vlastníkem rizika, hodnoty významnosti, stav snížení, navýšení, nebo stav beze změny za období např. roku zpětně ke dni spuštění reportu,
v. Rizika dle agendy - přehledová tabulka rizik s názvem rizika, vlastníkem rizika, hodnoty významnosti na základě předem definované agendy,
vi. Rizika dle vlastníka – přehledová tabulka rizik s názvem rizika, vlastníkem rizika, významností přiřazených konkrétním pracovníkům nebo organizačním útvarům,
vii. Dílčí úkoly (opatření) – přehledová tabulka dílčích úkolů s názvem dílčího úkolu, řešitele dílčího úkolu, termínu splnění, stavu plnění, názvem rizika, v rámci kterého se dílčí úkol plní.

t) Z reportu bude možné si otevřít Kartu rizika nebo Kartu dílčího úkolu. Dále bude možné v reportu přidávat nebo odebírat další požadované sloupce (např. popis rizika, pravděpodobnost výskytu a další), a filtrovat dle zvolených kritérií (např. rizika dle pravděpodobnosti výskytu sestupně a další).
u) Přehled rolí, jejich činností a příslušných oprávnění, které se účastní správy rizik:
i. Vedoucí zaměstnanec příslušného organizačního útvaru (= hlavní zadavatel rizik, 70 uživatelů) – editace rizika (zadání a změna) v rámci své agendy, editace plnění opatření, zobrazení dalších rizik v agendách, ke kterým bylo přiděleno oprávnění, zobrazení reportů s daty, na která má oprávnění, obdržení notifikace,
ii. Řešitel dílčího úkolu (= řešitel plnění nápravného opatření, 36 uživatelů) – editace dílčího úkolu (opatření), zobrazení reportů s daty, na která má oprávnění, obdržení notifikace,
iii. Administrátor IA (= administrátor odboru interního auditu, 4 uživatelé) – editace rizika pro všechny agendy, editace všech dílčích úkolů, zobrazení reportů, tvorba nových reportů, přiřazení oprávnění výše uvedeným rolím,
iv. Administrátor (= administrátor aplikace, 2 uživatelé) – nastavení číselníků, tvorba WF, nastavení číselníků, nastavení notifikací,
v) Jeden uživatel může mít více rolí. Oprávnění na data budou pak dle příslušných rolí.

2.2 Správa a řízení rizik kybernetické bezpečnosti

a) Správa a řízení rizik kybernetické bezpečnosti probíhají pro každé identifikované aktivum Úřadu (aktuálně 7 aktiv – 1 primární aktivum + 6 podpůrných aktiv).
b) V rámci správy a řízení rizik kybernetické bezpečnosti se pro každé jedno aktivum provádí hodnocení aktiva, hodnocení zranitelností aktiva a hodnocení hrozeb aktiva.
c) V rámci hodnocení aktiva se u každého aktiva posuzuje, jaký dopad by mělo narušení bezpečnosti informací z hlediska narušení důvěrnosti, integrity a dostupnosti.
d) V rámci hodnocení zranitelností aktiva a hodnocení hrozeb aktiva se u každého aktiva posuzuje dopad identifikovaných zranitelností a hrozeb.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

e) Souhrnná hodnota rizika každého aktiva je vyjádřená jako funkce, kterou ovlivňuje dopad narušení bezpečnosti informací, hrozby a zranitelnosti aktiva.

2.2.1 Hodnocení aktiva – dopad narušení bezpečnosti informací z pohledu dostupnosti, integrity a důvěrnosti

a) Hodnocení aktiva se provádí v dokumentu/záznamu Karta hodnocení aktiva.
b) Karta hodnocení aktiva obsahuje minimálně následující položky:
   - ID aktiva textové pole, identifikační číslo (pořadové číslo),
   - Název aktiva – textové pole o délce max. 150 znaků,
   - Garant aktiva – textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Dopad při ztrátě/diskreditace aktiva - textové pole o délce max. 150 znaků, obsahuje informaci o dopadu,
   - Váha – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Důvěrnost – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Integrita – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Dostupnost – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Celkové skóre – číselná hodnota, která je vypočítaná definovaným vzorcem: hodnota Důvěrnost x hodnota Integrita x hodnota Dostupnost u každého identifikovaného dopadu,
   - Stupeň ochrany - číselná hodnota, která je vypočítaná definovaným vzorcem: maximální hodnota z hodnot Důvěrnost, Integrita, Dostupnost u každého identifikovaného dopadu,
   - Průměr - číselná hodnota, která je vypočítaná definovaným vzorcem: průměrná hodnota z hodnot uvedených v položce Celkové skóre,
   - Maximum - číselná hodnota, která je vypočítaná definovaným vzorcem: maximum z hodnot uvedených v položce Stupeň ochrany,
   - Hodnota aktiva - číselná hodnota, která je vypočítaná definovaným vzorcem: (Průměr + Maximum)/2,
   - Hodnocení provedeno – datumové pole,
   - Datum příštího hodnocení – datumové pole.
c) Každé aktivum má vlastní sadu definovaných možných narušení bezpečnosti informací.
d) Možné narušení bezpečnosti informací se přiřazují aktivu tak, že se vybírají z předem definovaného číselníku narušení bezpečnosti informací.
e) Jednotlivé typy narušení zaznamenává Manažer KB, který u každého aktiva zaznamenává ID narušení bezpečnosti informací, název narušení bezpečnosti informací, stav platnosti narušení bezpečnosti.
f) Hodnocení aktiva provádí Garant aktiva.

Vzor dokumentu/záznamu Hodnocení aktiva – stávající záznam ve formátu XLS:

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

NKÚ - AKTIVA DLE VKB 316/2014		GARANT	MAXIMUM	PRŮMĚR
ZAM	2	[redacted]	8	4,3

HODNOTA AKTIVA

Zaměstnanci

NÍZKÁ 6.13

DOPADY PŘI ZTRÁTĚ / DISKREDITACI AKTIVA	Důvěrnost	Integrita	Dostupnost	Celkové skóre	STUPEŇ OCHRANY
Rozsah a důležitost osobních údajů nebo obchodního tajemství	3	2	1	6	3
Rozsah dotčených právních povinností nebo jiných závazků	2	1	2	4	2
Rozsah narušení vnitřních řídících a kontrolních činností	1	1	2	2	2
Poškození veřejných, obchodních nebo ekonomických zájmů	1	1	1	1	1
Možné finanční ztráty	2	2	2	8	2
Rozsah narušení běžných činností úřadu	1	2	1	2	2
Dopady spojené s narušením důvěrnosti, integrity a dostupnosti	2	2	2	8	2
Dopady na zachování dobrého jména nebo ochranu dobré pověsti	3	1	1	3	3

2.2.2 Hodnocení zranitelností a hrozeb aktiva

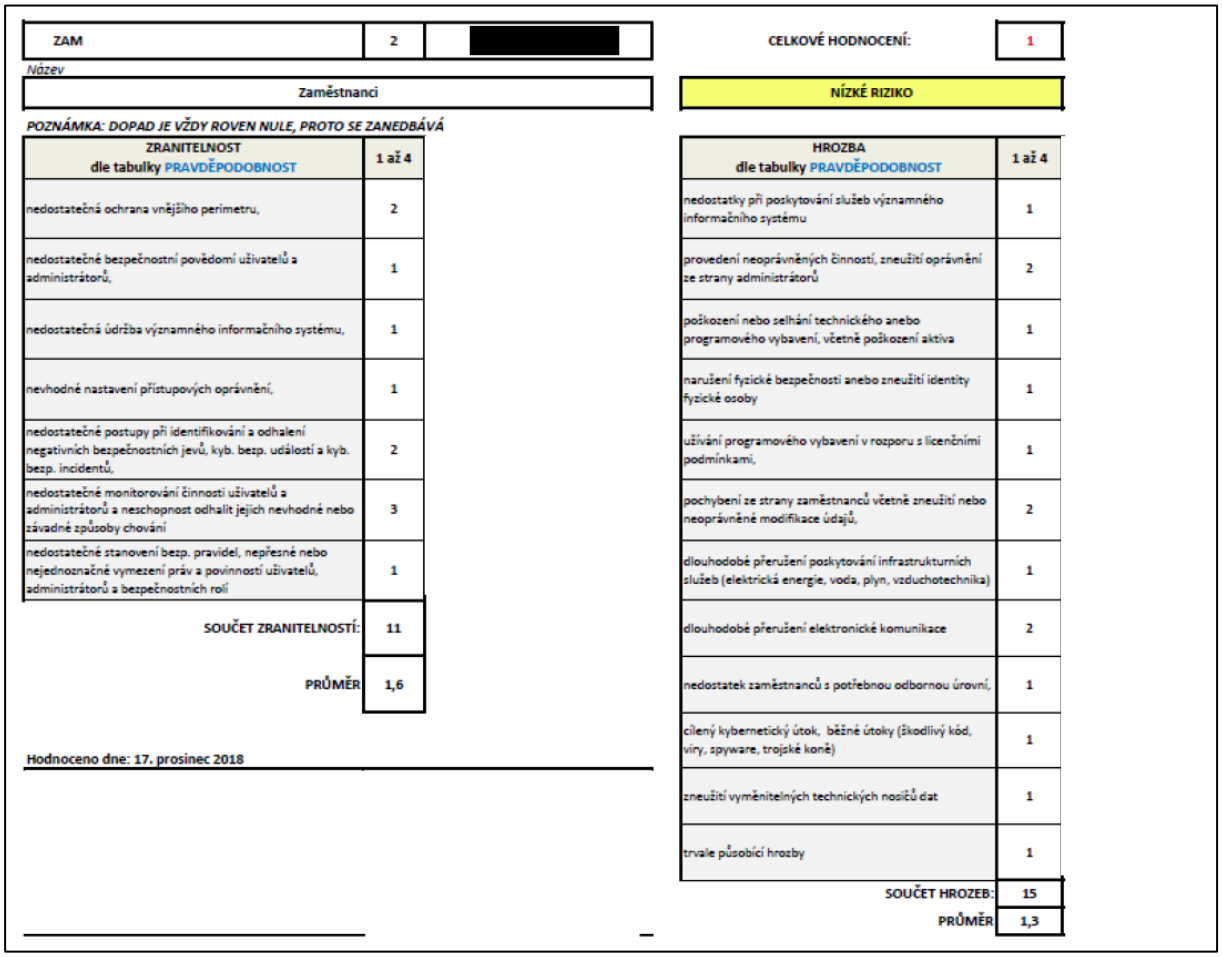
a) Hodnocení zranitelností aktiva se provádí v dokumentu/záznamu Zranitelnost aktiva.
b) Dokument/záznam Zranitelnost aktiva obsahuje minimálně následující položky:
   - Název aktiva – textové pole o délce max. 150 znaků,
   - Garant aktiva – textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Název zranitelnosti – textové pole o délce max. 255 znaků,
   - ID zranitelnosti – číselná hodnota, identifikační číslo (pořadové číslo),
   - Vlastník zranitelnosti - textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Váha – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Hodnocení zranitelnosti - číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Stav zranitelnosti aktiva - textové pole, hodnota se vybírá z předem definovaného číselníku (hodnota - aktivní, neaktivní),
   - Datum příštího hodnocení zranitelnosti – datumové pole,
   - Datum posledního hodnocení zranitelnosti – datumové pole,
   - Součet zranitelnosti aktiva – číselná hodnota, která je vypočítaná jako součet všech hodnot zadaných v položce Hodnocení zranitelnosti,
   - Průměr zranitelnosti aktiva - číselná hodnota, která je vypočítaná jako průměr ze všech hodnot zadaných v položce Hodnocení zranitelnosti.
c) Každé aktivum má vlastní sadu definovaných zranitelností.
d) Zranitelnosti aktiva se přiřazují aktivu tak, že se vybírají z předem definovaného číselníku zranitelností.
e) Zranitelnosti aktiva zaznamenáva Manažer KB, který u každého aktiva zaznamenává ID zranitelnosti, název zranitelnosti, stav zranitelnosti, vlastníka zranitelnosti.
f) Hodnocení zranitelnosti provádí Garant aktiva (v budoucnu bude hodnocení provádět i role Vlastník zranitelnosti).

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

g) Hodnocení hrozeb aktiva se provádí v dokumentu/záznamu Hrozby aktiva.
h) Dokument/záznam Hrozby aktiva obsahuje minimálně následující položky:
   - Název aktiva – textové pole o délce max. 150 znaků,
   - Garant aktiva – textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Název hrozby – textové pole o délce max. 255 znaků,
   - ID hrozby – textové pole, identifikační číslo (pořadové číslo),
   - Vlastník hrozby - textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Váha – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Hodnocení hrozby - číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Stav hrozby aktiva – textové pole, hodnota se vybírá z předem definovaného číselníku (hodnota - aktivní, neaktivní),
   - Datum příštího hodnocení hrozby – datumové pole,
   - Datum posledního hodnocení hrozby – datumové pole,
   - Součet hrozby aktiva – číselná hodnota, která je vypočítaná jako součet všech hodnot zadaných v položce Hodnocení hrozby,
   - Průměr hrozby aktiva - číselná hodnota, která je vypočítaná jako průměr ze všech hodnot zadaných v položce Hodnocení hrozby.
i) Každé aktivum má vlastní sadu definovaných hrozeb.
j) Hrozby aktiva se přiřazují aktivu tak, že se vybírají z předem definovaného číselníku hrozeb.
k) Hrozby aktiva zaznamenává Manažer KB, který u každého aktiva zaznamenává ID hrozby, název hrozby, stav hrozby, vlastníka hrozby.
l) Hodnocení hrozeb provádí Garant aktiva (v budoucnu bude hodnocení provádět i role Vlastník hrozby).
m) Celkové hodnocení - celková hodnota rizika aktiva je daná výpočtem: průměrná hodnota z hodnocení zranitelnosti aktiva + průměrná hodnota z hodnocení zranitelnosti aktiva)/2.

Vzor dokumentu/záznamu Hodnocení aktiva – stávající záznam ve formátu XLS:

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz



ZAM	2	[redacted]	CELKOVÉ HODNOCENÍ:	1

Název

Zaměstnanci	NÍZKÉ RIZIKO

POZNÁMKA: DOPAD JE VŽDY ROVEN NULE, PROTO SE ZANEDBÁVÁ

ZRANITELNOST dle tabulky PRAVDĚPODOBNOST	1 až 4
nedostatečná ochrana vnějšího perimetru,	2
nedostatečné bezpečnostní povědomí uživatelů a administrátorů,	1
nedostatečná údržba významného informačního systému,	1
nevhodné nastavení přístupových oprávnění,	1
nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kyb. bezp. událostí a kyb. bezp. incidentů,	2
nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	3
nedostatečné stanovení bezp. pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	1
SOUČET ZRANITELNOSTÍ:	11
PRŮMĚR	1,6

Hodnoceno dne: 17. prosinec 2018

HROZBA dle tabulky PRAVDĚPODOBNOST	1 až 4
nedostatky při poskytování služeb významného informačního systému	1
provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	2
poškození nebo selhání technického anebo programového vybavení, včetně poškození aktiva	1
narušení fyzické bezpečnosti anebo zneužití identity fyzické osoby	1
užívání programového vybavení v rozporu s licenčními podmínkami,	1
pochybení ze strany zaměstnanců včetně zneužití nebo neoprávněné modifikace údajů,	2
dlouhodobé přerušení poskytování infrastrukturních služeb (elektrická energie, voda, plyn, vzduchotechnika)	1
dlouhodobé přerušení elektronické komunikace	2
nedostatek zaměstnanců s potřebnou odbornou úrovní,	1
cílený kybernetický útok, běžné útoky (škodlivý kód, viry, spyware, trojské koně)	1
zneužití vyměnitelných technických nosičů dat	1
trvale působící hrozby	1
SOUČET HROZEB:	15
PRŮMĚR	1,3

2.2.3 Postup správy a řízení rizik kybernetické bezpečnosti

a) Správa a řízení rizik kybernetické bezpečnosti je prováděno pro každé definované aktivum. Rizika se zaznamenávají v dokumentu/záznamu Karta aktiva.

b) Karta aktiva obsahuje minimálně následující položky:
   - ID aktiva – textové pole, identifikační číslo (pořadové číslo),
   - Název aktiva – textové pole o délce max. 150 znaků,
   - Garant aktiva – textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Typ aktiva – textové pole, hodnota se vybírá z předem definovaného číselníku (hodnota – primární aktivum, podpůrné aktivum),
   - Váha – číselná hodnota, hodnota se vybírá z předem definovaného číselníku (hodnota 1-4),
   - Datum posledního přehodnocení – datumové pole,
   - Důvod posledního přehodnocení – textové pole o délce max. 150 znaků,
   - Datum příštího přehodnocení – datumové pole,
   - Posouzení možných dopadů na aktiva – textové pole, do této části se vyplní zranitelnosti aktiva (položka Název zranitelnosti aktiva), které mají uvedenou hodnotu 3 a vyšší,
   - Hodnocení existujících hrozeb – textové pole, hodnota se automaticky vyplní z Karty hrozeb, položka Průměr hrozby aktiva,
   - Hodnocení existujících zranitelností – textové pole, hodnota se automaticky vyplní z Karty zranitelnosti, proložka Průměr zranitelností aktiva,

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

- Stanovení úrovně rizika – číselná hodnota, která je vypočítaná jako (Průměr zranitelnosti aktiva + Průměr hrozby aktiva) / 2,
- Určení a schválení přijatelných rizik – textové pole, hodnota se automaticky vyplní dle Akceptace rizika,
- Hodnocení existujících opatření + návrh nových opatření – hypertextový odkaz na dokument/záznam Opatření,
- Hodnocení aktiva – hypertextový odkaz na dokument/záznam Hodnocení aktiva,
- Hodnocení zranitelností aktiva – hypertextový odkaz na dokument/záznam Zranitelnosti aktiva,
- Hodnocení hrozeb aktiva - hypertextový odkaz na dokument/záznam Hrozby aktiva,
- Poznámka – textové pole o délce max. 150 znaků,

c) Dokument/záznam Karta aktiva vytváří manažer KB, který zaznamenává minimálně položky: ID aktiva, Název aktiva, Garant aktiva, Typ aktiva.

d) Garant aktiva v předepsaných termínech provede hodnocení aktiva (dle bodu 2.2.1) a hodnocení zranitelností a hrozeb aktiva (dle bodu 2.2.2).

e) Vlastníci zranitelností a Vlastníci hrozeb při zvýšení rizika navrhují Opatření ke snížení rizika aktiva.

f) Manažer KB relevantní Opatření zaznamenává v dokumentu/záznamu Opatření aktiva.

g) Dokument/záznam Opatření aktiva obsahuje minimálně položky:
   - ID opatření – textové pole, identifikační číslo (pořadové číslo),
   - Název opatření – textové pole o délce max. 150 znaků,
   - Typ opatření – textové pole, hodnota se vybírá z předem definovaného číselníku (hodnoty: dočasný, trvalý), je možné vybrat pouze jednu hodnotu v rámci této položky,
   - Řešitel - textové pole, hodnota se vybírá z AD/LDAP (Users/uživatel nebo Security Group/organizační útvar),
   - Termín splnění – datumové pole,
   - Vyhodnocení úkolu - textové pole, hodnota se vybírá z předem definovaného číselníku (hodnoty: splněno, nesplněno), je možné vybrat pouze jednu hodnotu v rámci této položky,
   - ID aktiva - textové pole/hypertextový odkaz, identifikační číslo (pořadové číslo),
   - Název aktiva - textové pole/hypertextový odkaz o délce max. 150 znaků na vybrané aktivum, ke kterému se opatření vztahuje,
   - Souvisí se zranitelností – textové pole/hypertextový odkaz o délce max. 150 znaků na vybranou zranitelnost, ke kterému se opatření vztahuje, je možné vybrat více hodnot v rámci této položky,
   - Souvisí s hrozbou - textové pole/hypertextový odkaz o délce max. 150 znaků na vybranou hrozbu, ke které se opatření vztahuje, je možné vybrat více hodnot v rámci této položky,
   - Příloha – vložení hypertextového odkazu, vložení dokumentu ve formátu PDF, WORD, EXCEL, JPG.
   - Poznámka – textové pole o délce max. 255 znaků.

h) Garant aktiva, Vlastník hrozby, Vlastník zranitelnosti, Řešitel opatření jsou ve stanovených termínech upozorněni emailovou notifikací a potřebě opětovného přehodnocení aktiva nebo opatření.

i) Přehled rolí, jejich činností a příslušných oprávnění, které se účastní správy a řízení kybernetických rizik:
   i. Manažer KB (2 uživatelé) – editace Karta aktiva (zadání a změna všech aktiv), editace Zranitelnosti aktiva, editace Hrozby aktiva, editace Opatření aktiva,

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

editace dat bude jenom u požadovaných položek, zobrazení reportů, obdržení notifikace, nastavení číselníků, tvorba nových reportů, přiřazení oprávnění a příslušných rolí,

ii. Garant aktiva (14 uživatelů) – editace Karta aktiva, editace Karta hodnocení aktiva, editace Zranitelnosti aktiva, editace Hrozby aktiva, editace Opatření aktiva editace, editace dat bude jenom u požadovaných položek, zobrazení reportů s daty, na která má oprávnění, obdržení notifikace,

iii. Vlastník zranitelnosti, Vlastník hrozby (20 uživatelů) – editace Zranitelnosti aktiva, editace Hrozby aktiva, editace dat bude jenom u požadovaných položek, zobrazení reportů s daty, na která má oprávnění, obdržení notifikace,

iv. Řešitel opatření – editace Opatření aktiva, editace dat bude jenom u požadovaných položek, zobrazení reportů s daty, na která má oprávnění, obdržení notifikace,

v. Administrátor IA (= administrátor odboru interního auditu, 4 uživatelé) – náhled Karta aktiva, náhled Karta hodnocení aktiva, náhled Zranitelnosti aktiva, náhled Hrozby aktiva, náhled Opatření aktiva editace, zobrazení reportů,

vi. Administrátor (= administrátor aplikace, 2 uživatelé) – nastavení číselníků, tvorba WF, nastavení notifikací.

j) Jeden uživatel může mít více rolí. Oprávnění na data budou pak dle příslušných rolí.

k) Při vytvoření nového dokumentu/záznamu webová aplikace přiradí číslo číselné řady – jednoznačný identifikátor.

l) Formát číselných řad může obsahovat fixní i proměnné části, v proměnných částech lze použít sekvence čísel i písmen.

m) Pomocí položek v dokumentech/záznamech lze dokumenty/záznamy třídit, pomocí filtrů lze dokumenty/záznamy vyhledávat, a to jednoduchým filtrem i rozšířeným filtrováním s libovolně složitými filtrovacími podmínkami.

n) Webová aplikace bude zaznamenávat provedená změny v dokumentech/záznamech.

o) Ke každému dokumentu/záznamu lze jednoduše zobrazit historii akcí, které s ním byly provedeny (např. kdy byl dokument/záznam do systému vložen, kdo a jak upravil dokument/záznam, a další) až na úroveň položek dokumentu/záznamu.

p) První zadání dat proběhne hromadně importem z již existujících souborů ve formátu XLS, které se využívají k správě a řízení rizik kybernetické bezpečnosti.

2.2.4 Předpřipravené reporty

a) Mapa rizik (= akceptační tabulka rizika) – grafické zobrazení všech aktiv ve vzájemném poměru hodnoty aktiva a hodnoty rizika, zobrazení v sítí 4x4 s rozlišením ve čtyřech barvách dle významnosti. Z mapy rizik bude možné si otevřít Kartu aktiva.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

KORELACE	← Hodnota rizika →			
Hodnota aktiva↓	1 Nízké	2 Střední	3 Vysoké	4 Kritické
1 Nízká	A - zcela vyhovující	A - zcela vyhovující	B - přijatelná	C - nedostatečná
2 Střední	A - zcela vyhovující	B- přijatelná	C - nedostatečná	D - zcela nedostatečná
3 Vysoká	A - zcela vyhovující	C - nedostatečná	D - zcela nedostatečná	D - zcela nedostatečná
4 Kritická	B- přijatelná	D - zcela nedostatečná	D - zcela nedostatečná	D - zcela nedostatečná

b) Přehled zranitelnosti aktiva - v přehledu se zobrazí tabulkový seznam všech zranitelností, ke kterým má daná role (Vlastník zranitelnosti) oprávnění, ve výstupu se zobrazí Název zranitelnosti, Vlastník zranitelnosti, Hodnota zranitelnosti, Datum posledního hodnocení zranitelnosti, Datum příštího hodnocení zranitelnosti, Název aktiva, Garant aktiva, Stav zranitelnosti, Název opatření (v případě, že existuje související opatření). Z reportu bude možné si otevřít Kartu aktiva, Opatření aktiva. Dále bude možné v reportu přidávat nebo odebírat další požadované sloupce (např. ID zranitelnosti), a filtrovat dle zvolených kritérií (např. zranitelnosti dle Data příštího hodnocení sestupně a další).

c) Průřezové hodnocení zranitelností – v přehledu se zobrazí tabulkový seznam, ke kterému má daná role oprávnění, ve výstupu se zobrazí Vlastník zranitelnosti, Organizační zařazení Vlastníka zranitelnosti, Název zranitelnosti, Hodnota zranitelnosti pro aktivum 1, Hodnota zranitelnosti pro aktivum 2, ..., Průměrná hodnota zranitelnosti za všechna aktiva.

	ZRANITELNOST	KIS:	ZAM:	DOD:	TECH:	KOM:	PRG:	ZAR:	průměr
Zranitelnost 1	nedostatečná ochrana vnějšího perimetru,	2	2	1	2	3	2	1	1,86
Zranitelnost 2	nedostatečné bezpečnostní povědomí uživatelů a administrátorů,	1	1	2	2	3	1	1	1,57
Zranitelnost 3	nedostatečná údržba významného informačního systému,	1	1	2	2	2	1	1	1,43
Zranitelnost 4	nevhodné nastavení přístupových oprávnění,	1	1	2	2	2	2	1	1,57
Zranitelnost 5	nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kyb. bezp. událostí a kyb. bezp. incidentů,	1	2	2	3	3	2	2	2,14
Zranitelnost 6	nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	2	3	2	3	3	2	2	2,43
Zranitelnost 7	nedostatečné stanovení bezp. pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	1	1	2	2	1	1	1,43

d) Přehled hrozby aktiva - v přehledu se zobrazí tabulkový seznam všech hrozeb, ke kterým má daná role oprávnění (Vlastník hrozby), ve výstupu se zobrazí Název hrozby, Vlastník hrozby, Hodnota hrozby, Datum posledního hodnocení hrozby, Datum příštího hodnocení hrozby, Název aktiva, Garant aktiva, Stav hrozby Název opatření

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

(v případě, že existuje související opatření). Z reportu bude možné si otevřít Kartu aktiva, Opatření aktiva. Dále bude možné v reportu přidávat nebo odebírat další požadované sloupce (např. ID hrozby), a filtrovat dle zvolených kritérií (např. hrozby dle Data příštího hodnocení sestupně a další).

e) Průřezové hodnocení hrozeb – v přehledu se zobrazí tabulkový seznam, ke kterému má daná role oprávnění, ve výstupu se zobrazí Vlastník hrozby, Organizační zařazení Vlastníka hrozby, Název hrozby, Hodnota hrozby pro aktivum 1, Hodnota hrozby pro aktivum 2, ..., Průměrná hodnota hrozby za všechna aktiva.

ID	POPIS	KIS:	ZAM:	DOD:	TECH:	KOM:	PROG:	ZAR:	průměr
Hrozba 1	nedostatky při poskytování služeb významného informačního systému	2	1	1	1	1	1	1	1,14
Hrozba 2	provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	2	2	2	3	3	2	1	2,14
Hrozba 3	poškození nebo selhání technického anebo programového vybavení, včetně poškození aktiva	2	1	1	1	1	1	3	1,43
Hrozba 4	narušení fyzické bezpečnosti anebo zneužití identity fyzické osoby	1	1	1	1	1	2	2	1,29

f) Seznam Opatření aktiva - přehledová tabulka opatření s názvem opatření, řešitelem opatření, termínu splnění, stavu plnění, názvem rizika, názvem aktiva, související zranitelností, související hrozby, v rámci kterého se opatření plní. Z reportu bude možné si otevřít Kartu aktiva, Kartu opatření. Dále bude možné v reportu přidávat nebo odebírat další požadované sloupce (např. typ opatření, souvisí se zranitelností), a filtrovat dle zvolených kritérií (např. termín splnění sestupně a další). Z reportu bude možné otevřít Kartu aktiva, Kartu zranitelnosti aktiva, Kartu hrozby aktiva,

g) V reportech se budou uživateli zobrazovat data dle oprávnění na jednotlivá data.

3 Další funkční požadavky

3.1 Workflow (schvalovací proces), plánované úlohy a emailové notifikace

a) Webová aplikace bude umožňovat konfiguraci workflow (schvalovací proces) nad agendou dokumentů/záznamů.

b) V rámci workflow (schvalovacího procesu) bude možné nakonfigurovat též emailové notifikace.

c) Uživatel může být emailem notifikován o nových dokumentech/záznamech v agendě, nebo o dokumentech/záznamech, které má vyřídit v rámci workflow (schvalovacího procesu).

d) Notifikace mohou být nastaveny jako souhrnné, např. jednou za den, nebo jako okamžité, tj. uživatel dostane email okamžitě po založení nebo změně stavu dokumentu/záznamu.

e) Ve webové aplikaci bude možné definovat pravidelně spouštěné akce – plánované úlohy. Pomocí plánovaných úloh bude možné např. hlídat termíny plnění dílčích úkolů, nebo workflow (schvalovacích procesů) dokumentů/záznamu.

3.2 Autentizace a řízení přístupových oprávnění k dokumentům/záznamům

a) Uživatele a/nebo role (skupiny) bude možné automaticky synchronizovat se stávající Active Directory.

b) Prostřednictvím administrátorského rozhraní je možné přidělovat přístupová oprávnění uživatelům na jednotlivé agendy, dokumenty/záznamy v roli Administrátor.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

c) Nastavování přístupových oprávnění k dokumentům/záznamům bude k dispozici i pro roli Správce agendy v rámci agendy, u které je správcem.
d) Přístupová oprávnění bude možné řídit až na úroveň jednotlivých dokumentů/záznamů.

3.3 Administrátorský přístup

a) Systém poskytne administrátorům správu prostřednictvím grafického uživatelského rozhraní (GUI).
b) Administrátor zde bude moct zakládat nové agendy, konfigurovat položky dokumentu/záznamu pro Kartu rizika a Kartu dílčích úkolů, konfigurovat číselníky, konfigurovat oprávnění a vytvářet přístupové skupiny, definovat stavy workflow, emailové notifikace a plánované úlohy.
c) Webová aplikace umožní omezit administrátorské akce např. pouze na vkládání uživatelů do rolí.

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

Příloha č. 3 – Seznámení externího uživatele se zásadami bezpečnosti a užívání ICT

Seznámení externího uživatele se zásadami bezpečnosti a užívání ICT

VYPLŇTE TISKACÍM PÍSMEM

Jméno a příjmení	
Mobilní telefon	
Firma	

Přístup k ICT NKÚ (nebo funkční subsystém)	

Dle smlouvy	**Do data (platnost smlouvy)**			
Přístup k ICT NKÚ	**Vzdálený přístup**		**Vlastní zařízení**	
	Lokálně v NKÚ		**Zapůjčeno NKÚ**	
	☐ ANO / ☐ NE		*✓ ANO / × NE*	

Přístupová práva	
k čemu - jaká	

Odpovídá zaměstnanec	
Datum a podpis	
Útvar	

Externí uživatel podpisem tohoto dokumentu
potvrzuje, že pozorně přečetl a porozuměl pravidlům,
která jsou na druhé straně tohoto dokumentu.

Podpis externího uživatele	
Datum, jméno, příjmení	

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz

Seznámení externího uživatele se zásadami bezpečnosti a užívání ICT

(1) Externí uživatel:
   a) potvrzuje, že byl seznámen s těmito zásadami bezpečnosti ICT Nejvyššího kontrolního úřadu (dále také „Úřad"), a zavazuje se tyto zásady dodržovat,
   b) potvrzuje, že ke splnění jeho povinností vůči Úřadu postačuje výše uvedený rozsah uživatelských práv,
   c) je tímto zavázán používat svá uživatelská práva pouze k dosažení výše uvedeného účelu, případně k dosažení oprávněného zájmu Úřadu, pokud je mu tento zájem znám,
   d) je tímto zavázán zachovávat mlčenlivost o veškerých informacích, které se dozvěděl v souvislosti se zpřístupněním ICT a IS Úřadu,
   e) je tímto zavázán pro případ porušení výše stanoveného závazku uhradit Úřadu škodu vzniklou v důsledku tohoto porušení.

(2) Externí uživatel je oprávněn používat ICT pouze v souvislosti s plněním svých závazků vůči Úřadu a dále je povinen chránit ICT Úřadu před poškozením, zneužitím, neoprávněnou manipulací, udržovat jemu zapůjčené prostředky ICT v čistotě a funkčním stavu a při práci dodržovat zásady hospodárnosti a bezpečnosti.

(3) Externí uživatel je dále povinen:
   a) chránit veškeré jím používané nebo spravované informace Úřadu a o Úřadu;
   b) chránit přístupové prostředky Úřadu, které používá nebo se jejich prostřednictvím připojuje do IS Úřadu, proti jejich zneužití jinými osobami; v případě podezření, že došlo ke kompromitaci přístupových údajů (heslo, PIN apod.), nebo v případě ztráty či poškození přístupového bodu je povinen okamžitě nahlásit takové podezření odboru informatiky;
   c) v případě vad či nefunkčnosti ICT neprodleně informovat odbor informatiky.

(4) Externí uživatel odpovídá za informace, které vytvořil, a za způsob jejich uložení.

(5) Externí uživatel nesmí:
   a) přemisťovat prostředky ICT Úřadu mimo dohodnutá a schválená místa,
   b) pokoušet se instalovat jakékoliv aplikace, služby, programy a měnit systémové soubory ICT Úřadu bez souhlasu odboru informatiky,
   c) umožnit jiným osobám přístup do ICT Úřadu pod svou identitou s výjimkou vzdálené pomoci od zaměstnanců odboru informatiky,
   d) zjišťovat informace, ke kterým nemá práva, a jakkoli s nimi nakládat,
   e) poskytovat neveřejné informace z Úřadu jiným osobám, než kterým přísluší,
   f) odesílat neveřejné informace mimo Úřad bez zabezpečení,
   g) ukládat neveřejné informace Úřadu na externí datové zdroje, pokud nejsou zabezpečeny nebo není zajištěna jejich bezpečnost mimo Úřad,
   h) porušovat licenční a záruční podmínky komponent ICT Úřadu.

(6) Informace o zpracování osobních údajů podle čl. 13 nařízení Evropského parlamentu a Rady (EU) č. 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), (dále jen „Nařízení").
NKÚ z důvodu ochrany bezpečnosti IT systémů před nežádoucími zásahy požaduje po externím uživateli poskytnutí těchto osobních údajů: jméno, příjmení, číslo mobilního telefonu. Bez poskytnutí těchto dat nebude externímu uživateli přístup do IT systémů NKÚ umožněn. S osobními údaji NKÚ jako správce údajů nakládá výhradně v souladu s platnou legislativou, zejm. s Nařízením. Osobní údaje nejsou poskytovány třetím stranám ani do zahraničí. Osobní údaje budou zpracovávány po dobu trvání vztahu mezi NKÚ a externím uživatelem. Externí uživatel má právo požadovat od NKÚ opravu nebo výmaz osobních údajů, vznést námitku proti zpracování, případně podat stížnost u dozorového úřadu.

Odbor informatiky: rozumí se odbor informatiky Nejvyššího kontrolního úřadu, linka na Helpdesk 5333, mimo Úřad 233 045 333.

Přístupový prostředek: počítač, notebook, smartphone či jiná technologie, kterou se externí uživatel připojuje do IS Nejvyššího kontrolního úřadu.

PŘEČTENÍ POTVRZUJE EXTERNÍ UŽIVATEL PODPISEM

Tel.: 233 045 111, e-mail: podatelna@nku.cz, internet: www.nku.cz